ELIMITY

HOW TO BUILD THE PERFECT RISK COCKPIT FOR MICROSOFT ACTIVE DIRECTORY

Eight essential building blocks of a solid AD risk cockpit

TABLE OF CONTENTS

CONVENTIONS

💡 Additional information and insights

💻 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.

Strong identity analytics and clear reporting are two essential building blocks that help you deal with these challenges. Unfortunately, this is easier said than done.

In many companies, these two building blocks are often improperly used, or even non-existent. When done right however, they will keep your company secure and empower your IT team.

This is why we created this document: to help you getting started by handing you crucial insights in identity analytics, as well as best practices to make clear and useful reports. In this document, you’ll find a clear roadmap to navigate through the right steps to set up a comprehensive, clear and scalable risk cockpit.

WHY DO YOU NEED A RISK COCKPIT IN THE FIRST PLACE?

1. Get back in the driver's seat

Employees use more and more applications, of which a growing number is cloud-based. Besides, hybrid environments are becoming the new standard. Maintaining an overview of who can access which application therefore becomes increasingly difficult. And increasingly important as well. Think of security breaches, compromised data, all of the regulations your organization needs to comply with, … Using a well-designed risk cockpit, you can easily assess and audit access to your critical applications, gain actionable insights, and control the users and their access rights.

2. Empower your IT team

In many organizations information security audits and other identity controls are still based on the use of spreadsheets. However, this method is very time-consuming and cumbersome, and often leads to inaccurate results, and therefore in wrong decisions. Moreover, the relations between people, access and data are often hard to spot in non-dedicated identity tools such as Excel.

In addition, in many cases IT teams are overwhelmed with all kinds of business requests and security tasks. Increasing efficiency by using dedicated identity tools that are able to automate repetitive and highly manual tasks, can greatly reduce this IT friction.

3. Gain access control

Today, many employees don't simply climb the ladder within a single department. Instead, they regularly switch across departments and functions. If you sit back and relax, access rights and permissions will inevitably pile up and users will end up with excessive access rights they no longer need to do their job. These excessive access rights pose a risk to the organization as they can be misused or compromised.

In summary, a comprehensive risk cockpit allows your IT team to easily detect and reduce risks. Moreover, passing your next internal or external audit will happen much smoother and faster.

BUILDING A RISK COCKPIT BASED ON THE NIST FRAMEWORK

The NIST CSF is not the only 'framework' implying that the implementation of IT security will be - slightly - different for each company (see additional info on the right). Think for example about the standard ISO 27001 that also leaves room for interpretation and meaning of processes and controls. This is reflected in the step by step approach shown on the next page. Following these six steps will enable you to set up an identity & access risk cockpit that is aligned with the IT and business strategy of your organisation. This approach can be used to design a comprehensive risk cockpit for any important application or system in your organization. Ideally, you even have a single risk cockpit that gives you complete visibility into all users and their access rights across all important applications in your organization. In this ebook, however, we will focus on building a risk cockpit for Microsoft Active Directory.

NIST CSF

The NIST Cybersecurity Framework (CSF) is developed by the National Institute of Standards and Technology (part of the U.S. Department of Commerce) in order to help companies identify, assess and manage cyber risks. However, this Framework is not a one-size-fits-all approach that can be copied word for word and applied to each company. That is because organizations often face unique cyber and information security risks. The trick is to identify the relevant pieces, customizing them to your business needs and implementing them within your organization.

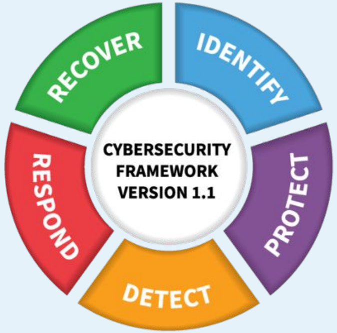
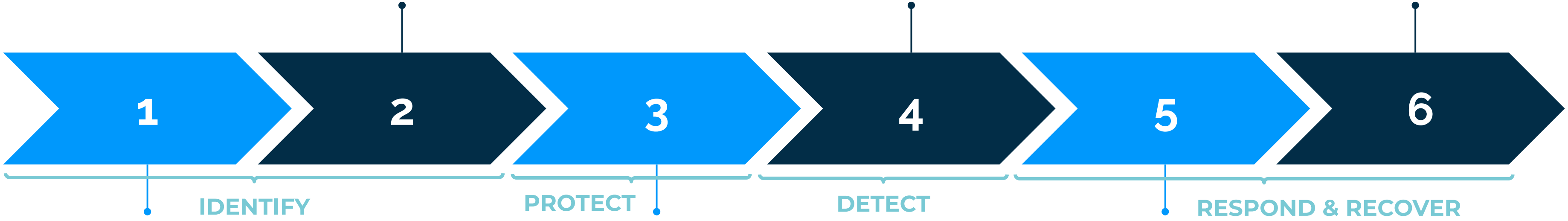


FIGURE: NIST Cybersecurity Framework version 1.1

Source: https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

Step by step guide to set up the ideal risk cockpit

based on the **NIST FRAMEWORK**



IDENTIFY THREATS & REGULATIONS

What regulations must your company comply with and which threats could jeopardize the security of business critical data?

REFLECT ON CRITICAL OBJECTS

What are the most critical - and therefore vulnerable - AD objects in your organization?

DETERMINE CONTROL SETS

Which security control sets do you need in your risk cockpit?

ANALYZE

What is the current AD risk posture?

FOCUS & TRANSFORMATION

Where should you start, and which issues should you tackle first?

FOLLOW-UP

Monitor the situation, follow-up over time and respond proactively.

WHY FOCUS ON ACTIVE DIRECTORY?

First of all, Active Directory (AD) is an indispensable system for the vast majority of organisations around the world to authenticate and authorize users and computers in a domain network. AD is deployed in 90% of all businesses [1] and within those businesses around 80% of the applications rely on AD data [2]. As Active Directory is often strongly intertwined with a number of critical applications it is crucial to ensure that is securely managed.

Next to this reasoning, applying the principles of the CIA triad also results in the conclusion that Active Directory is one of the fundamental building blocks to create such a unified risk cockpit. Read more about that in the next section.

The CIA Triad

In information security environments, the CIA triad (see figure next page) is a well-known and commonly used framework which helps to determine the value of applications for your business based on three main properties: confidentiality, integrity and availability.

1. **Confidentiality** is about protecting information from unauthorized access.
   "What if someone would obtain unauthorized access to the information contained within that application?"

2. **Integrity** is about keeping information accurate and consistent.
   "What if the integrity of the data would be compromised? What if incorrect changes are made by unauthorized people?"

3. **Availability** is about ensuring the information is available when needed.
   "What if the application (and thus the information contained within) would no longer be available?"

[1] https://www.darkreading.com/active-directory-mismanagement-exposes-90--of-businesses-to-breaches/d/d-id/1328101

[2] https://www.quest.com/community/blogs/b/en/posts/active-directory-is-the-backbone-of-your-organization

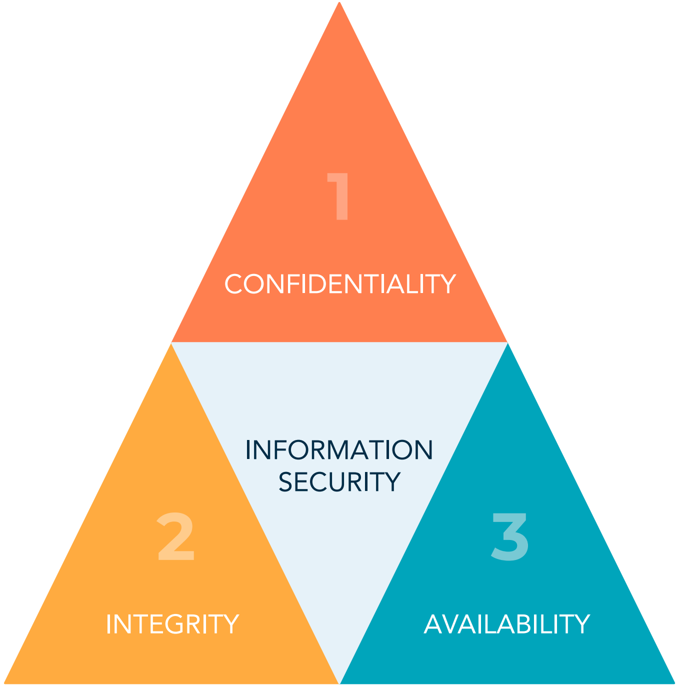


FIGURE: CIA TRIAD

It is fair to say that AD does not only hold the keys to the IT environment but is also the lifeblood for your users, apps and files. Without it, nothing else really works, and employees would not be able to access the data and applications they require to do their jobs. This could have serious consequences. For example, if doctors or other medical personnel cannot access the data and the applications they need to review patient records, or if that information is inaccurate or compromised, both the patients and the organization would be severely affected. Or imagine what would happen if employee data or financial data is unavailable or inaccurate. It’s pretty clear that, based on the CIA triad, securing your Active Directory must be a top priority.

Target for cyber criminals

Not convinced yet? Historically, physical and network infrastructure got most of the security attention while AD security has been lagging behind. Today however, cyber criminals are increasingly targeting Active Directory to look for users, servers and computers in a company network. Once they have that information (e.g. access credentials), they set up attacks to gain access and abuse organization data (e.g. encrypt business critical data) and resources.

In the next sections we will walk you through the different steps to create a comprehensive risk cockpit to audit your Active Directory. The goal is to enable you to analyze and report on the AD data, in order to improve overall security.

STEP 1: IDENTIFY THREATS AND REGULATIONS

"What regulations must your company comply with and which threats could jeopardize the security of business critical data?"

Regulations concerning information security are primarily developed to protect employees and customers against the misuse of their personal (and sensitive) data, such as GDPR and CCPA. In doing so, those regulations force companies to take certain measures to protect themselves and to protect the data they keep from potential threats. The threats that could jeopardize the security of your sensitive and business critical data play an important role in this.

For many organizations, striving for compliance with relevant regulations is an important driver to implement or improve their security processes and controls. While this is of course a valid and very useful reason, there are companies out there that also use these regulations as the basis for their security program because they consider this good business management. In fact, more and more stakeholders attach importance to organizations using the data entrusted to them in a sensible and responsible matter.

Understanding the business and regulatory context you are operating in allows you to align your risk management strategy with your business needs and set the right priorities. Moreover, this is a prerequisite to design and build an appropriate risk cockpit. Note that, next to the purely objective aspects (such as regulations imposed by a governmental body), it's also about the issues that you and your team are concerned about. What's in your head all day and what keeps you awake at night?

Fact is that the success of your security efforts greatly depends on your ability to focus energy where it really matters.

STEP 2: REFLECT ON CRITICAL OBJECTS

"What are the most critical - and therefore vulnerable - AD objects in your organization?"

Before setting up the relevant control sets, it's important to know which groups, and therefore which user accounts[3], are critical for the mission and security of your organization. Nowadays it's common practice to use standard rules to give you an indication of these groups. Those rules are often based on the use of AD default security groups, such as Administrators, Domain Admins and Enterprise Admins. However, those groups do not take your business context into account, nor your organizational and AD structure (e.g. custom groups). Nevertheless, those standard rules are a good starting point.

Once these 'default critical' groups are identified, you should evaluate whether they are actually critical and actively used in your organisation. Additionally, identify custom groups (if you have any) and check - keeping the business and regulatory context in mind - which groups are critical or riskier than others.

In the section about privileged accounts you can find some elements you should definitely look into.

In order to properly execute this step, gaining full visibility and understanding across all groups and other AD objects is essential. If you don't know how to get started, don't hesitate to contact us and get some more detailed instructions.

[3] We assume that a user account that belongs to a critical group (e.g. with access to critical applications or systems, or sensitive data such as IP) can be considered a critical - or privileged - user account.

STEP 3: DETERMINE CONTROL SETS

"Which security control sets do you need in your risk cockpit?"

You can improve the overall security health of your AD by identifying, analyzing and responding to risks and potential threats.

The ISO 27001 based identity wheel (see figure on the right) shows eight control sets that are applicable for the majority of modern organizations. Each of these control sets ideally entails several specific controls. Within 'orphaned accounts', identifying users that have not logged in for some time is such a specific control.

In our AD controls guide we bundled a comprehensive collection of controls within each control set, which has proven to be useful for the majority of organizations.

Download AD controls guide

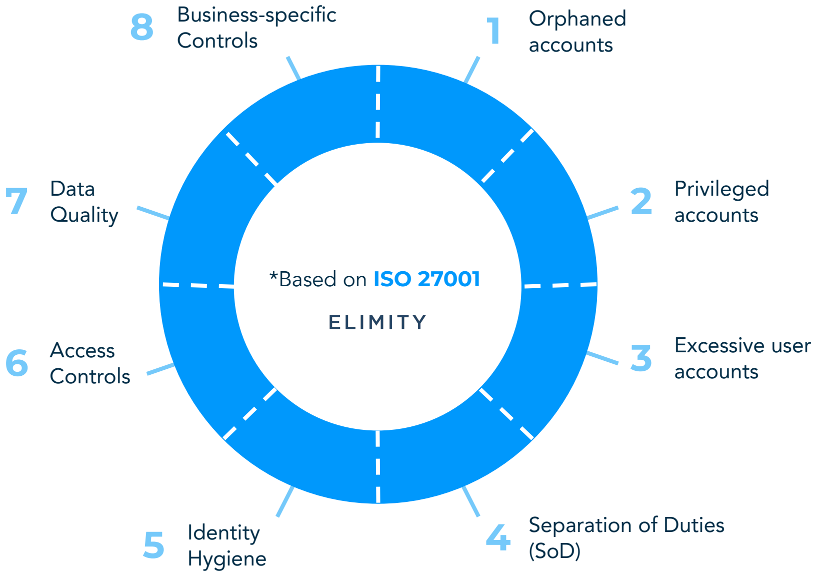


FIGURE: IDENTITY WHEEL

STEP 4: ANALYZE

“What is the current AD risk posture?”

Before you start analyzing the security control sets we discussed before, it’s recommended to look at the current identity repository size to know what’s out there. Some metrics to look at:

- The number of user accounts
- The number of groups
- The number of computers
- The number of managers

Once you have a general overview of the size of your AD, you can start with analyzing the security controls. As said in the introduction, it’s about getting to know the unknowns. Find out how many orphaned accounts there are, which accounts are privileged, ... Once you’ve done that, assess the results of the security controls by indicating the corresponding risk level (see on the next page). This will help you to prioritize your efforts in the next step.

Note that specific user accounts or groups within a control can be riskier than others. Take for example the orphaned accounts control set. If it turns out that both an admin user account and a non-admin user account have been inactive for some time, the orphaned admin user account entails the most risks. This is because it allows hackers to abuse more organization resources and data if they get in.

Once you have determined the right risk levels for each security control it’s important to document the main findings, so you can use them to support decision-making in the next step.

RISK ANALYSIS

It is not obvious to define the right priorities and risk levels. Several frameworks are available that can guide you through this process. A frequently used approach (see Risk Matrix below) uses both likelihood and impact.

First you have to reflect on how likely it is that hackers or malicious insiders will misuse a specific weakness. Next, you should check how big the impact would be. Both questions should be scaled (see the axes on the Risk Matrix), and the resulting risk level can be found as the product of both likelihood and impact.

IMPACT

LIKELIHOOD	NEGLIGIBLE	MINOR	MODERATE	SIGNIFICANT	SEVERE
VERY LIKELY	Low	Medium	High	Critical	Critical
LIKELY	Low	Medium	Medium	High	Critical
POSSIBLE	Low	Low	Medium	High	High
UNLIKELY	Low	Low	Medium	Medium	High
VERY UNLIKELY	Low	Low	Low	Medium	Medium

FIGURE: RISK MATRIX

STEP 5: FOCUS & TRANSFORMATION

"Where should you start, and which issues should you tackle first?"

Based on the results and the indicated risk levels that were determined in the previous steps, you can now set up a roadmap (that contains several control projects) to secure your AD environment and gain more control.

It is of course recommended to include control projects that contain pressing issues early in the roadmap. In the figure on the right you can see how effort and risk reduction are often interrelated, and how a control project fits in.

Once the roadmap is started and you're gaining control over your AD environment, you should track progress, so you can measure anytime whether you're still on track. This allows you to report on the current situation to your manager and other stakeholders. Note that you need actionable insights for each project (however small it is), so you know who to address. For example: which manager needs to review whether a certain empty group may or may not be removed.

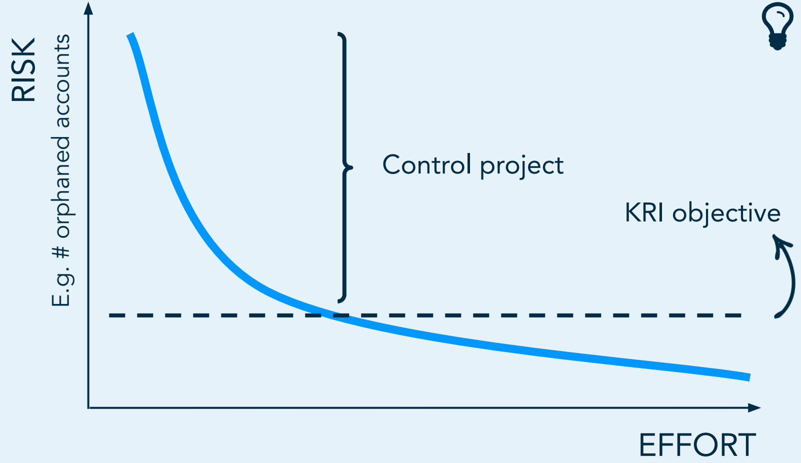


FIGURE: RISK REDUCTION vs EFFORT
The shape of the graph depends on the type of control and the risk distribution within a control.

An AD control project can often be seen as a clean up project whereby incorrect access rights or inactive user accounts are remediated or mitigated. A certain control project can be considered finished when the KRI objective has been achieved.

STEP 6: FOLLOW-UP

“Monitor the situation, follow-up over time and respond proactively.”

It’s not because a control set is under control now, that it will remain so in the future, especially if no further action is taken. People join and leave the company and move across departments all the time. Furthermore, companies might go through mergers, acquisitions, etc.

This means that you have to keep on monitoring these controls and react promptly when any relevant changes occur. This way, you can better manage information security risks and prevent threats.

Moreover, the regulatory landscape is continuously changing. Keep your eyes open for changes, so you can anticipate and take proactive actions right away such as including an additional 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 in no time

EPILOGUE

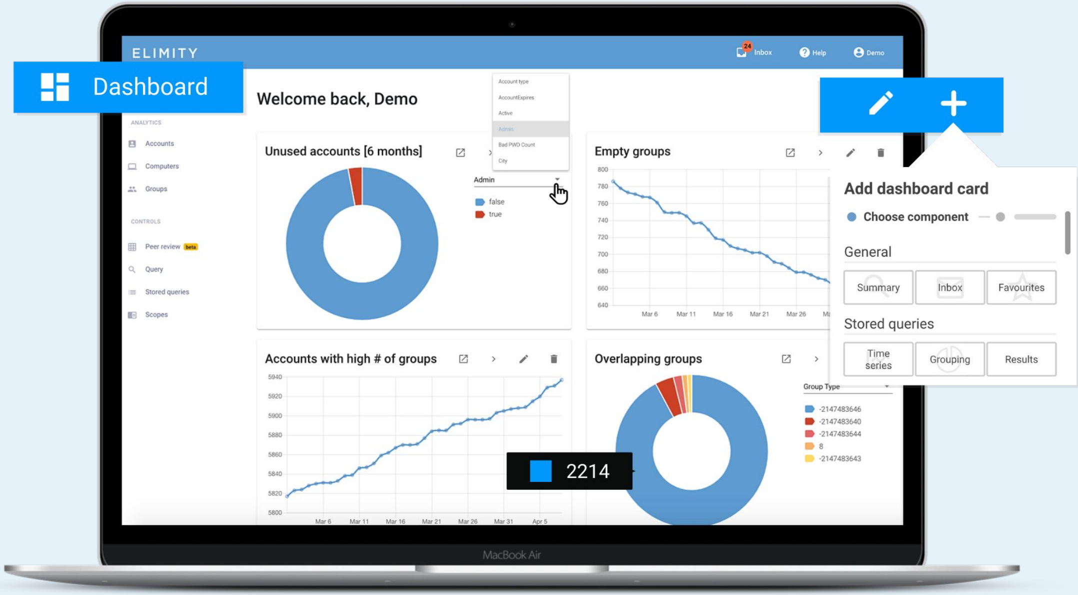
WHERE TO GET THE RIGHT TOOLS?

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.

Curious? View the next page.

ELIMITY INSIGHTS FOR ACTIVE DIRECTORY

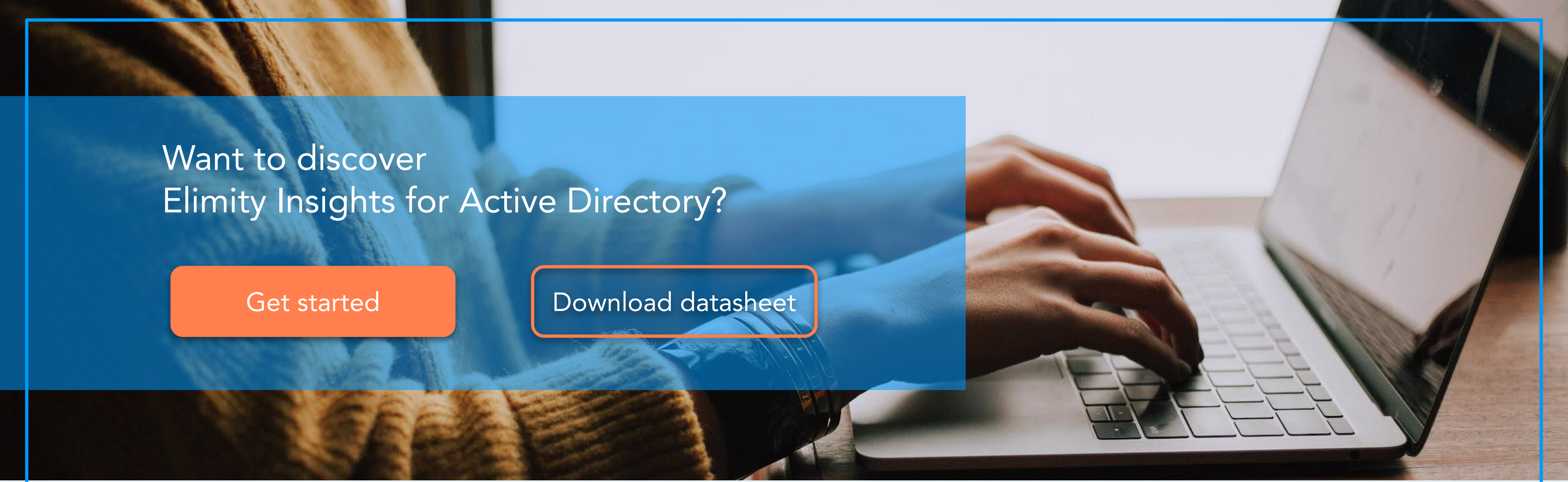


Risk cockpit

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