ELIMITY

MICROSOFT ACTIVE DIRECTORY
IDENTITY CONTROLS GUIDE

TABLE OF CONTENTS

CONVENTIONS

Additional information and insights

Tips & tricks

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

Some clarifications before you continue reading this ebook:

- The words 'user' and 'user account' are used interchangeably throughout the text.
- 'Access rights' should be understood as a collection of specific accesses and permissions that user accounts are entitled with because they are assigned to one or more AD groups.

INTRODUCTION

In a business and IT context, there's only one constant: change. Think of hybrid IT landscapes that keep on evolving, tens or even hundreds of systems and applications that need updates on a regular base, a growing number of temporary contractors such as freelancers and consultants, etc. Considering this pace of change, maintaining an overview of the situation has become more challenging than ever. But if you can't see all the users across your IT environment and if you don't know what applications and data each of those users can access, it is close to impossible to control risks and prevent threats. Understanding the relationships between people, access and data is a crucial factor in this regard. In other words: getting to know the unknowns.

In this guide, we bundled the identity controls that apply to Active Directory. Moreover, this set of controls has proven to be applicable to the majority of the organisations. In the ebook 'How to build the perfect risk cockpit for Microsoft Active Directory' we discussed the six steps to set up comprehensive and scalable risk cockpit. In this guide, we'll elaborate on the eight building blocks of such a cockpit. Implementing these controls will help you to uncover all the unknowns. Because you can't protect what can't see.

This guide is written for IAM, IT and security professionals. The contents are not limited to any organizational size, structure or industry. The premise is, however, that the organization uses Active Directory. Nevertheless, most of the controls also apply to other applications albeit with some adjustments.

CONTROL SETS

You can improve the overall security health of your Active Directory by identifying, analyzing and responding to risks and potential threats. On the following pages, we provide you a comprehensive collection of controls, which has proven to be useful for the majority of organizations. Each of those control sets includes several specific security controls. You can extend or limit this set of controls according to the security standards you want to comply with and to the business-specific context you are working in.

The ISO 27001 based identity wheel (see on the right) shows eight control sets that are applicable for the majority of modern organizations. On the following pages, these control sets are explained in more detail.

Roadmap for a risk cockpit

Based on our experience, we have designed a six steps framework to build a comprehensive risk cockpit for Active Directory.

Download AD risk cockpit guide

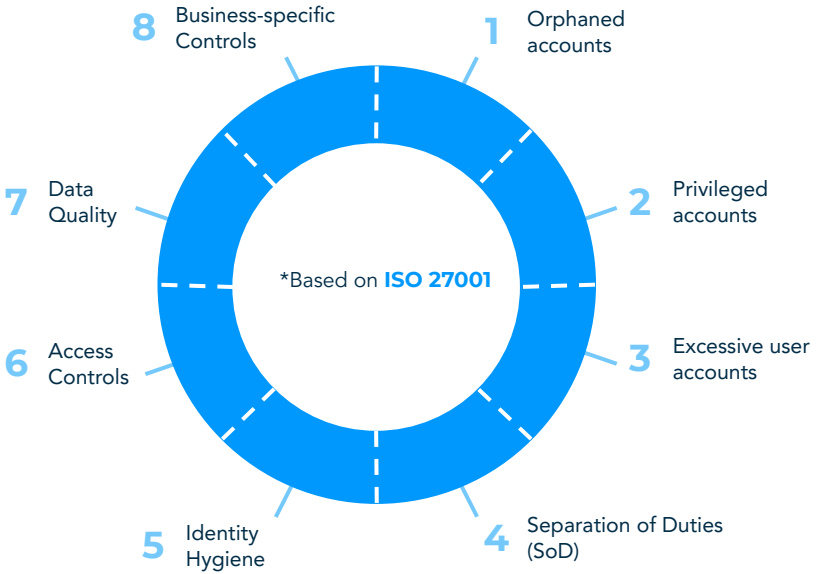


FIGURE: IDENTITY WHEEL

1. Orphaned accounts

Would you ever leave for a vacation and leave your front door unlocked? Or lock it but leave the keys scattered around the yard? Of course you wouldn't. Still, this is equivalent to what organizations do when they leave orphaned accounts hanging around. Much like robbers, hackers or disgruntled (ex)-employees look for the easiest and quietest way in. One such path is through user and service accounts that are no longer actively used. From a hacker's perspective, it's relatively easy to find these accounts: a quick search on LinkedIn could reveal who's recently left the company. This applies to both employees leaving and external contractors who finished a project in your organization. Organizations that fail to take the necessary steps to close these entry points leave the door on a jar for attackers. This way, hackers could compromise an account with access to security systems or access to sensitive information like intellectual property (IP), personally identifiable information (PII) or financial documentation.

When an employee leaves the organization or when a contractor's project has ended, their user accounts must be deactivated without further delay. This should be part of the typical offboarding procedure of both employees and contractors.

However, in practice, those user accounts are often not correctly deactivated, or even not deactivated at all. Within AD there are two ways to detect those accounts:

- Spot user accounts - e.g. by using a search function - that have not been used for a certain period of time (also known as dormant accounts). In other words, users that have not logged in for some time. 90 days is often considered the limit but depending on your business context and the appeal your organization has on hackers, that period can be shortened or extended.

- In AD, user accounts can be given an expiration date when they are created. However, those accounts are not automatically disabled on the expiration date. As a result, these accounts are often forgotten, but can still be misused for malicious practices. It is therefore strongly recommended to make a list of all expired accounts. Likewise, a list should be made with all accounts that are about to expire in the coming weeks or months. Next, review the lists to decide which of the accounts must be extended or disabled. It's also possible to create a user account in AD without an expiration date, but it's advisable to do so as little as possible and evaluate those accounts regularly.

The best practice to get rid of orphaned accounts – disabling or deleting – can vary between companies. In many organizations, disabling the accounts is the standard. That is because this method leaves all the traces around the account intact, which can be very useful for audits.

2. 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. Below you find some examples of privileged accounts that you must definitely consider in your evaluation.

YOU CAN'T PROTECT WHAT YOU CAN'T SEE

Typically, **administrator accounts** are considered privileged accounts. This is especially true for Domain Admin Accounts, as they have full access control over the AD Domain.

Stealthy accounts are another privileged account type that should not be overlooked. Accounts like that often have sensitive privileges and tend to exist below the radar because they are not a member of a default privileged (or critical) AD group.

Yet another example are **privileged service accounts**, such as Domain Service Accounts. In most cases, service accounts are not tied to a unique user identity, which means there may not be a natural person who is held accountable for their management.

However, **privileged data user accounts** are probably the most dangerous type of all privileged accounts in an organization. Why, you might think. Simply because they are the least noticeable. Granted, such accounts are not typical privileged accounts, but 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. Companies must know where their sensitive data resides and who can access that.

Interested in more in-depth examples showing the importance to know who can access what? Read our blog.

Depending on the group settings you made in AD, certain group types can be considered privileged. Therefore, we should consider user accounts assigned to one or more of these groups as privileged accounts. The key to minimize security risks and prevent improper use of privileged access rights is identifying all privileged accounts in your organization and proactively monitoring them. It's impossible to eliminate every risk factor. You need admin users for business-critical purposes even though they are high-risk users. In many situations it's about uncovering these privileged accounts and monitoring them closely. However, in some situations action can and should be taken to remediate unused or incorrect privileged accounts. In that situation, you must set the right priorities to tackle the incorrect privileged accounts you discovered. For example, it's appropriate to give the highest priority to accounts that are both privileged and orphaned.

3. User accounts with excessive access rights

One of the most important principles in information security is the principle of least privilege.

THE PRINCIPLE OF LEAST PRIVILEGE

The principle of least privilege (POLP) is the practice of limiting access rights for users to the bare minimum they need to perform their intended work. For instance, an internal auditor should only be able to read data and not modify it. Hence, he should only be given read permissions and not read and write permissions. The write permissions can be misused by him or a malicious outsider that gains access to his account.

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.

Many user accounts with excessive access rights arise because of position changes. When employees change positions, it often happens that the former permissions and memberships of groups that are no longer necessary are not revoked. It's recommendable to track these users and take action to minimize their access rights to only those that they really need to perform their jobs.

Also misconfigurations, such as a 'select all' command whereby accidentally privileged access rights are granted to everyone within a certain department, can lead to user accounts with excessive access rights. But how do you detect such user accounts?

- Outlier detection: identify users that have more access rights (i.e. belong to more groups or have more permissions) than their peers. Often this is the result of employees changing departments or functions without the former - and now unnecessary - access rights were deprovisioned.

- Identify users with more rights than they should have. In many organizations a person with a certain role or function will be part of specific groups. User accounts having the same role or function but that are members of more groups need your attention.

- Identify users that are assigned to an overly high number of groups. Often this is the result of a misconfiguration.

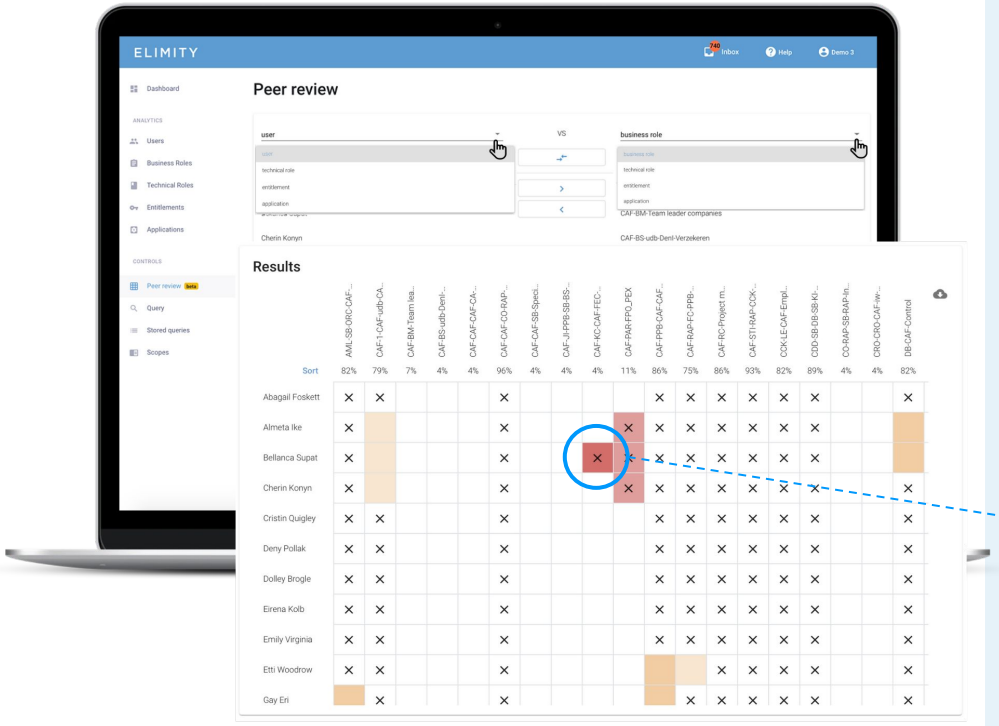


FIGURE: ELIMITY INSIGHTS
Screenshot of peer review interface

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. belong to the same groups). 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/belongs to a certain group while the others do not.

Try for free

4. Separation of Duties (SoD)

Separation of duties, also known as segregation of duties, is considered as one of the most difficult and often costly 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 or a person that can both pay and approve invoices. Nevertheless, understanding (in theory) and putting it into practice is something completely different.

Implementing a proper SoD control set starts with defining 'toxic' combinations of groups, and therefore access rights. In case users are found who have access rights combinations that are considered toxic, this should be mitigated or remediated.

REMEDIATION OR MITIGATION?

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

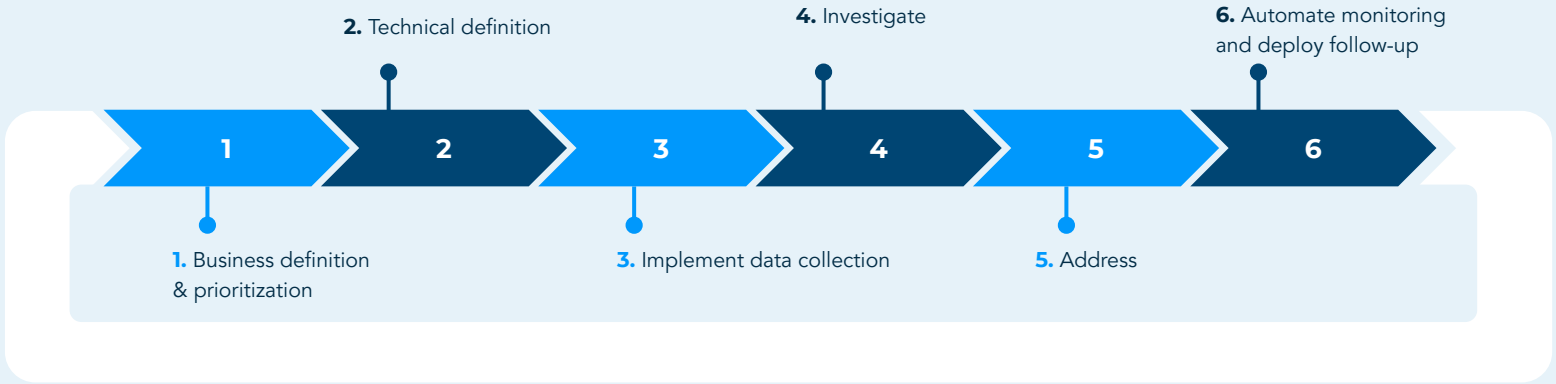
- Tactical clean-up: revoke a group, delete the user account, …
- Strategic redesign: redesign certain groups or processes

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.

Note that it is recommended to evaluate whether the toxic combinations are still up to date and aligned with the business needs.

Manually controlling for SoD violations 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



If you need more information about designing and implementing SoD controls efficiently, don't hesitate to reach out to us.

5. Identity hygiene

There is an interesting parallel between personal hygiene and identity hygiene: people take care of their personal hygiene to maintain good health and well-being, while organizations (should) engage in good identity hygiene to maintain a good overall security posture. In this context, it is important to realize that identity hygiene and information security are strongly interconnected: a well-maintained IT environment is better protected against information security risks. Applying good practice to users and groups 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.

It is therefore advisable to opt for ongoing proactive maintenance of your critical systems and data. These are some appropriate tips & tricks to do so for AD:

- Look for empty groups (groups that are not assigned to any user) and check if you can remove them. The thing is that empty groups that give access to critical applications or sensitive information can be abused by malicious actors. Retain only those groups in your AD that are actively being used and that still align with the business needs of the organization.
- The same as in the previous bullet also applies to groups that are assigned to one user only. Even if there is a good reason for this, it is still worth to monitor these groups closely so that immediate action can be taken if something changes (for example, if that user no longer uses the group).
- Evaluate large groups to which all or almost all users are assigned to. A typical example are groups such as 'Domain users' or 'Everyone'. Check whether these groups provide nothing more but the necessary rights that everyone needs to perform their jobs.
- Evaluate highly overlapping groups. In many cases, similar groups (i.e. with almost the same users) often indicate changes made throughout time. Possibly, some (or all) of these groups can be combined in a new group which is then the only one that is actually aligned with the current business needs. The other groups should then be deleted.
- Evaluate user accounts which are not assigned to any group. This could indicate a misconfiguration or a user which only has direct permissions.

- Evaluate groups and user accounts that have not been changed for the last e.g. 12 months. Also see Orphaned accounts.

- Monitor accounts that are locked, recently disabled, created or enabled to detect potential threats. In general, maintain an overview of potential alarming changes. These changes can then be evaluated so action can be taken if necessary. For example if an account is locked the reason behind it should be discovered to decide on the appropriate action.

RULE OF THUMB

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

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

6. Access controls

Logon activity

Shield your Active Directory by detecting suspicious logon activity, so action can be taken before a security breach hits your organization:

- Identify accounts with a large number of failed login attempts. This could indicate a hacker trying to get in using a brute force attack.

- Identify accounts with a large ratio of logons relative to the activity duration, as this could indicate hacker activity as well.

- Identify users that have never logged on since their account was provisioned. This lack of activity is probably caused by a misconfiguration. Still, if that account provides access to sensitive data or critical systems, it can easily be abused by malicious outsiders or insiders.

Password policy

Password policy best practices are often debated. We will, however, not elaborate on those in this ebook. Nevertheless, if your company enforces a password expiration policy, all accounts for which the password has not been changed in the last 90 days, for example, should be identified so those users can be notified.

7. Data quality

In order to get accurate results from all of the controls mentioned above, it's crucial that all data ('attribute values') are entered correctly in AD.

In every organization, a formal process must be in place whereby HR (or another department) passes on information about changes to the one(s) responsible for entering the right information in AD – either manually or automatically –, every time an employee joins or leaves the organization, or when the employee changes positions (moving to another department and/or getting promoted) within the organization. Practice, however, does not always match theory.

The information in this document will only lead to trustworthy insights on the condition that the data in your AD is accurate, complete and up to date. Besides ensuring reliable insights, proper data quality is also important to ensure that the insights can be acted upon. Suppose, for example, that the orphaned accounts really need to be cleaned up. In that situation it's important that you have enough information about those user accounts to decide whether those accounts can be disabled or not. Preferably you have that information without having to ask other people as this often results in frustration and long lead times.

GARBAGE IN IS GARBAGE OUT

In order to prevent certain AD fields from being left blank (for too long) because the necessary information is not available, it is advisable to immediately link each user account to a responsible manager, who should be the first point of contact for missing information about his team members.

8. Business-specific controls

As mentioned in the beginning of this chapter, you can enhance these control sets with business-specific policies. In financial institutions, for example, it's often the case that an employee needs the proper certification to perform a certain action. Hence, checking whether everyone who has the permissions to execute that action also has the proper certification could be such a business-specific control. Another frequently seen situation is when companies focus on security awareness training and want to check for whom such training has been too long.

ELIMITY INSIGHTS: ADVANCED IDENTITY INTELLIGENCE

Gain 360-degree insights with the most powerful identity analytics engine ever built and easily automate the controls mentioned in this guide. Think of privileged and overly privileged users, unassigned users, toxic combinations of groups, 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) identity control.

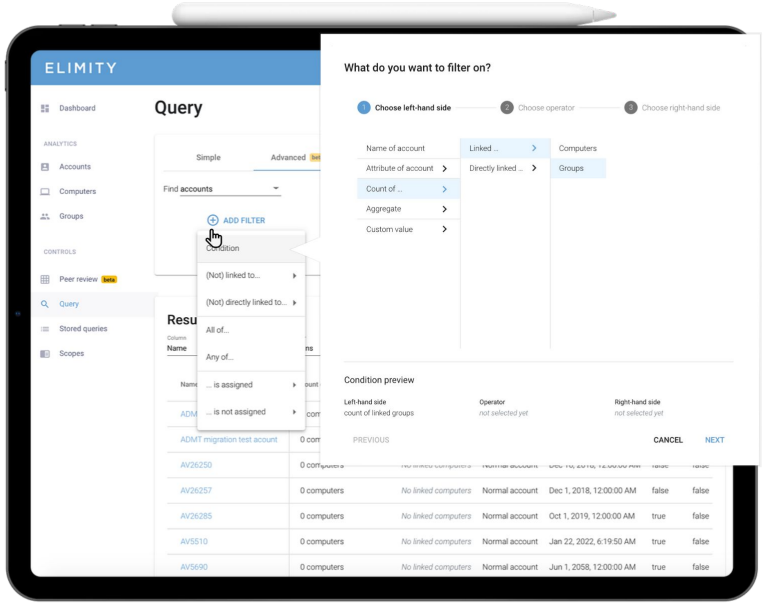


FIGURE: ELIMITY INSIGHTS
Screenshot of creating an identity control

CONCLUSION
MAIN TAKEAWAYS

You can now build a clear and comprehensive risk cockpit that helps you to understand the relationships between users, access and data in your AD environment.

This way, you can:

- Gather trustworthy insights on current AD security state
- Monitor the risk situation with minimal effort, today and in the future
- Make clear and detailed reports for all relevant stakeholders

EPILOGUE
WHERE TO GET THE RIGHT TOOLS?

It's one thing to have the right knowledge, but of course you also need the right tools to make things work in practice.

For this purpose, Elimity designed 'Insights', a very powerful yet easy to use SaaS solution which allows for an automated and continuous assessment of Active Directory.

ELIMITY INSIGHTS FOR ACTIVE DIRECTORY

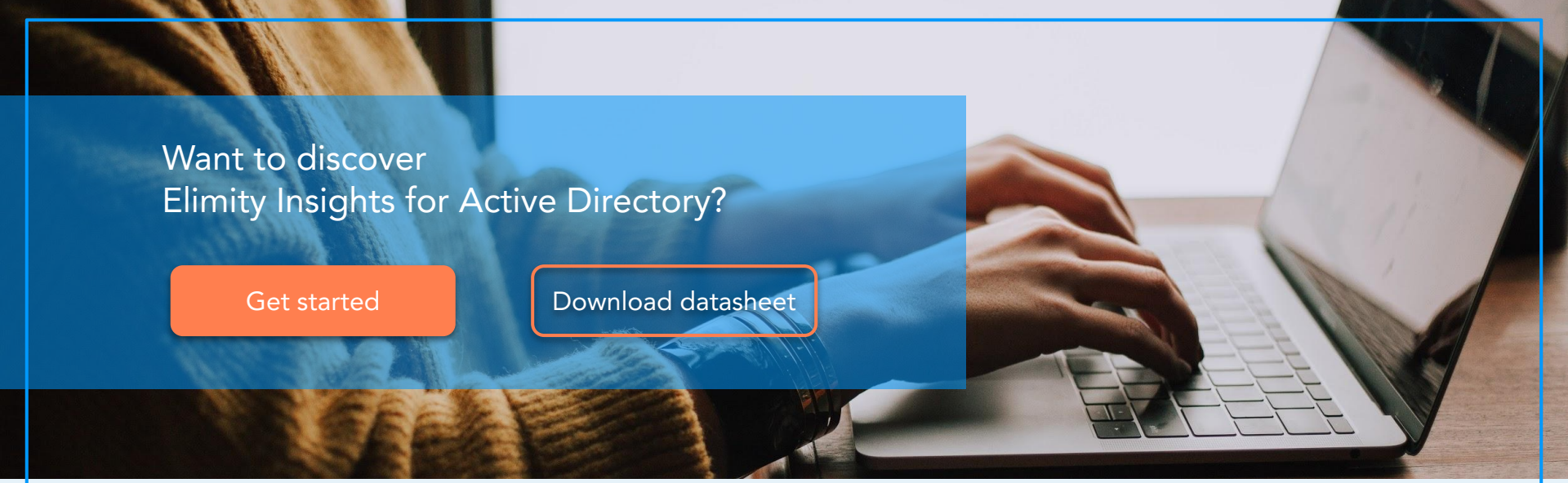
FIGURE: ELIMITY INSIGHTS
Screenshot of dashboard customization / risk cockpit

Risk cockpit

The personalizable risk cockpit gives you an overview of the security state of your Active Directory at a glance. It enables you and your team to identify access risks, prioritize efforts, discover trends over time and easily follow up on the most important AD controls for your organization.

Elimity Insights for Active Directory comes with a predefined set of identity controls. Perfect to assess the security state of your AD environment in no time.

Try for free



Want to discover Elimity Insights for Active Directory?

Get started

Download datasheet

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

NELE S'HEEREN
Solution Architect
nele@elimity.com

GILLES VANCANNEYT
Solution Engineer
gilles@elimity.com

ELIMITY