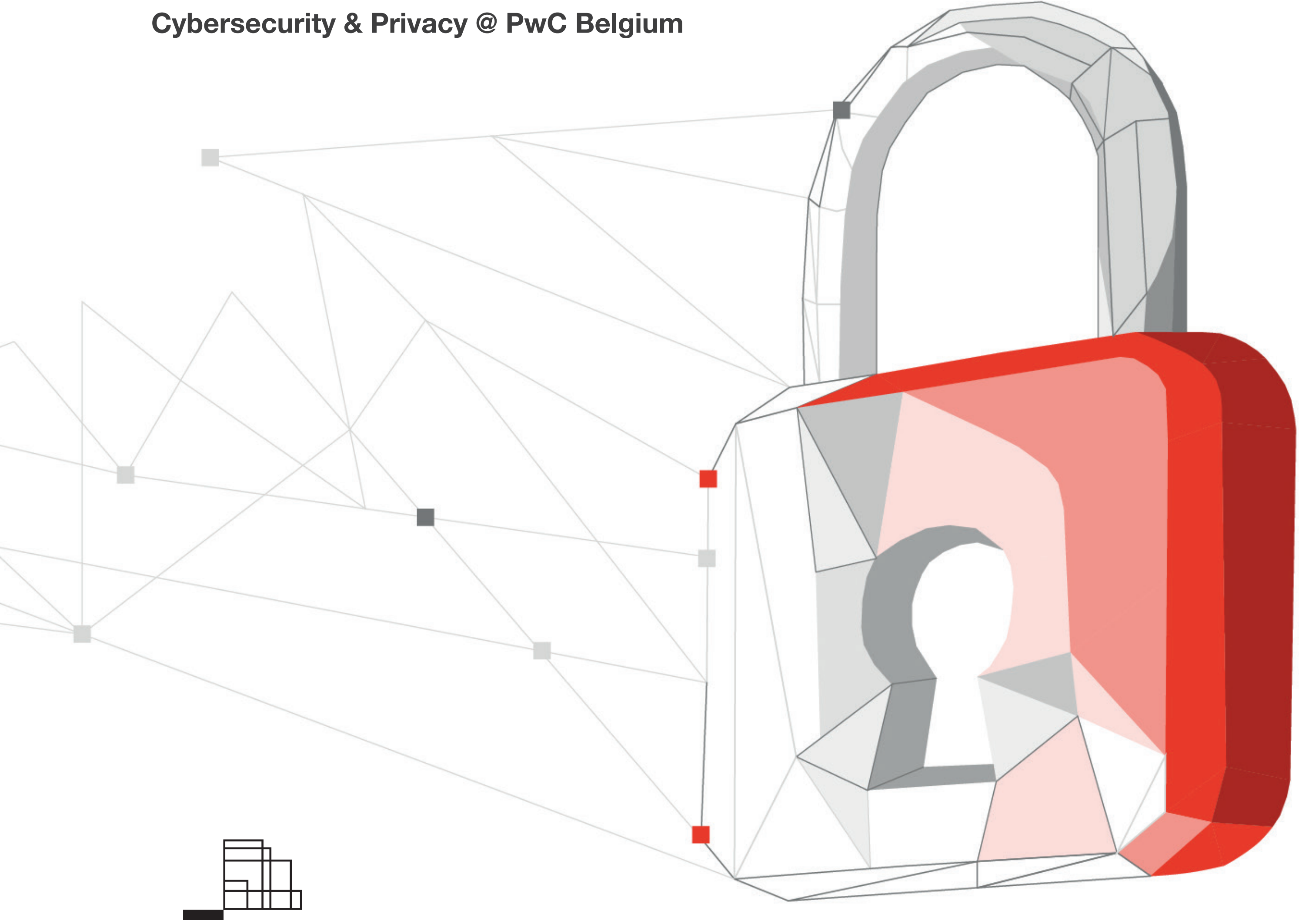
PwC Cybersecurity & Privacy whitepaper series:

Identity and Access Management – Insights and comments

By Jasper Bogaerts – Manager
Cybersecurity & Privacy @ PwC Belgium

and Sven Pauwels – Director
Cybersecurity & Privacy @ PwC Belgium



COVID-19 and IAM – Changes and challenges ahead

A year into the COVID-19 pandemic, it is clear that it has brought about changes that will impact our daily lives for years to come. Going forward, it is important to assess precisely what consequences we can expect in order to anticipate potential issues, determine how to approach upcoming impediments, and grab any opportunities the situation may offer.

The pace at which the pandemic has influenced the world has introduced changes at an unprecedented scale and rate. It will have an ongoing impact on how we conduct business. As COVID-19 is setting in motion considerable changes that are here to stay, it is important that we keep on top of the current and future challenges ensuing from the situation in order to stay in control. This also holds true for its impact on Identity & Access Management (IAM).

In order to shed light on this impact, PwC is launching a whitepaper series that reflects on the challenges, impediments, threats and opportunities that the pandemic raises with regard to IAM. By covering various topics, we intend to create a comprehensive view on what organizations can expect both in the near future and in the aftermath of the pandemic.

In this first part of this series, we focus on a non-exhaustive set of upcoming trends that we envision COVID-19 to induce. On this basis, we discuss common changes and challenges with regard to the general domain of IAM. Doing so, we consider the overarching shifts that may require action or planning on the part of your organization. Not only can this help you anticipate immediate challenges, it can also prepare you for future shifts. As such, this whitepaper serves as an introductory part of the COVID-19 IAM series. The next whitepaper covers the Identity Management (IdM) challenges and opportunities in the light of COVID-19 in more detail.

The pandemic has already been introducing considerable challenges over the last year. In particular, the manner in which we organize remote working has changed radically. In order to get a complete understanding of what this means in terms of IAM, as well as the recommended actions to take, we strongly recommend reading the Digital Identity & Remote Digital Workforce whitepaper (https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/digital-identity-supports-a-secure-remote-digital-workforce-duri.html) that focuses on the problems COVID-19 has brought about.

A whole new world, tomorrow

While the world's response to COVID-19 has typically been considered to be one of temporary measures to cope with pressing circumstances, deeper analysis suggests that it will have long-standing structural implications on many aspects of our lives. Many of those implications are hard to predict, and any attempt to compile a comprehensive list would likely prove ineffective. However, we foresee four major shifts that will have a significant impact on the positioning of IAM within organizations. Although some of the consequences originating from these trends are already becoming apparent, we believe that this is only the tip of the iceberg, and that IAM leaders should consider how these trends will impact their direct responsibilities in the mid to long term.

A different way of working

Perhaps the most evident impact that COVID-19 has had on many lives is the change in how we collaborate. In many parts of the world, an immediate response of businesses towards the direct consequences of the pandemic has been to stimulate or impose remote working as much as possible. This has already influenced the IAM responsibilities and operations significantly over the last year, and will continue doing so for the foreseeable future.

The mid- to long-term impact, however, is not always clear. While we expect some form of normalization towards a pre-pandemic era, the trend of remote working seems to have been put in full throttle, and a continuing shift towards smaller office spaces and an increased home-working mode is likely to occur. With regard to IAM, a permanent impact on policies, processes and technologies to support both office and remote working is to be expected. IAM leaders should ensure that the policies, processes and technology remain aligned with the vision and culture of their businesses.

The impact of increased remote working, however, will probably be deeper, as the flexibility this entails will likely lead to temporary positions being favoured even more for project and other work. The partial loss of control and oversight over the day-to-day activities of employees may open the door for an increased demand for freelancing and contract workers instead of full-time employees. This increased shift towards the so-called gig economy requires IAM operations to be prepared for the short term, a more dynamic nature of the responsibilities and policies, resulting in processes that should be well-defined to ensure efficient yet secure provisioning and deprovisioning of access.

What is more, the shift towards remote collaboration may result in a workforce that is not necessarily rooted in the same geographical region. This could pose implications with regard to how access management policies are defined and have consequences for the legal obligations and restrictions for businesses that IAM leaders should also be aware of. For example, ensuring that remote collaboration complies with legal or regulatory restrictions such as GDPR must be analysed prior to pursuing such labour strategies. Remote working may even impair troubleshooting issues and problems due to the lack of physical interaction.

As a consequence of this novel approach to working, trust relationships may also be put under pressure. Remote collaboration and freelancing relationships may increasingly result in situations where the involved parties never even meet physically. This substantiates even more the need for Zero-Trust Architectures, for which IAM is an important component. Absence of physical contact also complicates processes and policies that facilitate and secure credential provisioning, access rights approval flows and onboarding procedures. A clear approach to handle this in a standardized manner should be considered. Similarly, controls should be implemented to detect and act upon irregularities that could spring from such changing work relationships.

Lastly, remote working may lead to a disconnect between the employees and your organization. This can lead to complacency in executing processes and adhering to policies, which may introduce inaccuracies potentially resulting in efficiency loss and/or security risks. Similarly, due to an increased workload for employees, IAM tasks and responsibilities may not be followed up on in a timely manner, thus resulting in further efficiency loss and in SLAs not being met. Therefore, it is essential to ensure that accurate and effective metrics and controls are in place to detect such changes and to address potential hazards before they become structural issues.

Changes in threat actors

Economic, geopolitical and collaborational changes have shifted the risks that organizations are faced with. In particular, this has resulted in changing risk profiles for threat actors. Appropriate measures must be taken to mitigate these risks as much as possible.

Disgruntled employees

Restructurings and reduced leeway for compensating employees may increase the risk of them being disassociated or disgruntled with their organization. Appropriate controls must be put in place to protect your organization against insider threats. IAM is one such fundamental control. Recertification campaigns and optimized IAM processes are paramount as a defence against such risks.

Organised crime

Increased digital collaboration and higher dependence on digital infrastructure have caused a spike in ransomware attacks. Not only is IAM an important means to ward off the danger of organized crime, it is a key component to raise the bar and effectively protect your organization against such attacks.

Hacktivists and nation state actors

Economic and geopolitical trends due to the pandemic have the potential of stirring up activity from hacktivists and nation state actors. Organizations should be aware that they can become a target for cyber attacks from such external parties, and put in place IAM controls to mitigate inacceptable risks.

Competitors

Looming economic turmoil may heat up competition, opening the door for less than honest practices that yield economic advantages for the initiating party. Industrial espionage has been reported to have increased during the COVID-19 crisis. Your organization can protect itself against it through a comprehensive cybersecurity strategy of which IAM must also be a key element.

Increased global cooperation, and geopolitical shifts

The failure to contain the virus has had the effect of propounding the idea that a closer and more integrated cooperation between governmental entities in the field of several public goods such as public health is bound to benefit everyone. A need for cross-border coordination and collaboration on several fronts is likely to be considered by governmental bodies worldwide in an attempt to prevent risks that cross political borders. Such needs translate to concrete requirements for IT systems, be it for systems that are actively involved in the transfer of data that requires coordination, or through legal obligations and restrictions that organizations may have. A vision that considers the policy, guidelines and best practices for handling such data should be set out explicitly, and the IAM approach should be aligned with this vision. Organizations active in healthcare should especially be aware of any initiatives taken towards this end.

On the other hand, the rapid shifts and changes in measures have emphasized the need for governments to arrange their administrative operations in a flexible manner. A clear and efficient approach to compose and communicate administrative decisions to citizens could become an important factor for future strategies for IT in governments. Both governmental officers and organizations closely working together with governments should take note and ensure that they anticipate any changes that steer in this direction even more than before.

Unstable economic waters ahead

The response to contain further COVID-19 outbreaks has resulted in measures that have had and continue to have a deep economic impact. Both business initiatives and governmental measures have contributed to a situation that will have significant economic effects for years to come. Analysis as to the precise effects are beyond the scope of this document, but it suffices to say that fluctuations in economic activity are to be expected in the coming years.

The impact of COVID-19 on the economy is real but not necessarily structural for every market. Nonetheless, changes in business cycles will force businesses to become more efficient. This will lead the way for mergers, joint ventures and restructuring as a means to weather (potential) economic downturns or to seize new opportunities. As for IAM, such organizational reforms are likely to strongly impact the way in which IAM programs are organized, as well as the policies, processes and technologies that are used to support them. Furthermore, there will be a pressing need for optimization of IAM services so as to minimize employee downtime. For example, ensuring that accounts and accesses are provisioned in a correct and timely manner will become even more important, as it reduces downtimes for employees whenever they need to take on new responsibilities.

Additionally, a looming recession may lead to tech budget cuts. This will have an impact on tech roadmaps and potentially on how internal tech services are handled throughout an organization. The ramifications of these changes on IAM are twofold. First, investments targeted at improving IAM services may be put on hold. Second, there may be a significant influence on planned or anticipated developments within the application landscape of your organization. This in its turn impacts efforts required within the IAM program to align these developments with IAM policies and guidelines. This can result in opportunities to direct attention to tactical or strategic responsibilities within the window of attained time. It could be opportune to determine the priorities to be pursued.

At the same time, the economic outlook is not entirely pessimistic across the board either, and businesses should remain vigilant against overly conservative positioning as well. Fluctuations and novel opportunities could lead to sudden upticks in workload and activities, and IAM leaders should anticipate this by focusing on servicing elasticity and capacity planning. Preparing for IAM consequences due to increases in short-term contracts and customer demand boosts could prove a worthwhile investment of time and effort and ensure that businesses are adequately supported in their daily operations.

Evolving markets and business models

COVID-19 has initiated a wide variety of changes that impact and will keep impacting our everyday lives. Such changes open the door to new opportunities, and push businesses and markets towards innovative models. Also, the pandemic may spur regulatory and legal restrictions on markets, forcing businesses to align their processes and controls for compliance. Although the long-term impact on business models and markets is non-trivial to predict, pressure on production, value chains and processes in the short term seems likely. As circumstances evolve, organizations are or will increasingly be considering a digital transformation. This also has a likely impact on the IAM strategy.

- **Relationships with customers may change significantly.**
- **The trend towards digitization of sales may require maturity levels with regard to C-IAM to be elevated.**
- **Alliances may become more interesting.**
- **User interfaces will need to be clear in order to add value to the organization as compared to competitors.**

Reference: Forrester ["Staffing: Retailers Must Review Their Marketing And Customer Experience Budgets In The Wake Of The COVID-19 Pandemic", October 28th, 2020, "Rick Parrish, Fiona Swerdlow, et al.", https://www.forrester.com/fn/1BBowh10YURJkTpdIR8Ts0]

One key development in this context is the accelerated adoption of cloud computing infrastructures and applications. Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) solutions from providers such as Amazon AWS and Microsoft Azure are increasingly being adopted as the fundamental building blocks for enterprise applications. Moreover, Software-as-a-Service (SaaS) applications are also being adopted increasingly, requiring changes to business processes and new approaches to how businesses solve problems. Such changes unavoidably have an effect on IAM and on how these systems are onboarded and remain protected through policies, processes and technologies.

In addition, an increased focus on digital transformation and digital interaction with customers is also probable. This digital transformation will be new for some and well-known for other target customer groups. It will be key for businesses to organize the way they interact with these groups so that they capture their attention first and hold it through a positive experience. IAM leaders should support their businesses in ensuring that interaction with customers and employees is both smooth and secure. Accommodating frictionless data transfers between customers and business partners in a secure manner can drive innovation and enable a business to differentiate itself from its competitors. Moreover, a well-thought-out customer IAM approach could be a key component to distinguish your business from the competition. These will become key factors that make the difference for businesses, and so they will need to be considered.

Never let a crisis go to waste

Over the last century, an increasingly interconnected world has been offering us unprecedented opportunities and prosperity. However, such interconnectedness also holds risks. Local crises can quickly evolve to global catastrophes with widespread consequences. A growing global population will magnify already considerable challenges to an increased extent. This is not in the least true for pandemics, which could be expected to rise in frequency as well in the light of a strongly growing world population.

Consequently, as an IAM leader, it is paramount that you do not only focus on the challenges that your organization is facing today but also on the upcoming challenges and opportunities. In order to be prepared for the challenges ahead, we advise you to take into account the following considerations:

1

Realign your vision

COVID-19 will inevitably have a long-lasting impact on us, and on our businesses. Evolving circumstances may lead your organization to change its vision and priorities. With this in mind, it is important to follow suit with your IAM program and to ensure that the IAM services your team offers remain coordinated with business requirements and expectations.

2

Set up an IAM roadmap

Align your roadmap with the strategy that your organization will be taking to cope with the aftermath of the pandemic. Economic outlooks may influence budgets and your organization's workforce, for better or worse. Anticipate the challenges and opportunities associated with this through prioritization of tactical and strategic projects to strengthen your IAM service catalogue, and make sure that it remains aligned with the direction of your organization.

3

Re-evaluate all IAM processes and policies

The pandemic has forced businesses to improvise or compromise on how policies and processes were enforced. Through time, there may already have been a chance to normalize these compromises and iron out the biggest risks involved. However, in order to ensure that no recent changes have and will keep on having a significant impact on your IAM program, it is opportune to evaluate the processes and policies. Temporary compromises that were taken to cope with exceptional circumstances may turn out to become permanent. Other compromises need to be reversed and potentially audited.

4

Validate that IAM technologies and tools address established and emerging requirements

Trends following COVID-19 may introduce novel requirements that need to be met in order to ensure the same quality of service from your IAM program. These requirements need to be supported by appropriate tools and technologies. For example, access controls such as Multi-Factor Authentication (MFA) may need to be implemented or tightened for untrusted devices, or additional attention may need to be given to scalability of access management systems. Similarly, considering more advanced Customer IAM strategies could be an important game changer within the market your organization is active in.

5

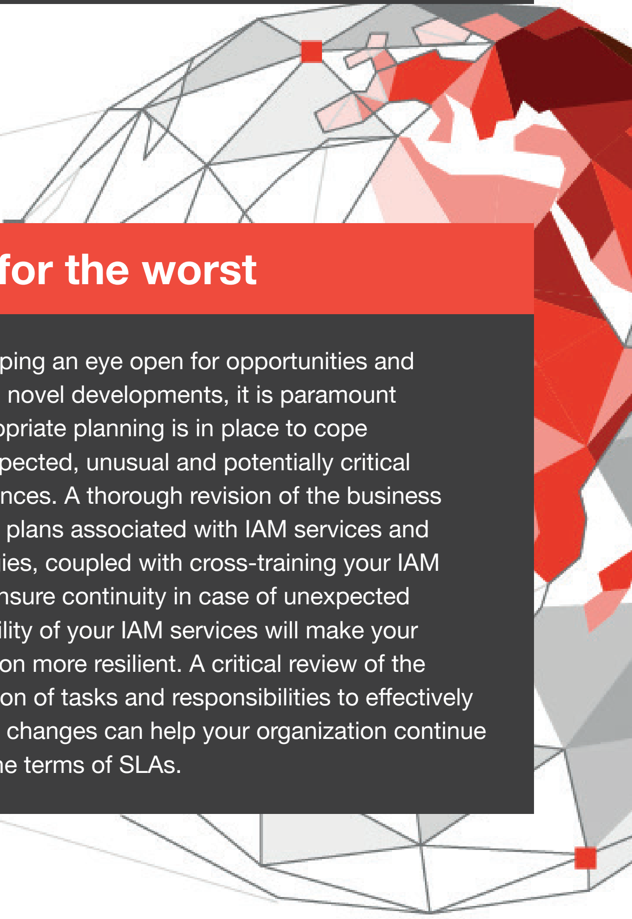
Leverage digital transformations, changing strategies and upcoming trends

With crisis comes opportunity. The pandemic is indeed widely considered to have boosted digital transformations within businesses to a significant extent. The pace of cloud adoption has been stepped up while seemingly inert processes have changed fairly quickly. This paper has touched upon several trends, changes and challenges that may occur in the mid to long term. Anticipating and preparing for such changes ensures that your organization remains ahead of the market and is able to cope with novel circumstances with less friction.

6

Implement a zero-trust architecture

Through digital transformations and changing employee relationships, existing assumptions on the security architectures of organizations must be reconsidered, and the future of legacy systems may require re-evaluation. In order to cope with these novel and elevated risks, one important trend is the evolution towards zero-trust architectures. In such architectures, IAM takes up a key role. Evaluating the requirements for IAM programs to support such architectures ensures that a future-proof strategy is pursued.



7

Plan for the worst

While keeping an eye open for opportunities and promising novel developments, it is paramount that appropriate planning is in place to cope with unexpected, unusual and potentially critical circumstances. A thorough revision of the business continuity plans associated with IAM services and technologies, coupled with cross-training your IAM team to ensure continuity in case of unexpected unavailability of your IAM services will make your organization more resilient. A critical review of the prioritization of tasks and responsibilities to effectively cope with changes can help your organization continue to meet the terms of SLAs.

We should not remain blind to forthcoming challenges. Anticipating our IAM strategy to be ready for expected developments ensures that we remain in a good position to seize the opportunities that such changes produce, and ensures that our organizations remain strongly anchored in a future-proof approach.

Want to know more?

PwC houses one of the largest and most skilled teams in Belgium when it comes to Cybersecurity and Privacy (C&P). We have combined our General Data Protection Regulation (GDPR) and data protection capabilities with our cyber and information specialists to help build a secure digital society. Discover more about who we are and what we offer at https://www.pwc.be/cyber.

About the authors

Woluwedal 18
1932 Zaventem
Belgium

Mobile: +32 (0)499 18 37 67

Email: jasper.bogaerts@pwc.com

Jasper Bogaerts – IAM Expert PwC Belgium

Manager Cybersecurity & Privacy

Brief introduction

Jasper Bogaerts is a Manager at PwC with a strong focus on Identity and Access Management (IAM) and Privileged Access Management (PAM). Jasper holds a PhD in Computer Science Engineering, specializing in access control.

Over the course of his career, he has gained experience in several information technology domains, including distributed systems, cloud computing platforms, architectural analysis, software development, and security in general. He has done so in the context of projects at different Belgian organizations, performing analysis and managing operational tasks for different aspects within security, particularly IAM and PAM.

Jasper has also published several research articles in international journals and at conferences as part of his academic career, with a focus on facilitating and improving authorization in multi-tenant Software-as-a-Service (SaaS) applications.

Relevant experience & core competencies

Jasper has been involved as a business analyst with a strong technical background in a wide variety of IAM projects for various Belgian organizations. In these projects, he has taken on several responsibilities including but not limited to:

- defining IAM architectures and roadmaps,
- defining PAM architectures and roadmaps,
- performing IAM and PAM requirements analysis,
- performing IAM and PAM maturity analysis,
- providing IAM RFP process guidance and support.

These competencies have been amassed in multiple industries, including Finance, Healthcare and Governmental organizations.

Generaal Lemanstraat 67
2018 Antwerpen
Belgium

Mobile: +32 (0)475 70 63 86

Email: sven.pauwels@pwc.com

Sven Pauwels – IAM Leader PwC Belgium

Director Cybersecurity & Privacy

Brief introduction

Over the last 15 years, Sven has been involved in building Information Security Competence centres in a diversity of environments. He has provided guidance to companies as an Information Security Advisor and an IAM Expert. Sven helps companies define their strategy and vision to secure their information, and set their requirements, and assists them in making product choices and in evaluating vendor offers. Sven has been involved in managing IAM engagements in various set-ups and with various levels of complexity.

Relevant experience & core competencies

As a Strategy and Tactical Subject Matter Expert on IAM topics, Sven advises client senior management on Identity Project management and success factors. Acting as the supervisor having final responsibility for delivered IAM services, he has worked with various local, European and global companies in multiple sectors including:

- Finance,
- Healthcare & Pharma,
- Utilities,
- Retail,
- Telecom,
- Local, Federal, European Government,
- Transport.

Identity programs completed under the lead of Sven

- Consumer Identity/Digital Customer Experience
- Identity Management and Identity Governance
- Privileged Account Management
- Complex access management and federation engagements
- Setting up IDaaS environments
- Setting up and building internal IAM Governance and IAM Support Teams for clients