Conclusion of iC Consult's Pit Stop #1: Identity Governance and Administration

Presented during the iC Consult IAM Pit Stop Series

Pit Stop #1: IGA

The IAM Pit Stop Series is iC Consult's new digital expert roundtable format. It provides deep insights into emerging industry trends and practical advice for IAM experts and C-levels alike. Each Pit Stop session focuses on a specific topic which is presented from exciting new perspectives.

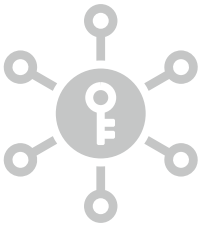
The first session's topic was Identity Governance and Administration (IGA).

Andre Priebe, global CTO of iC Consult, took the stage first. In his opening presentation "Hypes and Trends and Digital Identities", he reported on the most relevant developments in the IGA sector.

Jonathan Edwards, Vice President of Strategy & Consulting at iC Consult, spoke on "The Evolution of Access Certifications," explaining how access credential validation has changed over time and how a process validation model could change the certification validation.

Jackie Rotchwolski, Head of Identity and Access Management and Security Engineering at Mass Mutual, concluded the session by presenting their journey towards a process validation model and the challenges they faced.

Content



Key Insights from the Pit Stop Session

1. OpenID Connect is here to stay

OpenID Connect is not a new technology, but it has been gaining a lot of traction due to a recent paradigm shift: The responsibility for managing identity proofing processes is shifting from individual business applications to a centralized identity access management system. The benefits are obvious: Identity proofing becomes much more cost-effective and robust due to multiple uses of the same data, and centralized management greatly improves the user experience.

Therefore, more and more enterprises are focusing on centralized IAM solutions, and a lot of this is happening around the OpenID protocol. The core idea is to extend the information shared by OpenID Connect with a verified claims object that could provide additional information about which trust framework was used. It is likely that this will include, for example, regulatory requirements such as money laundering laws, detailed information about the type of verification (physical or digital), the organizations involved, and documentation of the documents verified.

While the final protocol definition has not been published yet, OpenID Connect promises to make the exchange of identity-related information much more efficient and ID verification much more robust and secure in an era of increasing threats.

2. Bring your own Identity & IAM as a Service will shape the future of IAM

According to recent Gartner recommendations, organizations looking to improve their IGA processes should keep an eye on the trends “Bring your own Identity” and “IAM as a service”. In both cases, Microsoft is crystallizing as one of the key players, as it can provide both identity and rich business capabilities – and most enterprises have already migrated to Office 365 or M365 anyway. But how can you leverage this along with your existing IAM solution?

Typically, you have an identity provider who takes care of processes like authentication, authorization, and so on – and an IGA provider who takes care of the ID lifecycle, roles, and privileges, among other things. And since both areas cover an increasing number of employee, partner, and customer identities, combining all this in one solution is becoming both more attractive but also more difficult.

Microsoft and Active Directory can help you to leverage the already strong identities that Microsoft provides for their applications. One of the most exciting capabilities in this context is the „guest invitation feature“ which allows users to invite guests or team members based on policy to collaborate in a very efficient way. For example, companies looking to invite external guests to their work environments can simply use their external mail address – which, usually, is already known to Microsoft because the invitees are also using M365 in some way.

This is the foundation for the innovative Federation feature that comes for free with Microsoft Tenant and allows organizations to connect to thousands of companies on a large scale. Obviously, this will require Microsoft Azure to integrate strong IGA tools first, to fully understand, which guests are out there, to maintain control over the invitation process, to be able to prove guest identities, and to define clear rules about

what types of guests should be allowed. Organizations should take a close look at the capabilities and the hazards and consult knowledgeable experts.

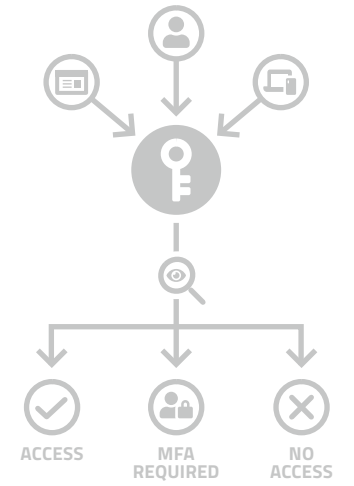
3. Zero Trust & Identity Risk Management are shaping enterprise architectures

Zero Trust is one of the topics that is already in the late phase of the Gartner Hype Cycle and is now widely known in the IT world. However, there are some challenges in implementing this approach:

- **Complex policy management**
  Policy management is becoming increasingly complex as organizations seek to incorporate more information and dynamic threat intel into their access decisions. The decision-making processes need to be carefully defined e.g., to avoid a specific type of device getting blocked with a severe impact on partners and suppliers.

- **Management of policy enforcement points**
  The second major challenge is policy enforcement: It needs to guide access to all resources, to support multiple protocols and architectures, and to interact with a variety of different technologies – all while being tailored to protect that one specific resource. This is very difficult.

- **Lack of visibility**
  And there's an even bigger problem: We can only protect what we see. If we don't know about a resource, we can't set a policy enforcement point. This is why visibility and transparency are paramount and have to cover all assets. Even those that really shouldn't exist – like an Excel sheet with critical account and password information.



The solution: Comprehensive identity risk management
There are two ways to reduce the potential risk to an organization: You can reduce the likelihood of a successful attack with technologies like multi-factor authentication. Or you can minimize the impact of a successful attack with technologies like Zero Trust. Ideally, both types of measures should be combined to adjust the risk level to match the organization's risk appetite.

A comprehensive identity risk management should cover the following areas:

Organizations should identify their most critical users via **Identity Risk Scoring** based on their IGA framework and implement additional layers of protection for them, for example by providing each of them with additional authentication factors.

They should also analyze the technical interfaces from an attacker's perspective to perform what is called an **Identity Risk Discovery.** There are very intelligent tools available for this, which help to enforce particularly strict authentication processes for specific groups. With this path analysis, companies are also likely to identify any high-risk accounts not on the original list.

A third aspect is **Identity Threat Monitoring (ITM)** which focuses on specific identity-related threats. Seeing that in the world of Zero Trust identities are becoming the new perimeter, this tool is becoming increasingly important to reduce the probability of an identity-based attack.

Another fairly new technology is **Cloud Infrastructure Entitlement Management (CIEM),** allowing companies to transparently analyze which cloud resources they own and which accounts and permissions can access them. Microsoft is already investing heavily in this technology, turning it into a key component for Azure, but also for AWS and GCP resources.

When these new identity risk management tools are combined with traditional tools, the likelihood of an account being taken over can be significantly reduced, as can the impact of a successful attack.

4. Micro Segmentation is alive and kicking

Micro-segmentation gets often overlooked when speaking about zero-trust architectures, as most applications in modern environments run on Kubernetes or Docker and the traditional DMZ seems to be a thing of the past. But Micro Segmentation is far from dead: There are several new, smart, and exciting approaches to it.

One of the more innovative Micro Segmentation approaches is to simply assign a simple, easy-to-understand label to each system. For example, a database in the development phase might be labeled as „development". Similarly, another system will be labeled „logging", and there will be a very large area labeled „Internet." Once these labels have been assigned, it becomes possible to formulate very robust policies in a very natural language. Thus, despite its simplicity compared to traditional TCP/IP-based firewalls, this approach solves most of the challenges of micro-segmentation in Zero Trust architectures. It is also very dynamic and can be easily combined with strong identity-centric approaches and is not limited to virtual machines or bare metal boards but provides a powerful tool for dealing with container environments.

A long-term challenge will be to find the right number of tags for your environment – not too many, to keep complexity low, but enough for any tasks at hand – and to use them to drastically reduce the number of policies. When all is said and done, this model should pave the way for simple and concise rule sets that are easy to understand and easy to verify.

5. The "Process Validation Model" promises to shake up IGA

The process validation model is fairly new and has not yet arrived in all organizations. The idea behind it is that organizations should be able to fully define their lifecycle management and access request processes and, as they mature, introduce additional processes to verify that these provisioning, deprovisioning and request processes are still working as intended.

Any changes made to these processes or policies will be added to a change control process and reviewed by a Change Advisory Board (CAB) before they are practically applied. This requires a major change in company culture, but it also eliminates burdensome, manual, and error-prone Access Certification reviews and allows all the automated management of access rights from a single location – a great opportunity for a comprehensive upgrade of the identity program.

For example, companies can use the new model to drastically reduce their technical

debt. They can also review their identity stack and determine if they really need their legacy IGA solution or if their access management solution still meets all needs. This will pave the way for open and repeatable standards like OIDC, JIT or token-based authorization and open the doors for greater flexibility and agility. It also allows organizations to return the ownership of identities to the user, making it much easier to manage personal data and to ensure compliance with regulatory requirements.

In short, the process validation model is a powerful tool to replace costly verification tasks, and to focus on the higher-level processes instead.

6. Conclusion

There are many reasons why robust, identity-centric security mechanisms are in high demand today. Organizations need to establish comprehensive identity risk management frameworks and to proactively embrace innovative trends and technologies such as OpenID Connect, Identity Federation and CIEM to prevent dangerous and costly identity attacks. It is also worthwhile to look at access authorization validation at the process level which promises to dramatically increase the operational efficiency and the security posture. iC Consult is here to help you evaluate the new trends and technologies, and to show you how to unlock their full potential for your organization.

About iC Consult

The iC Consult Group, headquartered in Munich, Germany, is the world's leading independent advisory, systems integrator, and services provider for Identity & Access Management (IAM). The service portfolio covers advisory, architecture, design, implementation, and integration to IAM managed services and identity as a service offerings. The company's more than 650 employees have successfully delivered over 3,000 projects and managed services for IAM. The iC Consult Group, with its affiliates iC Consult, SecureITsource, xdi360, IAM Worx and Service Layers, has offices in Germany, Switzerland, Austria, Spain, Bulgaria, the UK, the U.S., Canada, and China.

More information at www.ic-consult.com