
cegeka

# Identity & Access Management

Discover our latest blogs

# 1

# IAM is the Swiss Army knife of IT Security

# IAM is the Swiss Army knife of IT Security: it can do it all. But you don't have to do it all at once

A few times a year, we have a chat with one of Cegeka's topical experts. Today we're with Ricardo Kowsoleea, IAM Product Manager at Cegeka and former VP of Technology at SecurIT – a company that has been strengthening Cegeka's work in the field of identity and access management since the acquisition at the end of last year.

We'll be talking about:

- What exactly is Identity & Access Management (IAM) and how has this field evolved?
- What are the three pillars of IAM?
- Why is it important that businesses don't focus just on the technical side of IAM?
- What are the current hot topics in IAM?
- What direction is IAM taking these days?

Are you also eager to learn his insights? Let's go!

> *Ricardo, you've been working in Identity & Access Management for over twenty years. Can you explain briefly what it's all about?*
>
> **– Bart Van den Branden, Cegeka Head of Product Management Networking & Security**

**Ricardo Kowsoleea:** "Identity & Access Management (IAM) is a field in cybersecurity; specifically, it falls under the heading of Prevention. The goal of prevention is obviously to prevent security incidents – but while still ensuring that the people using your IT have the permissions they need to do their work effectively, when they need them."

"There are three pillars to IAM: Access Management, Identity Governance & Administration, and Privileged Access Management. These are three sides of the same triangle: identity. Whenever you log into a system – be it your online bank account, Facebook, or perhaps your Administrator account when you arrive at Cegeka in the morning – you have to tell that system who you are. This identity information is vital for the automated environment to recognize you and determine what you're allowed to do."

## *Has IAM always been seen as important in cybersecurity?*

**Ricardo Kowsoleea:** "IAM has evolved a lot over the years. In the past, there was a lot of focus on 'return on investment', i.e. things like reducing the volume of Helpdesk calls, getting people logged in to start work as quickly as possible, and tools like Single Sign-On (access to several target systems with a single username and password) that make life easier for the user. "

"Then in around 2003, the focus shifted towards compliance. Legislation like SOX, HIPAA and Basel II was coming in and companies were suddenly obliged to set up IAM properly in order to comply with these new regulations. Companies and individuals could be held responsible if they didn't have properly configured IAM systems in place. So, for example, major banks were obliged to set up Privileged Access Management. There was a flip side though: because of the emphasis on legal compliance, IAM was often treated as something to be ticked off for audit purposes, and then forgotten about."

"There's been another shift in more recent years, with a growing emphasis on security, and IAM now plays a major role in security policies. We all know that threats like ransomware and other modern attack vectors are increasing rapidly. In the past, company data was stored on-premises, and protected from the outside world by a firewall. Firewalls are certainly still relevant, but the modern emphasis on cloud storage means different security paradigms: in particular, it's important to be able to authenticate identities reliably and provide access to the right data and applications. Of course, ROI and compliance haven't been forgotten. They still have a role to play in IAM policies. But they're really secondary to security now."

*"There's been another shift in more recent years, with a growing emphasis on security, and IAM now plays a major role in security policies."*

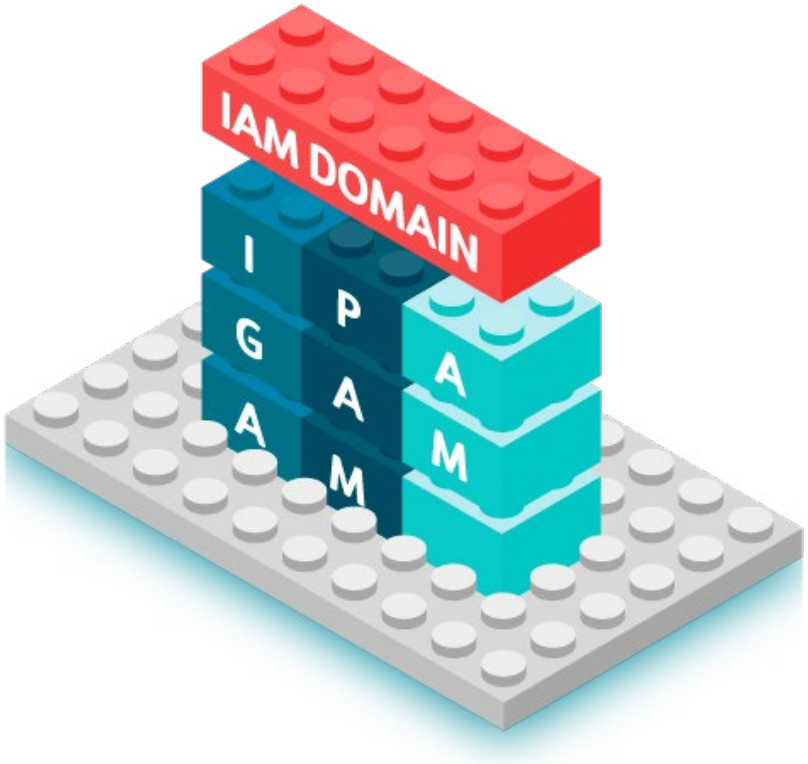
## *Is it just large organizations who need to think about IAM?*

**Ricardo Kowsoleea:** "Certainly not. The days when banks were the primary targets for security incidents are long gone. Smaller organizations are just as likely to get hit nowadays. We're seeing that shift reflected in the IAM market. It used to be just big businesses that had IAM programmes. But these days, companies with just 500 people on the payroll will see it as completely normal to implement an IAM system."

"This goes hand in hand with IAM having become much more accessible to smaller businesses. In the old days, setting up IAM would involve a lot of customization and a complex, highly specialist rollout through the organization. It often just wasn't practical. These days, we have much more user-friendly SaaS and Managed Services solutions that you can just plug into your systems via a connector."

## *Earlier, you mentioned the three pillars of IAM. Can you explain a bit more?*

**Ricardo Kowsoleea:** "Access Management is the oldest element of IAM. This pillar is about the infrastructure for authenticating and authorizing users to give them access to a resource. The traditional way to handle this is with passwords. However, passwords can be leaked. The trend nowadays is for multi-factor authentication – that means you need to provide more than one mode of authentication to be granted access – for example, a fingerprint scanner combined with a hardware token. Once an individual has been authenticated, they can be allocated permissions based on their authenticated identity."



*You said the second pillar is Identity Governance & Administration?*

**Ricardo Kowsoleea:** "Yes. Those used to be two different systems: Identity Governance on the one hand, and Identity Management on the other hand. However, the two systems have grown towards each other and we now think of them together as Identity Governance & Administration, or simply IGA."

"Identity Governance has its roots in the days when everyone was thinking about compliance. The new legislation that was issued around that time mandates that companies must be able to show who has access to what, and when, and even why those people need access to specific systems or resources. Managing that manually is complex, to say the least. Identity Governance systems make it possible to automate the task."

"The other side of the coin, Identity Administration, which used to be known as Identity Management, is the infrastructure for automating the joiners, movers, leavers process. When someone new joins the company, their details are entered in the HR system. Then, depending on their role, function, location, etc., the coupled IGA system is used to derive the permissions the new joiner needs. For example, accounts will be configured for Salesforce and Active Directory, Office applications, and potentially hundreds of other resources. The accounts and authorizations are set up automatically and rolled out through the target system. This is something you used to have a whole team of account managers working on manually."

"Another important issue is role tracking: accounts should be automatically updated when the person moves within the organization. If a company doesn't have an IGA system, it can often end up with 'collectors': people who have been working there for a long time, in a number of different jobs, and who have gradually collected up a whole bucketful of permissions that they actually no longer need."

"Then there are a few other things handled by IGA. For example, there's a concept called segregation of duties (SoD). The idea is to require more than one person to complete certain sensitive tasks. For example, someone in the Accounting department might be able to enter an invoice, but not pay it. Lots of companies haven't got this implemented fully at present, but an IGA system provides the necessary framework."

*The third pillar you mentioned was Privileged Access Management. What's the difference between that and your first pillar, Access Management?*

**Ricardo Kowsoleea:** "Privileged accounts are accounts with very extensive permissions. They may be accounts for humans, machines or applications. For example, the root account in a Unix system, or an Administrator account on Windows, are privileged accounts. So are service accounts for providing communication between applications and a database. This kind of account is commonly targeted by cybercriminals, since if

you manage to take over a privileged account, you can penetrate right into the depths of the system. Traditional access management isn't necessarily good enough for these accounts. With Privileged Access Management, you can do things like use rotating passwords for a root account: if someone is working as root, the password will automatically be reset to something new when they log out. That way, even if the password was exposed during the session, a cybercriminal still can't use it to break into the system in a new session."

> *Earlier, you mentioned that companies need to be able to demonstrate why individuals need the access rights they've been allocated. You mentioned separation of duties. Does that mean that IAM isn't just a technical solution – that companies need to think very carefully about the organizational aspects of identity and aspect management?*

**Ricardo Kowsoleea:** "That's right. In IT, we often talk about the 70/30 rule: usually, this means 70% technology, 30% people and processes. But for IAM, that ratio is the other way around: 30% technology, 70% people and processes. Introducing IAM at a company means making changes that people sometimes struggle to get to grips with. At Cegeka, we've been involved with the IAM journeys of large companies with over 100,000 people, and smaller businesses with perhaps just 500 employees. It's not just the technical environment that is different for every organization: the people and processes also need a different approach. Cegeka always works on the basis of close cooperation with its clients – that's the best way to get things right!"

"Here's a simple example: administrators don't like to be monitored! If you implement Privileged Access Management, their sessions will be recorded and/or their activities logged. Auditors can review these sessions to help them understand what system tasks are being done by the administrators. If you don't prepare your administrators for this kind of thing, you're likely to meet resistance during the implementation."

## What are the most important reasons for companies to roll out IAM?

Ricardo Kowsoleea: “Every company has a different problem it needs to solve. There’s no one-size-fits-all reason for organizations to implement IAM. Often, an incident highlights a specific issue, or an audit calls attention to certain shortcomings. When the company comes to us, it’s part of our job to identify the underlying problem and how we can solve it with IAM.”

“IAM is the Swiss Army knife of IT Security: it can do it all. But you don’t have to do it all at once! The first priority is to solve the company’s immediate problem; for example, if a security incident was the trigger for the company coming to us, we start by making sure that no further accounts can be compromised. After that, we can start to look at making the solution more efficient. And that’s the time to draw up an IAM roadmap.”

## What are the current hot topics in the IAM world?

Ricardo Kowsoleea: “Remote access is the big buzzword right now. The Covid pandemic showed people how much of their work can be done from home. But if a company is setting things up for remote work, it needs to provide secure remote access to the relevant company systems. Lots of PAM vendors are currently offering solutions to provide VPN-free secure access to company data for employees, clients, suppliers and third parties.”

“Of course, the compliance legislation hasn’t gone away. Identity Governance remains very important. In fact, more and more companies are getting themselves in a muddle with compliance at the moment – they try and set it up themselves, but eventually realize they don’t have the right skillsets in-house. That’s when they start looking for a vendor who can set up the processes for them, not just deliver the technology.”

## Will IAM evolve into a managed service?

Ricardo Kowsoleea: “Definitely! We’re already expanding our portfolio to include managed IAM services. Our goal is to relieve our clients of having to manage the three pillars of IAM. We want to make it as easy for them as Microsoft 365. They’ll pay a monthly price per user and connect to the system whenever they need it.”

## *Are there other developments you want to tell us about?*

Ricardo Kowsoleea: "Yes: we're finding that along with the transition to SaaS and managed services, the cloud vendors – companies like Microsoft – are bringing out cloud-native IAM solutions. These are interesting options for clients who are moving entirely to the cloud. Another development I'm seeing is that while often IAM vendors used to focus on just one of the three pillars, they're now expanding their portfolios to provide integrated IAM solutions."

## *To finish, can you tell us where IAM fits into Cegeka's cyber resilience story?*

Ricardo Kowsoleea: "One of the reasons that the acquisition of SecurIT by Cegeka was such a positive move is that we've been able to fill a gap in a critical domain in Cegeka's cyber resilience story."

"IAM extends the current portfolio by bringing in the 'Identity' component in each of the cyber resilience domains (see image below). This includes IAM assessment (Assess), tools for managing identities and privileged accounts (Prevent and Recover) and the coupling to SOC services (Detect & Respond). The latter is particularly important as it enables us to actively integrate identity and privileged account monitoring in our Managed Detection & Response service (called C-SOR$^2$C). We've thus been able to compile an extensive portfolio of cybersecurity solutions that we can offer our clients now and in future, based on the combined experience of our own experts and selected strategic suppliers. That way, our clients are free to focus on their core business, securely and efficiently!"

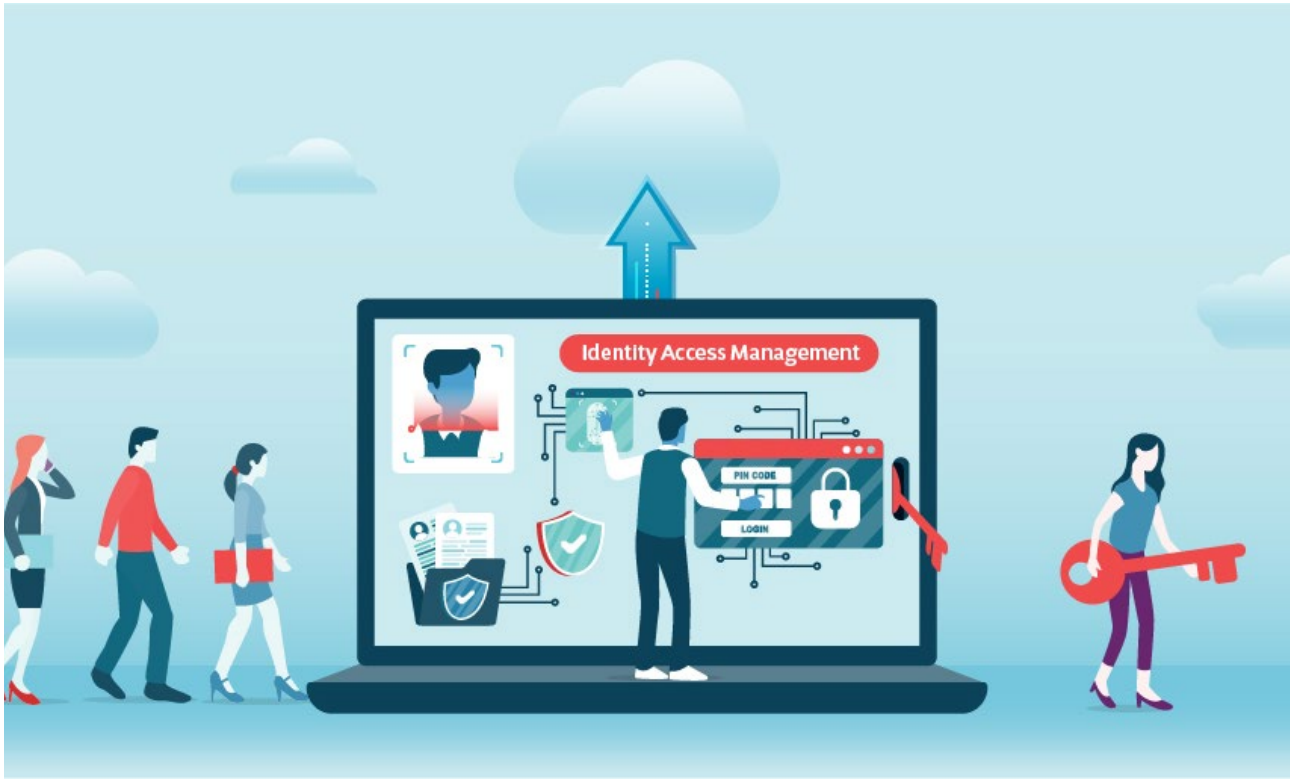
Written by
**Bart Van den Branden,**
**Cegeka Head of Product Management Networking & Security**

# 2

# Four ways in which IAM protects you from security threats

# Four ways in which IAM protects you from security threats

Imagine what a data breach can do to your organization. If your data are stolen or exposed in the public domain, this comes at a big cost. With Identity and Access Management you can prevent a large number of these breaches.




## What is Identity and Access Management?

Identity and Access Management (IAM) is the cornerstone of any organization's security infrastructure. It assigns a digital identity to each employee of the organization and authenticates, authorizes, monitors, and manages those identities throughout their lifecycle. This way you can ensure that users on your network are only able to access the resources that are necessary to perform their duties in your organization.

## Prevent cyber attacks with IAM

These are the four primary ways in which IAM protects your organization from security threats and vulnerabilities:

- **Automate provisioning of access privileges**

  Manually assigning access rights to new employees is a costly, inefficient, and error-prone practice. Identity and Access Management automates this process of assigning privileges to new employees, depending on their roles. And

when an employee moves to another department or gets another job role, the automated enforcement stops the issuance of unnecessary privileges and limits the privileges to the ones needed for the new job. Finally, IAM ensures that employees who are leaving the organization have all their privileges revoked automatically.

- **Tighten privileged account security**

  Privileged accounts are especially interesting targets for cyber criminals. If they can compromise such an account, they get broad access rights. This gives them access to a lot of resources and data, potentially to almost every part of your organization's systems. Moreover, it can take months or even years before an account compromise is detected.

  That's why you should prioritize privileged accounts as part of your IAM strategy. If you start implementing IAM with these users, your efforts immediately pay off the most because you lower the risks significantly. Passwords alone aren't enough to safeguard privileged accounts, as passwords can be stolen by social engineering or phishing. Multi-factor authentication is a must for these accounts.

- **Remove orphan accounts**

  Orphan accounts refer to inactive accounts: those that users are no longer using or actively managing. Every account on your systems is a possible security hole, so cyber criminals can compromise these for their fraudulent activities. That's why orphan accounts must be removed from your systems. Identity and Access Management services will routinely scan for idle accounts in your organization and notify you about their existence. This way you can limit the number of accounts, users, employees, and guests with access to your data, tools, and systems.


*"Passwords alone aren't enough to safeguard privileged accounts, as passwords can be stolen by social engineering or phishing. Multi-factor authentication is a must for these accounts."*

- **Use multi-factor authentication**

  If your password is the only defense between cyber criminals and your crucial business data, then you've lost. Passwords can and will be guessed, cracked, intercepted, or stolen by social engineering or phishing. That's why we always recommend multi-factor authentication (MFA), regardless of your organization's size, industry, or data. With MFA you can stay in the fight.

  Multi-factor authentication adds extra layers of security for users and their accounts. This means that your system will request another security credential every time a user wants to access it. This can be a code delivered as a text message to your phone or in an email, a code generated by a mobile app or a hardware security key, or it can be an extra biometric authentication step, for instance with a fingerprint scanner on your phone or laptop. This additional step significantly reduces the risks of unauthorized access to your systems, as the perpetrator now needs both your password and access to your email or mobile phone to continue.

## Protect your data with Identity and Access Management

We already said it in the beginning, but it is worth repeating: Identity and Access Management is the cornerstone of any organization's security infrastructure. A sound IAM strategy, coupled with knowledgeable service team members, the right IAM solutions and dedicated management, will be able to reduce the chance of a data breach in your organization.

Written by
**Jorrit Klarenbeek**
**Cegeka Identity Acess Management Architect**

**Reduce Cybersecurity Risks**

EBOOK

DOWNLOAD

3

# Identity Governance and Administration (IGA) technology helps tackle more than identity and access challenges

# Identity Governance and Administration (IGA) technology helps tackle more than identity and access challenges

Your workforce constantly evolves... People joining, moving internally or leaving your organization. This evolution continuously poses challenges from a security point of view. As your organization evolves, you need to keep up with access rights to various resources to various resources like applications, data, portals, databases on-premise and in the cloud.


The way you organize, monitor, manage and report the user access to these various resources while meeting audit and compliance requirements is what is Identity Governance and Administration (IGA) all about.

## Necessary but not a necessary evil

IGA technology is key to manage identity and access across your organization. It will enforce that the right people get the right access to the right resources at the right time for the right reasons.

There are more advantages to IGA technology than just the ease of identity access management.

- It will ease compliancy, using central reporting of access across your organization

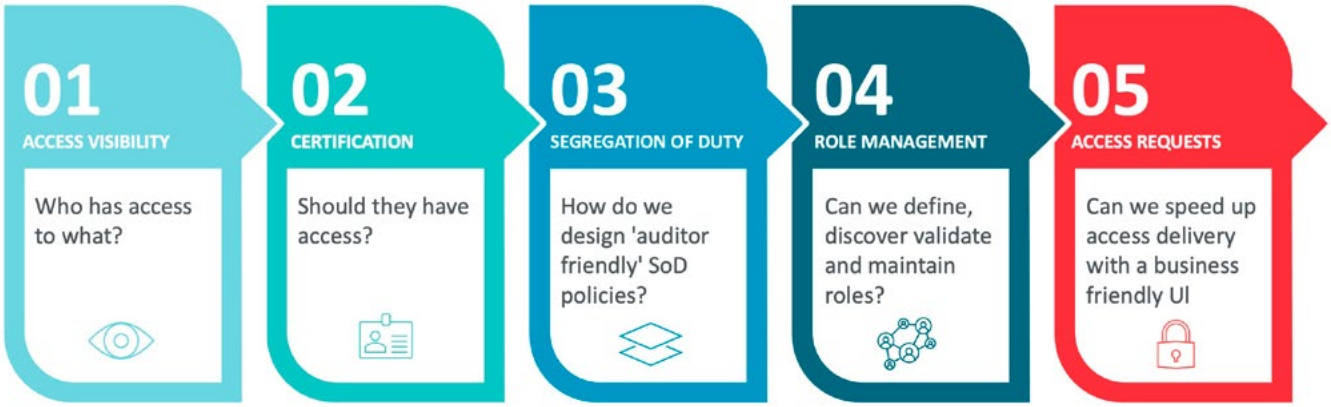
- It will also enable you to enforce ‘least privilege’ and ‘need to know’ principles by only granting the authorizations that are required and approved.
- By automating processes as much as possible, less staff is needed to execute authorization requests, reset passwords and deliver reports.
- Due to the link with “authoritative” sources (for example an HR system), the access to resources is in sync with employees that are active within your organization.
- It ensures that employees are onboarded faster, have the right access in their new role and are enabled from day 1.

## What are you risking?

An IGA system has tools which provide an organization insight into IT risks.

- Certification is a process in which a manager or application owner revises, revokes or confirms the authorizations of employees at regular intervals
- Classification of resources provides insight into which risk is associated with a resource, and which employees have privileged access to critical resources.
- Segregation of Duty identifies combinations of authorizations that may pose risks. For example an employee who can approve his own expense notes

These tools are needed to shift from functionality and efficiency (managing access) to mitigating corporate risk. This will increase the awareness in the organization related to identity and access management.



## Rome wasn't built in a day

Implementing IGA is a process where the organization will mature together with a growing awareness of identities and access. This is not a one-off project, it's rather an evolution. An organization must go through different stages of the IGA best practice approach to have fully implemented functionalities of IGA.

## The right access to the right resource

As your organization evolves, you need to keep up with the access to all resources. IGA helps you to enforce that the right people get the right access to the right resources at the right time for the right reasons. The system will provide the organization with insights into IT risks. Implementing IGA is not one-off project, rather an evolution. IGA is fundamental for compliancy, avoiding labor intensive tasks and reducing business risks and helps you to get in control of IAM.

Written by
**Bart Van den Branden,**
**Cegeka Head of Product Management**
**Networking & Security**

WWW.CEGEKA.COM