The Evolution of Access Certifications

Jonathan Edwards
Vice President of Strategy & Consulting at iC Consult

Presented during the iC Consult IAM Pit Stop Series

Pit Stop #1: IGA

Identity governance and especially the practice of Access Certification has been changing dynamically over the past years, always trying to keep up pace with state of the art Identity and Access Management (IAM). In his presentation at the first IAM Pit Stop meeting, Jonathan Edwards, Vice President of Strategy & Consulting at iC Consult, analyzed the evolution of Access Certifications over time and gave a thought provoking future outlook, discussing disruptive theories and models. Where is the journey of Access Certifications heading? And will we still need them in future? Join us on this evolutionary journey!

It is widely known that establishing strong identities and consistent access management programs is not a one-time project. It is a journey. And along that journey, you will always notice aspects that you could improve on. The same is true for Identity Governance: Once you decide to implement and mature a dedicated IGA program, you are in for the long run. Identity governance is an umbrella term which brings together a wide variety of aspects, from standards to controls to the automation required to enforce these standards. However, it is important to always keep the future in mind and act with foresight. After all, there is no point in initiating an IGA journey that is outdated by the time you reach your destination (as far as that is even possible in this context).

With all of this in mind, Access Certifications are the true backbone of governance. Automation is a tremendous help and the result of excellent governance practices, but without working validations, you'll be hard pressed to even prove that a program has been successfully implemented. Let's take a look at what Access Certifications are and where they come from.

Content

The Definition of Access Certifications

An Access Certification is a periodic check of the authorization and access rights for a particular account. This task is usually assigned to either a user's direct supervisor or an application owner who is aware of the permissions.

In order to protect your organization, the auditor must ensure that an account's access privileges are not more extensive than necessary to perform the job at hand. This is why, as a vital part of the audit, necessary access should be confirmed, and unnecessary rights must be revoked.

Depending on the application, these reviews are usually performed quarterly or annually. Alternatively, they can also happen ad-hoc, depending on the company's internal and external audit requirements.

Why Are Access Certifications So Important?

The relevance of the topic becomes apparent when several aspects are considered:

Aspect 1: Reduced risk of security breaches
Access audits help organizations mitigate the risk of a security breach.

Malicious actors keep on trying to gain access to organizations' accounts. Therefore organizations are generally well advised to act as if someone had already gained access to their network. By verifying access constantly, companies can ensure that all accounts have only the access rights they need. This will make it more difficult for malicious actors to move laterally through the corporate network to gain additional privileges – and thus protect sensitive information.

It will also put a stop to internal fraud. Example: If users can access the creation and approval of orders or to personal customer data, they could use these for illegal activities that harm the company or its customers.

Aspect 2: Compliance with audit requirements
A second major aspect is audit compliance. In many, if not most industries, there is some form of regulation that companies must comply with to be allowed to operate in that space. Prime examples are SOX, HIPAA, Hi-Trust, ISO, or GDPR. To meet these compliance requirements, organizations have to document that their access rights have been validated. Failure to do so can result in significant fines – SOX violations alone can cost up to $100,000 per month.

Even more important than the financial penalty, however, is that non-compliance can and will damage your image. This will make it very difficult to operate in certain industries – and that, in turn, can damage a company's credit rating and inhibit its ability to successfully engage in Mergers & Acquisitions.

The biggest problem, however, is the loss of trust. Once lost, customers' and partners' trust is difficult to regain, and bad reputation or bad press can prove devastating. This is particularly true for listed companies where a loss of trust will inevitably result in a loss of market value.

Access Certifications are a great tool to ensure that all audit requirements have been met, and to minimize the risk of security breaches.

And finally, regular Access Certifications support other key processes:

- Elimination of obviously unnecessary privileges from escalated accounts
- Elimination of unused privileges
- Ensuring repeatability of access granted to a user

The benefits of strong governance and robust access certification processes are obvious. On the other hand, this is an ambitious and daunting project and we definitely recommend to have a close look at the history of Access Certifications to fully understand the implications and the directions it can take.

The Evolution of Access Certifications

The design and the variety of applications, networks and infrastructures have all changed dramatically over the past decades, and the handling of Access Certifications has changed with them.

In the past: a cluttered and decentralized picture

IT Organizations used to be decentralized, and each application had its own administrators responsible for providing access. Typically, the process started with an email request or a help desk ticket. The administrators were also responsible for defining access guidelines for each of their applications. And since each application had its own rules and standards, it was almost impossible to compare (not to mention correlate) account handling between several applications.

Administrators usually granted access rights based on other employees in the same department, or simply copied access templates from one account to another. When a user changed departments or was promoted to a new position, the access they needed for their new role was simply added to their existing access.

No validation, or limited validation, was performed. The only time access was validated was when an incident occurred – something that made the administrator question a user's or user group's access. And if a user left the company or was terminated, it was the sole responsibility of HR or the direct supervisor to tell the application team that that user's access needed to be removed as well. In short, a lot of human interaction was needed, and that's where a lot of things went wrong.

For example, there were a lot of orphaned accounts or accounts where access was only partially removed. A typical scenario would be that a supervisor deleted access to all applications they knew about. But they had no knowledge of the employee's previous department's applications, and thus, these rights stayed in place and offered malicious or internal users the opportunity to access sensitive information.

To deal with the abundance of dead permissions, we saw the first organizations implement an annual access review process. However, it was usually the responsibility of the administrator to make these decisions based on their own institutional knowledge, and the handling of access rights was very subjective and inconsistent, often even depended on the user's relationship with the administrator (e.g., if the admin was afraid to take his bosses rights because he feared repercussions).

In the end, it was mostly the administrator's personal decision to validate and remove access – and not yet in line with any actual policies and procedures.

The next step: manual validation

Once companies realized that validating access was critical, they started to conduct regular audits. Security teams were put in place and helped to create company-wide standards for the first time. However, there was still no centralized location where access could be viewed and managed. When validating access, the application owners had to create long reports that included all user and their access rights for all applications.

These reports were usually printed spreadsheets, sent to the responsible party for review. The reviewer would then manually approve or disapprove the access rights on the report, and return the report to the application team to have their decision executed.

This was a lengthy process. It could take weeks, even months, to create the reports, categorize them, make sure they went to the right person – and then have the access validated by that person. Then, the reports had to travel back to the application team which might have to revoke access. Due to the long timeline, by the time they were executed the reviews were often outdated and no longer valid. In addition, this process was prone to human error and often inaccurate, with many inconsistencies between the spreadsheets and the actual system.

Centralization

With the spreadsheet model being very difficult to use and security teams becoming less and less confident in the results of certifications, organizations realized that they needed to implement a dedicated Identity and Access Management solution – one that included an IGA component or a governance and access component. These applications take time to implement and onboard. But implemented correctly, they promise to deliver full enterprise-wide visibility across user permissions in the application ecosystem.

There are some limitations, though: Auditors usually only see the accounts and the permissions associated with them, but don't know the exact access rights associated with individual entitlements. The rights themselves don't have descriptive names, don't contain descriptions, and there is no standard naming convention for them – so the reviewers often don't even know what they are approving or reviewing.

But at least reviewers now have a central place to check all accounts and the associated authorizations. The situation has become a bit less confusing – and there is also a clear audit trail for the approval process that provides additional guidance. In addition, auditors now know where all the authorization data is stored and do not have to go to great lengths to find it.

And yet: IGA is still a time-consuming process. As a result, auditors might put their stamp of approval on certain decisions without evaluating the rights on an individual basis, but simply following subjective patterns, e.g., by greenlighting access for all members of the same team without questioning the individual authorizations.

And another issue mentioned above remains: Due to time consuming processes, authorizations might already be outdated by the time of the check, as new authorizations have already been added or old ones removed. For example, an employee may have

changed positions in the company in the meantime and have a completely different set of authorizations then. There are even multiple cases where users have switched roles from employee to contractor – and should have received completely new access rights in the new role. However, their access rights were validated with the original role in mind, presenting a significant risk to the organization.

While this criticism is certainly valid, here is no doubt that a centralized IGA approach offers many tangible benefits, from the automated removal of outdated rights to the noticeable reduction of operating costs through the more efficient processes.

The introduction of role-based access certification (RBAC)

As organizations have matured, they have begun to define new roles. These roles can be based on business and technical functions, on department and office affiliation, or even on the location, in which an employee resides, and all come with a predefined set of access rights.

Long before true Identity and Access Management came along, roles were an important part of rights management, e.g., in ERP solutions such as SAP or Peoplesoft. With the introduction of an enterprise RBAC model (where roles tend to have more detailed descriptions), it became much easier for auditors to review the roles associated with an account and to make more informed decisions.

Today, auditors tend not to compare individual accounts anymore. Instead, they are more likely to review the roles associated with each account. That way, they still have to review all of their employees, but at least it's moving in the right direction, as they don't have to make a direct comparison, but can make informed decisions based on detailed information.

There also needs to be some sort of validation process in place to verify that roles are being managed by the correct role owner. Even if the approver manages or validates role X, someone in the background needs to verify that it is indeed the right role and that it is updated and maintained throughout the year.

A potential risk in this scenario is that the reviewers don't necessarily understand all the roles or permissions and don't know which ones might be risky to the organization. They make their decisions based on the information provided within the role, such as the role name or the description shared by the role owner. But there is no way for them to understand the risks associated with this role compared to another role.

State of the Art

This brings us to what organizations consider mature today. To reduce the number of certifications that auditors need to perform, companies have understood that it is not necessary to validate all access rights or roles. Roles such as birth rights, or accesses and roles that do not pose a risk to the organization, do not need to be validated.

When permissions are created (or added or updated) today, they have a level of risk associated with them – and this level of risk determines if and how often the access needs to be validated. If a user's access represents no or low risk, there is no reason to review their rights. On the other hand, the rights of high-risk users with administrative privileges should be checked more frequently. And as always, there are some exceptions: For example, if a user requests or receives non-default access, those permissions or roles should also be added to the periodic review process.

This is what we consider a mature process. But it still involves some counterintuitive developments: Repetitive reviews are supposed to improve the security standing. But the repetitiveness tends to tire the reviewer, and that increases the likelihood that access will simply be signed off. This is especially true for contractors and administrators who are assigned the same access rights over and over again: Their supervisor sees their name come up again and again, and it's becoming very easy to just greenlight them based on familiarity.

What Is the Future? What's Next?

Today, we are seeing organizations move to what we call a "process validation model". This is a fairly new model, but more and more security teams are increasingly engaging with it. It's based on the idea that organizations are fully defining their lifecycle management and access request processes – and as they mature, they are introducing additional processes to validate these provisioning, deprovisioning and request processes, too.

Any changes they make to their processes or policies are added to a dedicated Change Control Process. They must be pre-reviewed by a Change Advisory Board (CAB) or CAB Review before they are implemented in the organization.

This is a huge culture change, as it eliminates some of the direct access changes in each application. For example, native changes in Active Directory or in Salesforce are all managed from a single place through automation, and then validated downstream. This now allows organizations to take their identity program to a whole new level.

For example, they can use it to reduce their technical debt. They can also review their identity stack and determine if they really need an IGA solution or if their access management solution can meet their needs. And they can focus on developing open and repeatable standards like OIDC, JIT or token-based authorization. This opens the doors for more flexibility and agility.

The model also allows organizations to focus on the policies and procedures needed to grant and manage access. They can return ownership of the identities to the user, and make it much easier to manage personal data within the organization and to mitigate the risk of compliance violations.

Even though access certifications will always remain a necessity, especially for legacy applications, the process validation model opens the door for pure SaaS or microservices infrastructures. The goal is to reduce the burden on security and to seamlessly provide services and applications for employees or customers, while improving the user experience for all identities. If organizations focus on the process – and keep on validating that process and how it works – you won't have to spend users' time reviewing access that you know is properly provisioned and managed. However, as mentioned earlier, this concept is still very new and is just starting to catch on in the identity industry and among some auditors. In audits, this strategy has already been well received because it allows organizations to accurately demonstrate that their access management processes are working.

Conclusion

The methodology for verifying and certifying access to a network and its applications has changed considerably over time. It has become apparent that, for example, changes have been made for usability or security reasons, and new processes or ways of working have been introduced. The process validation model is a strong method to move away from the time-consuming verification of individual authorizations and to focus on the higher, process-oriented level. However, this requires organizations to fully define their lifecycle management and access request processes as they mature, and to introduce additional processes to validate their provisioning, deprovisioning and request processes. The effort required to implement this solution will quickly pay dividends and can significantly improve an organizations security standing.

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 600 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