A New Age of Authorisation: Empowering Zero Trust with Policy-Based Access Control

October 2023

pwc

www.pwc.nl

Table of Contents

Introduction

In the ever-evolving landscape of information security, access control stands tall as a fundamental principle, determining who is granted access to an organisation's precious information and resources. Access control mechanisms, consisting of authentication (AuthN) and authorisation (AuthZ), play a crucial role in ensuring that users are who they claim to be and have the appropriate access to organisational resources. By providing the necessary controls to enforce security policies, limit access to sensitive information, and thwart unauthorised entry, access control mechanisms serve as supporters of information security.

Imagine a world where the right individuals have seamless access to the resources required for their tasks, ensuring the smooth flow of work while keeping sensitive data safe from prying eyes. This vision is precisely what access control mechanisms can bring to life within your organisation. By implementing access controls at various levels, from operating systems and databases to applications and network devices, you can bolster your organisation's security posture and meet compliance requirements with confidence.

We are also living in an era of rapid technological advancement and escalating cyber threats, access control therefore, is the cornerstone of a robust information security system. While it's clear that access control is the way to go, its implementation should be coupled with a comprehensive information security strategy, one that safeguards your business and ensures business continuity. As a result, this is where embracing Zero Trust as a strategy can create a paradigm shift in the way we safeguard our valuable assets.

Embracing a forward-thinking perspective, Zero Trust challenges the conventional notion of blindly trusting everything within the organisational perimeter. Instead, it places a spotlight on securing the organisation's assets through a proactive and context-aware approach. In an environment where technology is evolving at an unprecedented pace and organisations are rapidly scaling, driven by the widespread adoption of cloud technology, data has permeated every facet of our operations.

Recognising the critical juncture at which organisations stand during their digital transformation journey, embracing Zero Trust as a strategic imperative becomes crucial. The swift scaling of organisations driven by cloud adoption has intertwined access with data at an unprecedented level. In response to this complex landscape, the Zero Trust strategy offers a beacon of security. It advocates not only for stringent access controls but also for a comprehensive approach that constantly evaluates and adapts to the evolving threat landscape. (Check out our paper *Decoding Zero Trust* to learn more about Zero Trust).

As you navigate this whitepaper, you will uncover a transformational access control mechanism known as Policy-Based Access Control (PBAC). A concept rooted in the tenants of Zero Trust and especially within the principle of least privilege. By embracing PBAC, you empower your organisation's Identity and Access Management (IAM) practices, solidifying your defence against emerging threats.

Throughout the following pages, we will embark on an exploration of the PBAC journey. We will delve into its myriad advantages and elucidate how it synergises with Zero Trust to fortify your organisation's security and resilience. Using clear language and actionable insights, this whitepaper serves as your guide towards forging a safer and more secure digital future.

So, buckle up for an enlightening journey as we dive into the New Age of Authorisation, where PBAC and Zero Trust join forces to usher your business into a new era of security and trust.

The Evolution of Access Control

Over the past two decades, access control has embarked on a fascinating journey, moulded by the ebb and flow of data security approaches. We witnessed the emergence of the Mandatory Access Control System (MAC), where access revolved around predetermined security labels and rules, paving the way for the structured Role-Based Access Control (RBAC) era, and the dynamic landscape of Attribute-Based Access Control (ABAC).

As we reflect on this journey, it becomes clear that the emergence of PBAC marks a groundbreaking breakthrough. PBAC, with its fusion of roles, attributes, and logic, heralds a new era of unparalleled fine-grained access control, reinforcing the principle of least privilege, and seamlessly harmonising with the visionary concept of Zero Trust. Now, let us delve deeper into the unique characteristics, advantages, and disadvantages of the earlier access control models; MAC, RBAC, and ABAC, as we unravel their distinct contributions to this transformative evolution.

Mandatory Access Control System (MAC)

- **Characteristics:** The MAC system operates by allowing or denying access to private information within an organisation. Users are categorised into special groups and access decisions are based on criteria set by the system administrator.
- **Advantages:** MAC provides high-level data protection, ensuring sensitive information is safeguarded from unauthorised access. The system's centralised control by one authority enhances privacy and security.
- **Disadvantages:** Setting up MAC requires careful attention and regular updates to accommodate changes in data. The system's centralised nature can lead to bottlenecks and operational inflexibility.

Role-Based Access Control (RBAC)

- **Characteristics:** RBAC revolves around creating roles with specific permissions for different resources (e.g., network, application). Users are then assigned to one or more roles.

Team lead marketing role
- Can view and edit Marketing Data
- Can view Marketing HR data
- Can create marketing campaigns

R&D department head
- Can view R&D budget
- Can view design documents
- Can create new R&D projects
- Can view R&D HR Data

HR employee
- Can edit employee data
- Can create new job positions

Internal Finance Analyst
- Can establish department budget
- Can view organization's finances

- **Advantages:** RBAC offers a simpler approach to access control lists (ACLs) by associating permissions with roles. It is well-suited for small to medium-sized organisations with a limited number of roles, enabling quick and cost-effective implementation.
- **Disadvantages:** Administrators may face challenges in managing user-role mappings, potentially leading to administrative bottlenecks. The complexity increases as the number of roles grows, contributing to long-term maintenance costs. Frequent changes in roles may result in role explosion.

Attribute-Based Access Control (ABAC)

- **Characteristics:** ABAC considers various attributes such as a user's position in the company, objects within the system, user actions, and environmental factors to determine access rights.
- **Advantages:** ABAC offers fine-grained access control, inspecting a wide range of attributes. It provides increased flexibility and scalability, as policies can be changed at any time without strictly adhering to a linear setup.
- **Disadvantages:** While ABAC provides enhanced flexibility, it may not be suitable for smaller companies due to increased complexity. Implementing ABAC requires writing rules in computer codes like XAMCL or JSON, requiring IT teams for deployment and maintenance.

Environment attribute

- Where is the user connecting from
- Time of the day

HR Attribute

- Subject's role
- Subject's department
- Subject's Manager

Asset attribute

- Location
- Data lype
- Data confidentiality
- Criticality level

The new age of authorisation

Just as RBAC elevated security and ABAC brought in granularity and scalability, PBAC introduces an enhanced approach to AuthZ, setting the stage for unprecedented flexibility and control.

At its core, PBAC is a masterful combination of roles, attributes and logic. Through this ingenious fusion, PBAC crafts flexible and dynamic control policies that adapt congruously to an organisation's diverse access requirements. A multitude of attributes become the guiding stars, determining who gains access and under what conditions. PBAC's design caters to all manners of access devices, ensuring a harmonious experience across the enterprise.

PBAC's fine-grained AuthZ opens doors to a new realm of possibilities. Access rules can now be shaped based on a variety of contextual factors, reducing the vast array of roles to a concise set of policies. Imagine thousands of roles condensed into just hundreds, a feat made possible by PBAC's user-friendly language and scalable implementation.

In a refreshing shift, PBAC introduces natural language rules, transforming the AuthZ landscape to be more business-oriented and user-friendly. Moreover, PBAC unveils a groundbreaking revelation: there are no roles to review! Embracing a role-less model, PBAC eliminates the need for cumbersome access reviews, streamlining the access control process.

PBAC embraces the essence of the least privilege principle, ensuring that access decisions are made based on a comprehensive set of data points. The access-decision making model delves deep into the following questions:

- Who are the identities seeking access, and what level of access do they require?
- What resources are being accessed, and what actions will this access allow the user to perform?
- Under what circumstances is access allowed, and what is the context, such as the time of day, network segment, or other factors, influencing this access?

Emphasising comprehensive AuthN and AuthZ, PBAC empowers organisations to protect their valuable assets with precision. By verifying user identities, locations, device health, workload, data classification, and even conducting anomaly checks, PBAC ensures access is granted only to those who genuinely require it. It's worthwhile noting that policies are continuously evaluated in real-time, dynamically responding to contextual information, allowing for fine-grained and adaptive access control. Context is paramount, as PBAC considers user attributes, locations, time of day, environmental conditions, and other vital factors when making access decisions.

In the end, while PBAC offers numerous advantages, including flexible control policies and fine-grained access rules, there are some considerations to keep in mind during the initial setup. PBAC demands extensive planning and technical assessment and retrieving all attributes may require additional connectors. However, the benefits of enabling a Zero Trust environment with PBAC outweigh the disadvantages. With careful planning, organisations can leverage PBAC's transformative potential to establish a robust and future-proof AuthZ framework.

PBAC Key Components and Processes

The key components of PBAC revolve around three crucial elements: the Policy Information Point (PIP), Policy Decision Points (PDP), Policy Enforcement Points (PEP), as well as the essential aspects such as Policy Language, Policy Management and Policy Governance.

The PIP serves as a critical source of attributes used by the PDP during the access control process. By providing relevant attribute data, the PIP empowers the PDP's policy engine to make informed AuthZ decisions based on established policies.

The PDP encompasses two fundamental components: Policy Administration and Policy Engine. The Policy Administration enables the management and governance of access control policies. It allows administrators to define, modify, and enforce access rules, permissions and other policy-related parameters. On the other hand, the Policy Engine is responsible for evaluating access requests based on the defined policies and various attributes, ensuring informed access control decisions.

The PEP acts as a vital guardian of the access control process. Deployed at various points within an information system or network, the PEP interprets access requests and enforces the appropriate access controls. As the gatekeeper, the PEP ensures that access is granted or denied based on the policy decisions made by the Policy Engine within the PDP. It plays a pivotal role in enforcing access policies, making real-time decisions, and actively participating in the establishment of a Zero Trust environment.

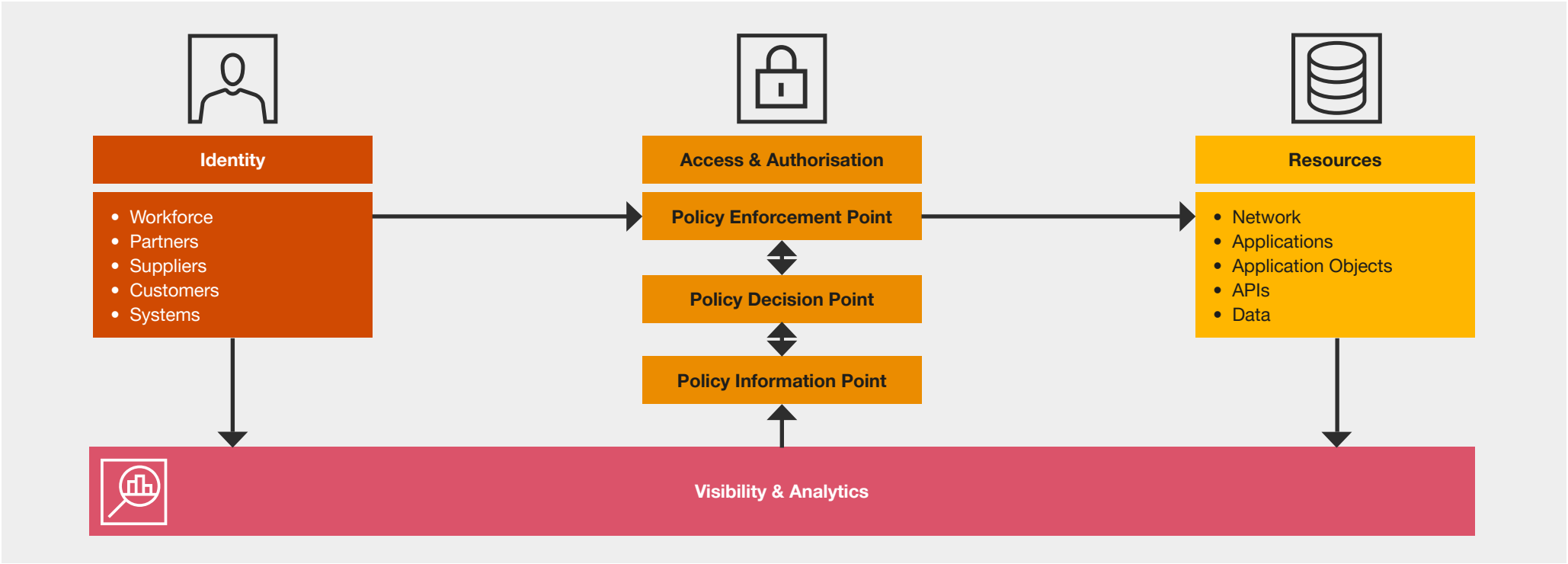
In conjunction with the PDP, PIP, and PEP, the Policy Language plays a pivotal role in defining access control policies. This formal or unstructured language enables administrators to express desired rules, conditions, and constraints, providing the necessary syntax and semantics for the Policy Engine's interpretation.

Policy Management is the process of creating, modifying, and maintaining access control policies. It involves defining rules and conditions that govern resource access within the system. Policy versioning and administration ensure that access control policies remain up-to-date and aligned with organisational requirements.

Policy Governance involves the oversight, control, and enforcement of access control policies. It establishes policies, defines roles and responsibilities for policy management, and ensures compliance with regulations and standards. Periodic policy reviews, audits, and updates ensure that the policies remain effective and aligned with the organisation's goals.

The diagram below demonstrates the key components of the PBAC process:

Through the harmonious interplay of the PIP, PDP (comprising Policy Administration and Policy Engine), PEP, and other vital aspects like the Policy Language, Policy Management, and Policy Governance, organisations can establish a Zero Trust environment that adheres to the principles of least privilege. These components, working in tandem, form the pillars of a robust and future-proof AuthZ framework. With these elements in place, organisations can confidently safeguard their valuable assets and bolster their security posture in an ever-evolving threat landscape.



RBAC is staying for the midterm

The emergence of PBAC calls for a balanced approach, building upon the strengths of ABAC and RBAC. While PBAC offers significant benefits, transitioning to this model requires careful planning and trial. Currently, RBAC stands as the most widely adopted access control model due to its simplicity in initial setup. However, its inherent limitations, such as role explosion and access reviews, necessitate a shift towards the more advanced PBAC for a truly empowered Zero Trust environment.

We recommend organisations to embark on a hybrid solution, strategically implementing PBAC. This entails creating well-defined policies and employing dynamic AuthZ to enable a frictionless transition. To begin, a risk-based approach should be adopted, with low-critical applications moving first to the PBAC model. This approach allows organisations to learn from the process and make necessary adjustments to the access-decision model. As confidence grows, crown jewel applications should also be migrated, ultimately eliminating the need for access reviews.

Yet, the journey to PBAC integration may face challenges when dealing with legacy applications. These applications, built on outdated technologies and architectures, may not readily align with PBAC requirements, requiring complex retrofitting that consumes time and effort. The lack of adequate documentation and vendor support further compounds the integration process and increases the risk of errors. Modifying legacy applications without proper testing may lead to system instability and security vulnerabilities, necessitating a careful evaluation of integration requirements.

Given the high adoption of RBAC in the market, PBAC will not immediately replace it. The transition to a PBAC-empowered Zero Trust environment demands patience and strategic management of legacy application integrations. A pragmatic approach will allow organisations to leverage the benefits of PBAC while upholding the strengths of RBAC, leading to a smoother and more successful transformation.

Securing Customer Insurance Information with PBAC: A Pragmatic Use Case

In collaboration with a prominent insurance company, our focus was to safeguard their vast repository of sensitive customer insurance information, including policy details, claims history, and personal data. The goal was to ensure that only authorised employees could access the system, adhering to contextual factors such as job functions, customer confidentiality requirements and the principle of least privilege.

The journey to fortify access control commenced with the design of robust PBAC policies, encompassing three key elements:

1. **User Functions and Attributes:** such as certifications, department affiliations and job responsibilities.
2. **Resource Classifications:** such as personally identifiable information (PII) and sensitive financial data.
3. **Contextual Factors:** such as customer consent, purpose of access, location, etc.

The real strength of the use case came to life with the policy enforcement and decision points, where PBAC's capabilities shone brightly:

- **Access Request:** When an employee requested access to the insurance information system, the PEP intercepted the request and directed it to the policy engine for evaluation.
- **Policy Evaluation:** The Policy Engine assessed the access request, considering the employee's function, attributes, resource classification, and contextual factors.
- **Access Decision:** With a wealth of information at hand, the Policy Engine dynamically determines access privileges, providing a decision on whether to grant, deny, or require additional AuthN or AuthZ.

A pivotal aspect of this use case was the incorporation of contextual factors and attribute-based policies. For example, when an insurance claims adjuster personnel sought specific customer claim information, the Policy Engine scrutinised the request, by possessing the appropriate requirements, relevant certifications and necessary customer consent. Additionally, the classification of the information, the adjuster's location and the time of the request were considered before granting access.

Through this practical use case, you can see how PBAC can enhance access control, ensure data security and align with the organisation's least-privilege principles. The success of this project served as a testament to PBAC's adaptability and effectiveness in safeguarding sensitive information and bolstering the insurance company's security posture.

The benefits of PBAC for this insurance company was improved data protection, compliance and regulations and the mitigation of potential unauthorised access. PBAC has helped ensure that customer insurance information is only accessed by authorised employees based on their functions, attributes and contextual factors. PBAC ultimately improved the protection of customer confidentiality and adherence to data privacy regulations including the General Data Protection Regulation (GDPR).

Below are some use cases in action:

Use Case 1: View sensitive information from a regular claim when working from home (or anywhere not within the Insurance Company network).

Claims Adjuster logs in and wants to view a Claims Declaration of a Customer using an application

The application automatically makes an API call/request to PBAC solution

PBAC solution evaluates the request and kicks off a policy

The policy allows the Claims Adiuster to view the file if the Claims Adjuster is in the right department and the Claims Declaration is in the same Region as the Claims Adjuster is working in

Policy: Customers Insurance Claim (CIC) can be Viewed by the Claims Adjuster belonging to the 'Customer Claims' department if the CIC is in the same Region as the Claims Adjuster.

User Case 2: Modify sensitive data from a regular claim when working from home.

Claims Adjuster logs in and wants to view view and modify a Claims Declaration of a Customer using an application

The application automatically makes an API call/request to PBAC solution

PBAC solution evaluates the request and kicks off a policy

The policy does not allow the Claims Aduster to modify the file

The Claims Adjuster is from the right department and the CIC is from the same Region as the Claims Adiuster

But the Claims Adjuster is not working from the Corporate Network

Policy: Customers Insurance Claim (CIC) can be Modified by the Claims Adjuster belonging to the 'Customer Claims' department if the CIC is in the same Region as the Claims Adjuster and the Claims Adjuster belongs to an assigned Case Handler Team + the Claims Adjuster is working from the Corporate Network.

Conclusion

In conclusion, this whitepaper has guided us through a transformative expedition, tracing the evolution of access control models and unveiling the dawn of a new era in AuthZ with the introduction of PBAC. Throughout our exploration, the paramount role of AuthZ in ensuring information security has been illuminated, with a special focus on how PBAC synergises with Zero Trust environments to bolster data protection, enhance access management, and solidify the principles of least privilege.

As we stand at the threshold of embracing PBAC, it is imperative to acknowledge that this transition demands meticulous planning and a tailored approach to each system's unique characteristics and the specific needs of the business. PBAC's innate dynamism facilitates the active involvement of business personnel in policy design, alleviating the burden on technical teams and simplifying the intricacies of policy formulation.

Furthermore, within the context of this transformative journey, it is worth noting the significance of RBAC as an established and widely adopted model. While PBAC heralds a new frontier in AuthZ, the pragmatic integration of PBAC with RBAC presents a balanced and strategic approach. The strengths of RBAC continue to shine in the midterm, serving as a foundation upon which to build the intricate tapestry of PBAC's advanced capabilities. This hybrid approach ensures continuity, gradual adaptation, and a smoother transition to PBAC's empowered Zero Trust environment.

In essence, this whitepaper has not only highlighted the pioneering path of PBAC but has also acknowledged the enduring relevance of RBAC. As organisations venture forward, embracing the dual strengths of these access control paradigms will undoubtedly lead to a more secure and future-ready AuthZ landscape, reinforcing the fortifications of information security for years to come.

How can we help?

As the new age of AuthZ dawns, we at PwC stand ready to support your organisation's journey towards implementing PBAC and embracing the transformative philosophy of Zero Trust. Our range of comprehensive services is designed to empower your organisation's security posture and ensure a smooth transition to a more robust access control model.

Zero Trust Assess and Design: Navigating a Secure Future

In the ever-changing world of cybersecurity, securing your future requires careful planning. Our Zero Trust Assess and Design service is your partner in navigating this journey, focusing on IAM at its core.

Our IAM experts are at the centre of Zero Trust Assess and Design, guiding you step by step:

1. **Understanding Your Risks and Challenges:** We collaborate closely to grasp your unique risks and challenges.
2. **Blueprint for Security:** We design a target architecture aligned with your security and business goals.
3. **Assessing Your Now:** We evaluate your current state and pinpoint areas for improvement.
4. **Clear Roadmap:** Based on our assessment, we provide a clear roadmap to guide your secure future.

With Zero Trust and PBAC principles, we create an access framework that fits seamlessly with your business. This proactive approach ensures your security strategy is ready for tomorrow's threats.

Zero Trust Assess and Design specialises in IAM, covering Privileged Access Management (PAM), Customer Identity and Access Management (CIAM), and Workforce Identity and Access Management (WIAM). Strengthened by technology partnerships, we ensure your digital future is not only secure but also poised for success.

Zero Trust Readiness Assessment: Charting Your Path to Zero Trust Maturity

Within our Zero Trust Assess and Design service, we also offer a specialised component known as the Zero Trust Readiness Assessment. This focused evaluation allows you to gain deeper insights into your organisation's readiness to embrace the principles of Zero Trust. Delving into key domains such as identity, infrastructure, data, and application security, our assessment identifies vulnerabilities, assesses access controls, and evaluates threat protections. The result is a comprehensive report that offers actionable recommendations tailored to your organisation's unique needs. This subset of the Assess and Design assignment serves as a critical step to discovering your Zero Trust readiness and lays the groundwork for a more comprehensive Zero Trust strategy.

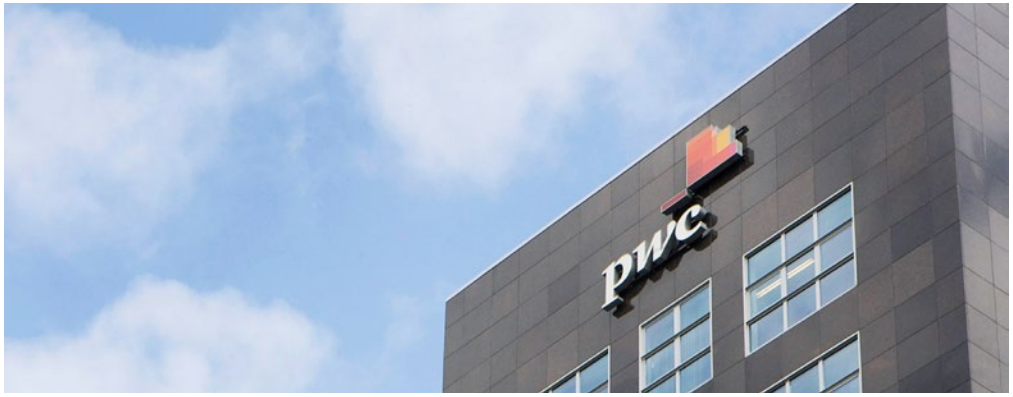
To embark on this transformative journey and elevate your organisation's security posture, do not hesitate to get in touch with us at PwC. Together, we look forward to partnering with you in a journey to navigate the complex landscape of access control with confidence and resilience towards enhanced security to support your agile and productive business.

Contacts

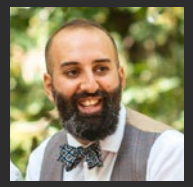
For more information and to initiate the assessment process, please find our contact details below.

Gerald Horst
Partner
gerald.horst@pwc.com
Tel: +31 (0)65 517 51 51

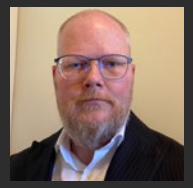
Fadi Daood
Manager
fadi.daood@pwc.com
Tel: +31 (0)63 875 94 32



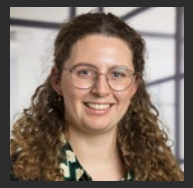
About the Authors:



Fadi Daood: Fadi is an experienced Information Security architect leading PwC's Zero Trust community in EMEA.



Micha Haas: Micha is experienced in the consulting of Identity and Access Management solutions, helping clients establish access control policies and standards.



Hannah Green: Hannah is an experienced Identity and Access Management consultant. Her expertise lies in change management and implementations that safeguard information security.