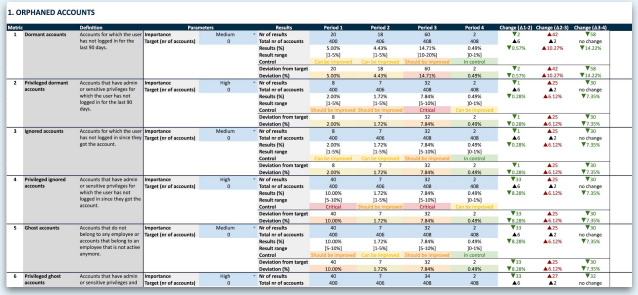
ELIMITY

HOW TO PROVE THAT YOU ARE IN CONTROL

CONTENTS

Eager to get started yourself?

We created a canvas to help you prove that you're in control of your users and their access.


1. ORPHANED ACCOUNTS

Metric	Definition	Parameters	Results	Period 1	Period 2	Period 3	Period 4	Change (1-2)	Change (2-3)	Change (3-4)
1 Dormant accounts	Accounts for which the user has not logged in for the last 90 days.	Importance: Medium Target (nr of accounts): 0	Nr of results	20	18	60	2	▼2	▲42	▼58
			Total nr of accounts	400	406	408	408	▲6	▲2	no change
			Results (%)	5.00%	4.43%	14.71%	0.49%	▼0.57%	▲10.27%	▼14.22%
			Result range	[1-5%]	[1-5%]	[10-20%]	[0-1%]			
			Control	Can be improved	Can be improved	Should be improved	In control			
			Deviation from target	20	18	60	2	▼2	▲42	▼58
			Deviation (%)	5.00%	4.43%	14.71%	0.49%	▼0.57%	▲10.27%	▼14.22%
2 Privileged dormant accounts	Accounts that have admin or sensitive privileges for which the user has not logged in for the last 90 days.	Importance: High Target (nr of accounts): 0	Nr of results	8	7	32	2	▼1	▲25	▼30
			Total nr of accounts	400	406	408	408	▲6	▲2	no change
			Results (%)	2.00%	1.72%	7.84%	0.49%	▼0.28%	▲6.12%	▼7.35%
			Result range	[1-5%]	[1-5%]	[5-10%]	[0-1%]			
			Control	Should be improved	Should be improved	Critical	Can be improved			
			Deviation from target	8	7	32	2	▼1	▲25	▼30
			Deviation (%)	2.00%	1.72%	7.84%	0.49%	▼0.28%	▲6.12%	▼7.35%
3 Ignored accounts	Accounts for which the user has not logged in since they got the account.	Importance: Medium Target (nr of accounts): 0	Nr of results	8	7	32	2	▼1	▲25	▼30
			Total nr of accounts	400	406	408	408	▲6	▲2	no change
			Results (%)	2.00%	1.72%	7.84%	0.49%	▼0.28%	▲6.12%	▼7.35%
			Result range	[1-5%]	[1-5%]	[5-10%]	[0-1%]			
			Control	Can be improved	Can be improved	Should be improved	In control			
			Deviation from target	8	7	32	2	▼1	▲25	▼30
			Deviation (%)	2.00%	1.72%	7.84%	0.49%	▼0.28%	▲6.12%	▼7.35%
4 Privileged ignored accounts	Accounts that have admin or sensitive privileges for which the user has not logged in since they got the account.	Importance: High Target (nr of accounts): 0	Nr of results	40	7	32	2	▼33	▲25	▼30
			Total nr of accounts	400	406	408	408	▲6	▲2	no change
			Results (%)	10.00%	1.72%	7.84%	0.49%	▼8.28%	▲6.12%	▼7.35%
			Result range	[5-10%]	[1-5%]	[5-10%]	[0-1%]			
			Control	Critical	Should be improved	Critical	Can be improved			
			Deviation from target	40	7	32	2	▼33	▲25	▼30
			Deviation (%)	10.00%	1.72%	7.84%	0.49%	▼8.28%	▲6.12%	▼7.35%
5 Ghost accounts	Accounts that do not belong to any employee or accounts that belong to an employee that is not active anymore.	Importance: Medium Target (nr of accounts): 0	Nr of results	40	7	32	2	▼33	▲25	▼30
			Total nr of accounts	400	406	408	408	▲6	▲2	no change
			Results (%)	10.00%	1.72%	7.84%	0.49%	▼8.28%	▲6.12%	▼7.35%
			Result range	[5-10%]	[1-5%]	[5-10%]	[0-1%]			
			Control	Should be improved	Can be improved	Should be improved	In control			
			Deviation from target	40	7	32	2	▼33	▲25	▼30
			Deviation (%)	10.00%	1.72%	7.84%	0.49%	▼8.28%	▲6.12%	▼7.35%
6 Privileged ghost accounts	Accounts that have admin or sensitive privileges and	Importance: High Target (nr of accounts): 0	Nr of results	40	7	34	2	▼33	▲27	▼32
			Total nr of accounts	400	406	408	408	▲6	▲2	no change

Key identity indicator canvas

Download the canvas

INTRODUCTION

Over the last decade, IT complexity has grown to challenging levels. Almost every company now has to manage a large amount of applications in a complex IT infrastructure consisting of large amounts of accounts and permissions.

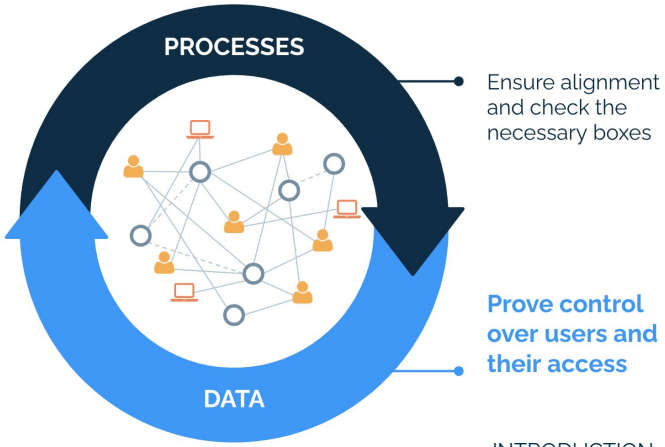
Having control over who can access which data in such an environment is crucial for privacy, compliance and protecting against cyber threats.

The traditional answer to this challenge is introducing human governance processes, typically for requesting, approving and reviewing employees' accesses. Those processes are crucial for your operational efficiency and having them checks the necessary compliance boxes, but they don't necessarily lead to actually being in control of the users and their access.

How do you know if you're in control? And how can you prove it?

Those questions are exactly why we wrote this guide. Because reporting about your current identity status and identifying potential risks or gaps remains a challenge.

Based on our own experience and frameworks such as ISO 27001, we bundled a set of crucial indicators that you should measure in order to know whether you are in control - and to prove that you are.



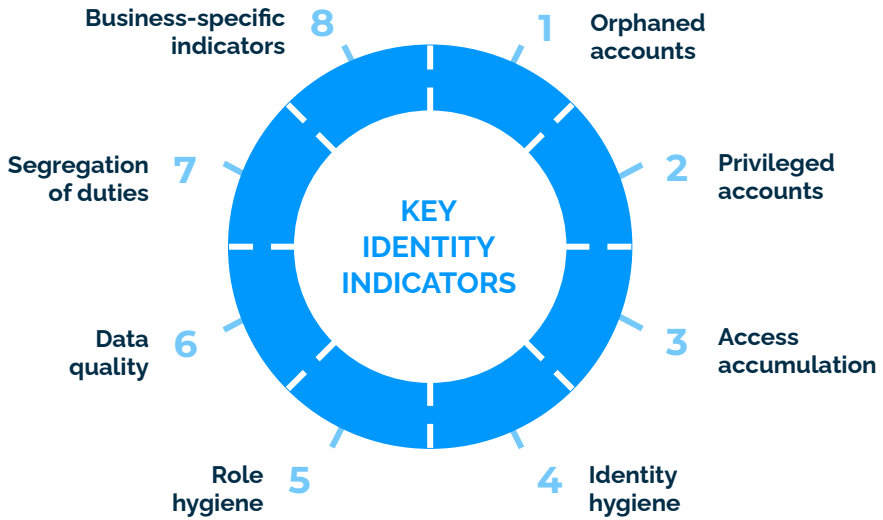
8 CATEGORIES OF KEY IDENTITY INDICATORS

In this guide, we'll give you an overview of eight categories of key identity indicators focused on showing that you're in control. These categories have proven to be complete for the majority of the organizations that strive for effective identity management and want to avoid major security risks.

KPI? KRI? KCI?

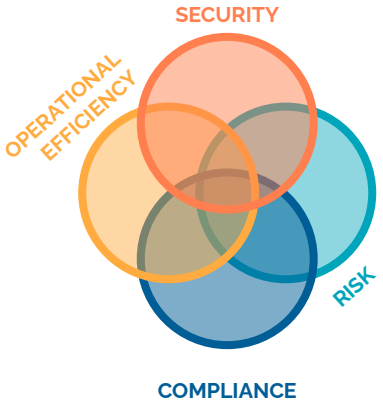
Key performance indicators (KPIs) measure performance - the achievement of identified goals. Key risk indicators (KRIs) measure risk exposure - they are an early warning to potential threats. Key control indicators (KCIs) measure the effectiveness of controls that are put in place.

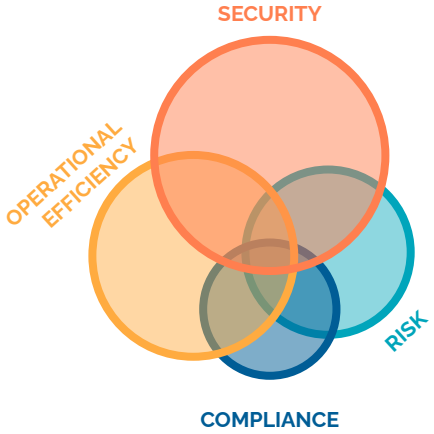
One of the main goals of identity management is, however, reducing risk. And the performance of identity management is translated for a large part into the effectiveness of processes, the output. As such, there is not always a clear or strict distinction between a KPI, KRI and KCI within identity management. In this guide, we use the term key identity indicator.



What does it mean to be in control?

There are 4 aspects of being in control of your identities: security, risk, operational efficiency and compliance. The key identity indicators described next often provide evidence for multiple aspects at once. This is illustrated in the figure below.





The right choice of indicators

For most of the organizations the same set of key identity indicators is relevant. Nevertheless, no two organizations are exactly the same. Depending on their focus areas of being in control, some indicators will be more relevant than others. Answering questions that matter and getting support from management will be much easier if the indicators are aligned with your focus areas.

It's important to understand that the choice and priority of indicators is not set in stone for all time. There are several factors that could influence what it means to be in control for your organization. Think about strategies and goals that develop over time, more information that becomes available, changes in the regulatory landscape, etcetera.

In the following pages we'll take a closer look at each of these categories.

1. Orphaned accounts

What: Accounts that are no longer active or have no owner.

Why: Security | Operational efficiency

Details:

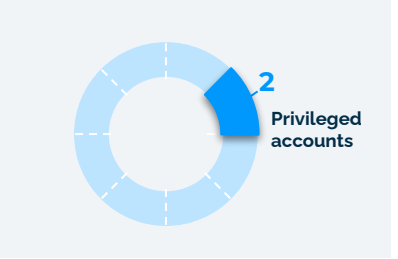
Orphaned accounts form an interesting path for hackers to gain access to organization resources, applications or systems. Organizations that fail to take the necessary steps to close these entry points leave the door on a jar for attackers, and expose themselves to unnecessary risk. By identifying and cleaning up these accounts, security risk is reduced significantly.

Moreover, tracking orphaned accounts can provide insights to improve operational efficiency. When an employee leaves the organization or when a contractor's project has ended, their accounts must be deactivated (i.e. disabled). This should be part of the typical offboarding process. However, in practice, it happens that those accounts are incorrectly deactivated or not deactivated at all. By finding out why these accounts were not deactivated, the offboarding processes can be improved.

Some metrics:

- Accounts for which the user has 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 vary for different types of accounts and between organizations. Often 90 days is considered for standard accounts.
- Accounts for which the user has not logged in since they got the account, also called *ignored accounts*.
- Uncorrelated accounts, also known as *ghost accounts*. These are accounts that do not belong to any employee or accounts that belong to an employee that is not active anymore. So in other words, accounts without an active owner.
- Accounts with a status indicating inactivity. Think for example about an employment status 'retired' or an activity status 'inactive'. The clue is to look at the user characteristics in the identity system that could indicate inactivity of a user.

2. Privileged accounts



What: Accounts that have significantly more access rights than ordinary accounts. They exist in many forms and shapes.

Why: Security

Details:

Privileged accounts give significant access to organization resources and sensitive data, or can change or disable (security) systems. 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'. It's impossible to eliminate all privileged accounts. You need them. But it's good practice to keep an eye on them and keep them to a minimum.

Rule of thumb

A rule of thumb about when an account can be identified as having a high number of roles or permissions: the total number of roles or permissions exceeds twice the average.

Some metrics:

- Administrator accounts.
- 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.
- Privileged data accounts. Even though these accounts are not typical privileged accounts, they should be considered privileged anyway, because of the sensitive data they can access.
- Privileged role-based accounts. Depending on the role model, certain roles can be considered privileged. Therefore, we should consider accounts assigned to one or more of these roles as privileged accounts.
- Accounts assigned with a high number of roles or permissions. What is considered as 'high' depends on the role model and organizational context.

3. Access accumulation

What: Users that have accumulated far more access rights than they need to do their job.

Why: Security

Details:

The cumulated access rights and permissions of all your users together determine the attack surface size of your organization. Unfortunately, there's often a gap between the granted access rights and the required access rights. This indicates that users have too many access rights, unnecessarily enlarging the identity attack surface.

Some metrics:

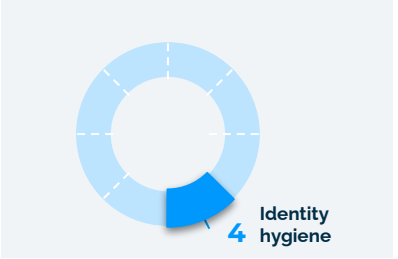
Reporting on access accumulation often boils down to finding and reporting on outliers.

- Peer outliers: accounts that have more access rights (i.e. are assigned more roles or have more permissions) than their peers.
- Accounts that deviate from the ideal profile. Depending on the job function a certain employee has, a certain set of roles might be appropriate. How effective this is depends on the correctness of the ideal profiles (i.e. the role model blueprint)
- Accounts that have more than twice the amount of roles or entitlements than average accounts.

Your own indicator definitions

In general, the exact definition of an indicator is often quite business-specific. It depends upon the type of transactions you have to perform, the systems you use, the role model you apply, etcetera. Involving the right stakeholders is often crucial to get the indicators right.

4. Identity hygiene



What: Identity clutter. Accounts that are not orphaned, but are just as unnecessary and make identity management less manageable.

Why: Security | Operational efficiency

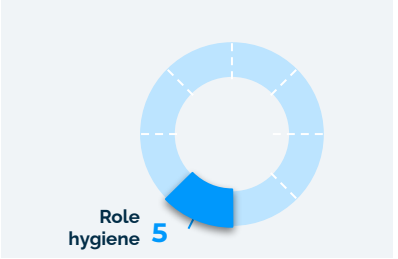
Details:

A well-maintained IT environment is better protected against information security risks. Applying good practice to users not only helps to prevent risks, but it also contributes to operational efficiency as it leads to a more structured environment and needs considerably less effort compared to a situation where you periodically have to clean up the mess. In other words: prevention is better than the cure.

Some metrics:

- The number of accounts compared to the number of employees.
- Accounts that have no roles or entitlements assigned, also known as *empty accounts*.
- Accounts that have no access to any applications.
- Accounts that have not been changed for a certain period of time. What that time period should be exactly can vary for different types of accounts and between organizations.
- Accounts for testing purposes (i.e. *test accounts*).
- Duplicate accounts.
- Shared accounts.

5. Role hygiene



What: Role clutter. Roles that are no longer necessary and only make role management more cumbersome.

Why: Security | Operational efficiency

Details:

Using roles to control access can greatly increase efficiency. However, if the role model is no longer manageable because of role proliferation for example, operational efficiency declines. Moreover, people might be assigned an outdated or wrong role and thus wrong access rights.

Rule of thumb

The total number of roles should be no more than 10% of the total number of accounts. In many organizations without proper role management this percentage is greatly exceeded. This represents an overly complex role model.

Some metrics:

- The number of roles relative to the number of accounts.
- Roles that do not consist of other roles or entitlements, also known as *empty roles*.
- Roles that are not assigned to any account, also known as *unassigned roles*.
- Roles that are assigned to only one account.
- Entitlements that are (not) assigned via a role. In other words, *directly assigned entitlements*.
- Similarity scores, or also called group homogeneity. This indicator measures for a group of people that are assigned the same role, how similar they are in terms of their access patterns.
- Overlapping roles: roles for which the users that have those roles are similar in terms of their characteristics (e.g. job function), or roles for which the access rights are similar.

6. Data quality

What: Poor data quality issues based on factors such as accuracy, completeness, consistency and reliability.

Why: Security | Risk | Operational efficiency

Details:

Garbage in is garbage out. Simple as that. In order to get accurate results - for any of the indicators or your governance processes -, data quality is crucial. The indicators will only reflect the actual state if the identity data is accurate and complete. Basing your decisions on incorrect indicators can have negative consequences.

Moreover, in some organizations many of the processes, such as joiner-mover-leaver processes, are automated with the help of governance systems. If they rely on wrong data, the outcome will be wrong, often leading to unnecessary security risks.

Some metrics:

The most easy to measure is incomplete information.

- Employees 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.

Inconsistencies across multiple applications such as employees with different account names (often typos), and inaccuracies such as employees that have changed functions while this is not indicated by the data yet, are harder to spot and measure. Nevertheless, when reporting to for example management make sure to mention this as well so it can be included when focus areas are discussed.

7. Separation of Duties (SoD)

What: Accounts that violate SoD rules and SoD policy coverage.

Why: Security | Risk | Compliance

Details:

Separation of duties is a crucial control for avoiding fraud by disseminating sensitive tasks and the required roles, entitlements or permissions. These combinations of permissions are often modelled as "toxic combinations". In addition to fraud, SoD is also implemented for security reasons or for sake of regulation.

Some metrics:

- Accounts with toxic pairs of roles or entitlements within a certain application.
- Accounts with toxic pairs of roles or entitlements across applications.
- Employees with toxic pairs of roles or entitlements across accounts and applications.
- Combinations of roles or entitlements for which no decision has yet been made about whether it's a toxic combination or not.

8. Business-specific indicators

What: Specific internal policies.

Why: Security | Operational efficiency | Risk | Compliance

Details:

To measure whether the internal policies are complied with.

Present the big picture or the details?

Not everyone prefers or needs the same level of detail. If you're convincing management that you are in control of the users and their access, a high-level status update will typically work best. This often translates to reporting at the level of the eight categories of indicators and only diving into more detail whenever the situation requires it. For example, when you're working on cleaning up orphaned accounts and want to demonstrate the progress.

Some metrics:

As a final category, many companies have business-specific security policies or risk controls that have to be monitored.

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 indicator.

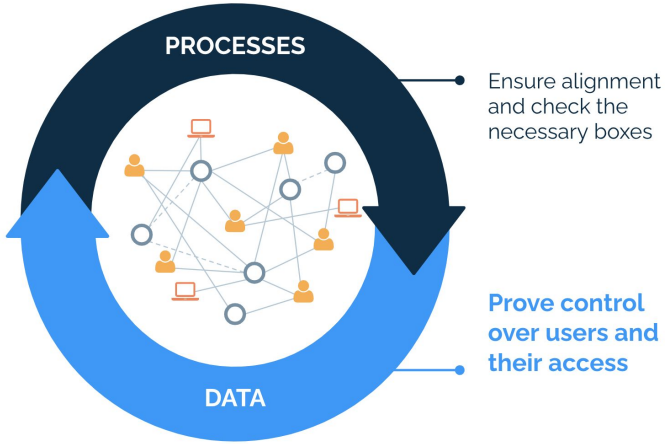
Another frequently seen situation is when companies focus on security awareness training and want to measure for whom such training has been too long ago, especially if these users have a lot of privileges. Also, in case the organization enforces a password expiration policy they can measure accounts with expired passwords.

CONCLUSION

Having control over who can access which data in such an environment is crucial for privacy, compliance and protecting against cyber threats. Many companies have human governance processes, but those don't necessarily lead to actually being in control of the users and their access.

How do you know if you're in control? And how can you prove that? By measuring key indicators and understanding your current status. Because knowing is owning.

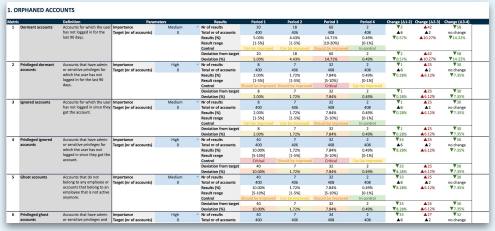
This guide bundled a set of 8 crucial indicators that help you to measure whether you are in control and to prove that you are.



Next steps: prove that you're in control

Eager to get started yourself? We created a canvas to help you prove that you're in control of your users and their access.

Download the canvas



Or want to read more on this topic? We made a guide about applying a KPI-driven approach to identity management.

Read the guide

Did this guide help you? Do you want to discuss this?

Get in touch!

Chiel Haesendonck
chiel@elimity.com

ELIMITY