SonicBee

Identifying the stakeholders in Access Governance

Published February 2022, SonicBee, André Koot

Connecting data and identities, growing business!

Abstract

Identity and Access Management (in short IAM) is a well-known topic in the domain of information security. Though it may be well known, that does not mean that it is well understood. Most IAM projects are defined as IT projects, caring about provisioning users via an onboarding process and deprovisioning them when they leave the organization. And after creating accounts for employees and customers, authorizations are granted, based on the role or position of a person. *And this is where things can go wrong. The big question is who is accountable for granting authorizations to employees, customers, or business partners. Or granting authorization to things (or non-human entities?)* for that matter. The problem is that organizations do not know, or these organizations neglect the accountability of several relevant stakeholders. The **wrong people** are made responsible for granting access to resources, systems, files, services.

This is where Access Governance comes into play. And therefore, we need to explain what types of stakeholders must be involved in access control decisions. Without defining the right accountability for access control decisions, an organization simply is not in control. The access governance model introduced in this article enables an organization to clearly identify what access decisions have been made and who is accountable for those decisions.

*This article touches on the needs for access governance, the challenges, and a focus on the various stakehol*ders in an organization responsible for setting up governance over access control decisions.

Table of Contents

ABSTRACT **2**

INTRODUCTION TO ACCESS GOVERNANCE **4**

Terminology 5

CHALLENGES FOR ACCESS GOVERNANCE STAKEHOLDERS **6**

Access Governance Philosophy 7

IDENTIFICATION OF KEY STAKEHOLDERS **9**

Line of Business 9
Process Owners 9
System Resource Owners 10
Data Owners 11
IT Owners 11
Relationships Between Stakeholders 11
Accountability 12

PRACTICAL IMPLICATIONS: ROLES AND GROUPS **13**

BRINGING IT ALL TOGETHER: ACCESS GOVERNANCE GOOD PRACTICES **14**

COLOFON **16**

Author Bio 16
References 16
Acknowledgments 17

Introduction to Access Governance

In every organization, people work together to realize the goals of that organization. Distribution of tasks to employees, based on their experience, certifications, competences, is done to maximize the effectiveness and efficiency of the organization. As an organization grows, the need for control rises. In a small workshop, the owner is responsible for performing every task and when the workshop grows, the owner will delegate tasks to other personnel, while still being accountable for the work done. Responsibility for the executing of tasks can be delegated, but accountability stays with the owner. And as such, the owner will implement controls to be able to be in control. Controls such as segregation of duties and 2-person control (or the four-eyes principle), to compensate for the lack of the owner being present all the time and watching over all performances.

These days people work with information in information systems and services. The lack of physical eye control cannot be ignored: implementing access controls is more important than ever, especially since a work location may not be a physical location anymore. Offices are global entities; the processing of tasks is cloud based and so the controls must change.

When organizations grow, or when they are active in specific industries, there are more stakeholders than only the owner and the employees. Shareholders, supervisory agencies, tax departments, consumers etc. also need the assurance that an organization is in control, and that an Enron-sized scandal[1] is not about to happen. “Who can have access to What and Why that is okay”, needs to be embedded in an organization. Governance is the keyword for that. The concept of Accountability does not change. Someone is still accountable; someone is still the Owner of the accountability problem.

Identity and Access Management, in short IAM, is often seen as the solution for this problem and the IT department is made responsible for solving the problem by implementing IAM. But then organizations usually make a big mistake. The IT department cannot be held accountable for solving the problem. IAM is not a responsibility of ICT, but of the business.

Even then the problem cannot be easily solved: who in the business should be held accountable? There are so many stakeholders, each with their own tasks, responsibilities, and mandates. Who can make an access control decision? Who can grant authorizations, or grant a role with entitlements to another person? This is where the concept of Access Governance can come to the rescue.

Access governance is the organization-wide control mechanism that sets the policies (e.g., decision criteria) and procedures for managing access to systems, services, and data. It requires business owners to define and accept accountability for access to protected resources such as an application, a database, or a document repository. For example, the business must answer critical questions, such as:

- Which users should have access to what resource?
- What are the minimum privileges necessary for an individual to complete required tasks?
- For how long should access be valid?
- Who should have oversight over the access granted to protected (of business critical?) resources?

Answering the question ‘Who is permitted access to specific resources’ is especially important. It is not always clear who decides an access policy or manages the necessary granular security levels protecting an organization’s critical information assets. The stakeholders involved in access governance must be clearly defined; they are responsible for all decisions regarding why access is granted to specific individuals or roles.

The access governance model introduced in this article enables an organization to clearly identify what access decisions have been made and who is accountable for those decisions. This model also allows the organization to identify where responsibility for access decisions is lacking. This accountability is essential for an organization to be ‘in control.’ Suppose other stakeholders (such as customers or employees) and supervisory agents do not have the assurance of good practicing. In that case, the organization's business value may drop because of a lack of transparency and trustworthiness.

Assigning and enforcing accountability explicitly is essential when more than a few stakeholders are accountable for access decisions. When there is only one individual filling the various stakeholder roles, such as in a Small or Medium Enterprise (SME), accountability for assigning access permissions typically lies with this single owner. But for larger organizations, separating responsibilities is good practice when multiple people can be made accountable for access decisions. Whereby for most industries it is even mandatory to separate responsibilities about access decisions to achieve compliance in this area.

Access Governance is a globally valid control mechanism, and the policies and processes for managing access should be clear. The question of why permissions are granted should be easy to answer, and each stakeholder should know their role in the process.

Terminology used

- Access Governance is the organization-wide control mechanism that sets the policies (e.g., decision criteria) and different procedures for managing access to systems, services, and data.
- The Data Owner is responsible for data quality and maintaining compliance with legislation and regulations on behalf of an organization.
- The Line Manager is a hierarchical manager responsible for the operations of an organizational unit. A Line Manager determines which employee can or may perform a task and assigns them to tasks within the business processes.
- The System Recourse Owner is responsible for a business system and determines which users should have access to it. System Owners deploy information systems and services that are used within the primary business processes.
- The Business Process Owner is responsible for setting up and maintaining processes and determining the quality criteria relative to the process's input and output.
- CIA Rating (Confidentiality, Integrity, and Availability) results from a risk analysis, or Business Impact Analysis, of business processes and data. A high level of risk (as seen in the different values for CIA) must result in more (and therefore mostly more costly) security controls than when the risk level is perceived as low or moderate.
- The Head of IT is the person who oversees all IT components, such as servers, PCs, networks, and mobile devices. These components are used to host information systems and support data storage and transfers
- Segregation of Duties (SoD or separation of duties) is the internal control principle that disallows a single individual to perform a functional task and its control task, e.g., entering an invoice in a Financial Management System and approving its payment (also called conflicting tasks or a ‘toxic’ combination of tasks).
- The Sarbanes-Oxley Act (SOx) is a US corporate governance law regulating public company accounting practices and instituting Investor Protection.
- Role-Based Access Control (RBAC) is an access control method for granting authorizations to people based on their roles.
- Attribute-Based Access Control (ABAC) is an access control method for granting authorizations to people utilizing one or more of their user attributes.
- Policy-Based Access Control (PBAC) is an access control method for granting authorizations to access requesters, if they comply with the access policy.

Challenges for Access Governance Stakeholders

In any area where protection of information is a concern, the core questions that define the security of that information are:

- *What* is the resource in question?
- *Who* is granted access to the resource?
- *Why* are they given the right to do so?

Being able to answer these questions easily supports proper organizational risk management and improves engagement with security consultants and auditors whose audit findings often address authorization management. Each stakeholder needs to be able to answer these questions in their area of responsibility.

The questions of 'Who, What, and Why' have profound implications. Access decisions around information systems are often broader than just Yes or No. Different actions can be performed, such as reading, updating, or deleting information, but there are also differences in competencies that further refine access levels. For instance: a 'junior' sales manager will typically have fewer permissions than a 'senior' sales manager. They may have the same business functions, but a senior employee might handle large customer accounts, and a junior may only be allowed to manage small accounts.

Complex access control environments make an organization's ability to answer the 'Who, What, and Why' questions quite challenging. One widespread problem found in organizations of any size is individuals being granted too many authorizations. These individuals may have been given access rights because they are long-term employees or an immediate, short-term need caused by a person's absence. These uncontrolled entitlements, as understandable as they are at the moment, lead to an increased risk of data breaches. Another frequent problem involves the ongoing tension between convenience and security. In an organization that enforces Segregation of Duties (SoD), employees may find the ease with which they expect to work is interrupted by multiple approval requests. They may then request, and be granted, broader permissions that will allow them to complete their task without interruption. However convenient this way of working may be, it breaks the security controls that have been put in place and exposes the organization to vulnerabilities.

Given the complexities of modern IT environments, determining which users are to be given access to a resource can be challenging and may involve multiple stakeholders. It requires the business C-level officers to assign ownership and accountability for access decisions. Ownership and accountability are key to control and governance.

Of course, other "W's" are When, Where, What device, What condition. These W's can be considered as part of the Why question, they are all part of the access policy (based on risk appetite) of the process owner. The access policy (whether we're looking at role-based access control (RBAC), attribute-based access control (ABAC) or policy-based access control (PBAC) should make it possible to evaluate these different attributes or conditions.

Access Governance Philosophy

We developed an access governance model that is built around the concept of establishing accountability for access control decisions and assigning accountability to the appropriate stakeholders in the organization. Stakeholders are individuals who hold organizational roles and who are in some way responsible for the assets being protected through access management. For instance, the person who holds the role of Finance Manager will be the stakeholder in access management for the finance business processes.

In larger organizations, roles may be distributed between multiple organizational units, and these stakeholders may have relationships with each other. This can be more complex in a matrix-management organization in which cross-functional responsibility for a protected resource may span multiple hierarchical structures.

The relationships between diverse types of stakeholders in the access governance model can be expressed visually:

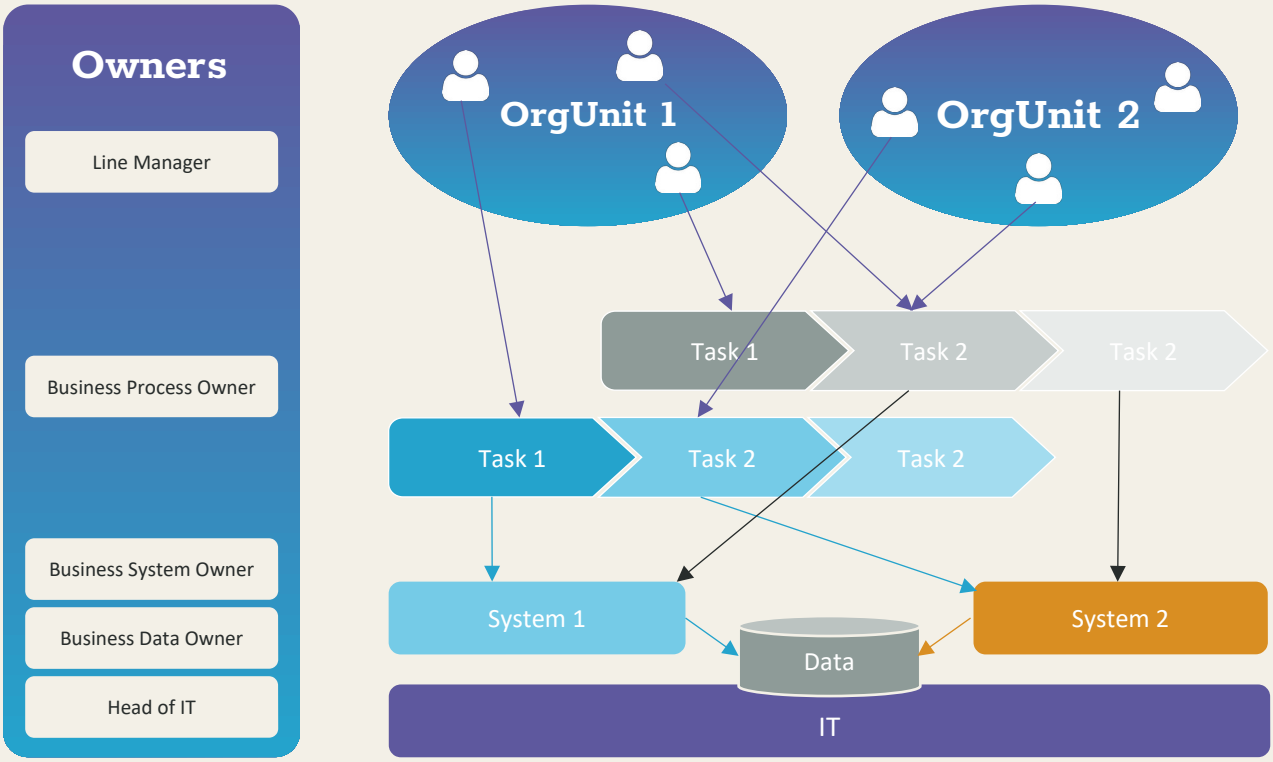

Figure 1 Access Governance reference model

Identification of Key Stakeholders

Line of Business

In an organization, people work within a hierarchy. Line managers assign their staff to perform tasks within the business processes. They determine which employee may perform what tasks. But that should be compliant with requirements from a business process owner: A process owner expects the person performing a job to have the required certifications and work experience.

Some of the tasks and responsibilities:

- HR-related tasks, such as certifying and evaluating employees.
- Assigning employees to tasks.
- Establish and facilitate career path with appropriate tasks.
- Managing employee workloads (not too much or too few tasks).
- Ensuring that productivity, such as billable hours, is met.

Not all identities who need access have a line of business owners. For example, contractors and third parties may not have *a line manager* in this instance, if they are assigned specific tasks, the hierarchical operational manager should be the accountable person, but the system owner is typically responsible for establishing access rights.

Efficiency is the core driver for workforce management.

Process Owners

Business process Owners do not typically participate in granting access control entitlements, but they should participate in establishing the access control policy. They are accountable for the quality of a process: defining the different process steps, critically reviewing performance, and controlling performance quality during and after the processing of tasks.

The process owner is responsible for setting up processes and determining the quality criteria relative to the input and output of the process. Examples include competence requirements about persons who can perform tasks within the process as well as segregation of duties (SoD). A business process owner defines the SoD rules, thereby allowing or blocking access to certain transactions. For audit and compliance purposes, SoD rules and *four-eyes* controls should be registered in the SoD rules registry in an IAM tool or in a configuration management solution. An SoD rule without an explicit owner is not a valid SoD rule and should be removed.

A business process owner should make sure that line managers are aware of these requirements for them to assign the tasks to their direct reports. They also want to be able to monitor who has performed a task, so for audit and forensic purposes, the identity of authenticated users should be logged.

The tasks and responsibilities of business process owners include:

- Defining quality criteria for process execution, inputs, and outputs.
- Establish management and risk prevention controls such as separation of duties and implementing monitoring systems.

- Define process KPIs.
- CIA risk assessment (confidentiality, Integrity, and Availability).
- Data contracts or interfaces.
- Authorization models in consultation with line managers, data owners, and system owners.

Business processes can be supported by one or more information systems and can be performed by one or more organizational units.

Effectiveness and process quality are drivers for the business process owner.

System Resource Owners

System owners are responsible for the implementation and running of information systems and services that are used within business processes.

The system owner ensures acceptance of a system that is deployed into production and for life cycle management of the system, such as version management, change management, etc. In addition, this owner keeps the budget of the system or service to keep it up and running.

A contract owner of a SAAS contract manager can also be regarded as a system owner.

The system owner will also make sure that the authorization model reflects the requirements for system governance and should make sure that system authorizations are granted appropriately, and that access complies with software license constraints.

In the access governance model, it is assumed that system ownership belongs to the business side of an organization, it is the person accountable for accepting a system in production and who owns the budget for the system.

A system owner's tasks and responsibilities include:

- Establishing an SLA with the IT group deploying the service.
- Acceptance of an information system before taking it into production.
- Change management (requirements analysis, management of a change request).
- Implementation of an authorization model; user management; application roles or system roles, built-in in the system.
- Budget responsibility for operating the system.

Systems can support one or more business processes and can be used by users from multiple business units.

Costs are a business driver for a system owner.

Data Owners

A data Owner is responsible for ensuring only appropriate access is granted to a data repository and that regulatory controls are met.

In terms of access by users, data owners supervise compliance with laws and regulations, such as retention or destruction of data, but also for enforcing consent management and restriction of access to the data in accordance with the goals of registration. These are written down quite explicitly in 'Laws of Identity' and in privacy regulations such as the European General Data Protection Regulation (GDPR).

Data owner tasks and responsibilities include:

- Maintaining laws and regulations regarding data (e.g., limitation of usage based on consent, retention, and removal of data).
- Drafting of data contracts (e.g., transfer of data between processes / process owners and systems), both internal and external (maintaining legal accountability, where applicable.

Compliance is an important driver for the data owner.

IT Owners

The head of IT, or sometimes the CIO, or CTO, is a common role in many organizations; it is a special type of owner. In many organizations, the head of IT is made accountable for access control, but this is poor practice. The IT department does not 'own' the access policy definitions. While IT does facilitate the access control process, the actual ownership of the processes, systems, and data is a responsibility of the lines of business.

The head of IT can only be the owner of access control decisions within the IT department itself. The head of IT 'owns' all IT components, such as servers, PCs, networks, and mobile devices. These components are used to host information systems and support data transfers. Access to these resources is usually reserved for IT administrators, but functional managers and 'ordinary users' also have access to various IT components, such as disk space, shares, and even the corporate Wi-Fi network.

Typical tasks and responsibilities include:

- Fulfilling the SLA with the system owner.
- Ensuring sound deliverance of IT security.
- Providing access to IT components and facilities.

Customer satisfaction is the driver for the head of IT.

Relationships Between Stakeholders

The distinct roles, as described in the previous section of this article, also maintain relationships with each other. The best known is the relationship between the system owner and the head of IT, which often takes the form of a Service Level Agreement (SLA). In an SLA, both the system owner and the head of IT agree on how a system is managed within the infrastructure, Quality of Service requirements, how it is funded, but also how the system can be used and under what conditions access to the resources can be granted, like coping with system accounts, or different device types or requirements concerning network connections.

Another well-known relationship is covered by the data contract or Interface. This contract is a technical description of the data elements that flow between systems and processes. From the viewpoint of a data owner, this also covers data about rights of use, consent, and inheritance of controls, as well as rules about data retention and storage.

In practice, the SLA is the only formal agreement between the diverse types of owners. What's lacking are the contracts/agreements between the line manager and the process owner and between the business process owner and the system owner. It is important to understand that formal arrangements must be made to govern access control.

It is also important to understand that while often multiple people can perform the same tasks at the same time, accountability for the actions taken (or ignored) cannot be shared. A single employee is *responsible* for the execution of a task, but the line manager is *accountable* for the actions performed by all their direct reports. There can be multiple line managers, but every employee can only have one accountable line manager (even if the employee works for multiple teams and thus for multiple line managers). If an owner of an authorization changes position or leaves the organization, then the ownership must be transferred to another appropriate person. When processing a 'mover' or 'leaver' event for an authorization owner, a check should be made to ensure their responsibilities have been appropriately transferred.

In theory, each of these five types of stakeholders contributes to determining who can have access to systems, services, and data. Identifying each owner's roles is important if governance over access control is to be maintained.

In practice, all five types of stakeholders will not be explicitly involved in granting access to protected resources, so access governance is needed to be able to control and mitigate the risk of granting inappropriate access to a user. For high-risk industries, additional access governance controls, such as versioning of access rules and logging and monitoring should be implemented, and all owners should be consulted in defining the access policies.

Accountability

Based on this access governance reference model *(Figure 1)*, access decisions are made by the collective owners, each for their own zone of expertise and responsibility.

Several of these types of owners can be identified in many organizations. A line manager, a head of IT, and a system owner are roles that exist in every organization. They are not always labeled as such, but the nature of the role is comparable.

In most organizations, the business process owner as an explicitly identified stakeholder, with the responsibility for access control decisions based on business process requirements, is lacking. If that is the case, it is a quite relevant omission. When we deduce that the business process owner is accountable for process requirements like Segregation of Duties, this requirement cannot be defined or implemented by a line manager or a system owner. These owners have their own responsibilities towards access control. Business process requirements differ from their regular responsibilities:

- The scope is different: business processes span multiple organizational units and systems.
- The knowledge is different: process quality requirements demand expertise in process management, input and output control, and risk management.
- The time horizon is different: a business process can be a single task that can be executed in a second or a sequence of many tasks, lasting many days or weeks.

A business process owner can also have requirements that conflict with the requirements of the line manager. As an example, the process owner requires SoD between the performer of task 1 and task 2 within the same process. But the line manager may not be able to assign different people to both tasks. This conflict can be critical, but it needs to be addressed, for instance, by adding additional security controls such as logging and monitoring or *four-eyes control*. But that control should be accepted by a stakeholder in the role of business process owner.

To be in control, it is essential to make sure that business processes have been identified and that for processes with a certain level of risk, the access rules have been defined by the business process owner. Meaning that toxic combinations of authorizations are not part of the same business role or assigned to the same person.

There is often confusion in organizations that focus on provisioning approved by line managers. For instance, a line manager may have a fresh staff member commencing work, so they establish access rights to the systems the new staff member needs to do his or her job. However, if the various system owners are not involved in approving a user's entitlement to their system, system owners cannot be held responsible for unauthorized access, for instance misusing the available licenses, to their systems.

Most governance systems produce attestation reports that provide a line manager with a list of subordinates and identify their system access rights. This allows managers to periodically verify the entitlements of staff members to verify that authorizations of people who have changed roles are still appropriate, and to check that system access that is no longer required has been removed. Governance systems should also be able to list user access by system to provide account control oversight to system owners.

Practical implications: Roles and groups

The problem of lacking Access Governance is nowhere more obvious than when discussing the standard way of giving entitlements to employees. To make assigning authorizations easy, the concept of ‘roles’ or 'group memberships’ is used. If entitlements are granted to a ‘business role’ or group, then every person with that role, or everyone who is a member of the group, automatically inherits the entitlement. By using this concept of Role Based Access Control, granting, or revoking authorizations is made convenient for the line manager of the employee. If a line manager gives a role to the employee, this employee automatically gets the entitlements that are connected to the role. And if the role is revoked, the employee automatically loses the authorizations that are connected to the role. An additional benefit of using RBAC is, assigning authorizations to employees or revoking them can easily be automated which results in:

- Lowering manual efforts, reducing errors.
- Preventing forgetting of revocation.
- Lowering operational risks and expenditures.

In practice roles are defined by line managers and system (or asset) owners. Sometimes the concept of roles is expanded by creating both business roles and application roles (or system roles) within applications.

So, governance-wise, what is the problem of this form of managing authorizations? Well, as can be seen in the access governance model, in these cases only 2 of the 5 stakeholders, 2 of the 5 types of owners, are responsible for managing access, whereas we saw that multiple types of owners should be involved in the access control decision. That means that different interests are not considered. And that adding additional requirements (like: we need a ‘Junior’ position) leads to an explosion of roles, to manage all kinds of exceptions.

An example: Let us have a look at the concept of Segregation of Duties: SoD’s can only be defined by business process owners: an SoD rule is a business process rule. How is it possible that in most organizations the process owners are not involved in defining authorizations where SoD is at stake? Why would you want an asset owner to define SoD restrictions, when a process can span multiple systems or multiple organizational units? The asset owner is not accountable for defining SoD, this owner cannot be considered competent to carry that responsibility, this owner cannot be accountable for this task.

There are similar examples for managing authorizations about different contextual restrictions (location, time), or data access restrictions (just think of privacy regulations), that can just not be defined by only a hierarchical manager or system owner.

Organizations need to identify and involve all relevant stakeholders.

Bringing It All Together: Access Governance Good Practices

Several good practices that can help implement Access Governance and guide the stakeholders in their roles:

- Every business process must have an owner: Assign owners to business processes. If the owner leaves, the accountability must be assigned to another person.
- Define a risk profile for each business process, based on CIA rating.
- Have the process owner of critical processes determine the quality criteria, such as rules for the context (such as time or location of access, type of device) and competencies (such as training, experience).
- Business process owners must define and formalize the SoD rules.
- Assess each SoD rule separately: who is the owner of the rule (who needs it?), and why has the rule been defined? If those questions cannot be answered, if there is no formal owner of the rule, then the rule should be removed. If a business owner opposes the removal of the rule - so a business owner who feels that the rule is essential - then this business owner can be considered as the owner of the rule.
- Business Process Owners must validate the existing business and system roles.
- The diverse types of owners should be defined, they should have the mandate to define the access policies, and they should be able to enforce their policies.
- A process for validating and re-certifying established entitlements should be developed.
- Line Managers will periodically verify granted authorizations of their direct reports.

This model is applicable for all types of access control, RBAC, ABAC, PBAC. It is also valid for access control for non-human accounts (Internet-of-Things (IoT) devices) and zero-trust architectures.

Good practices will guide an organization towards good governance. Implementing the Access Governance model into an organization's structure and culture requires **organizational change** and educating the stakeholders.

Access Governance is not a process; it is an ongoing responsibility that must evolve with changes within an organization.

Colofon

Author Bio

André Koot is a security and IAM expert with a background in business administration and accountancy. He is a principal consultant at the Dutch SonicBee consulting and IAM managed service company, and he is a member of the IDPro Body of Knowledge committee and member of the Advisory Board of IDNext.eu.

References

Organization theory, https://en.wikipedia.org/wiki/Organizational_structure

Laws of Identity, Kim Cameron eo, https://www.identityblog.com/?p=1065

Relevant IDPro BoK articles

GDPR: An Introduction to the GDPR, Andrew Cormack https://bok.idpro.org/article/id/11/

Introduction to Access Control, André Koot, https://bok.idpro.org/article/id/42/

Policy Based Access Control, Mary McKee, https://bok.idpro.org/article/id/61/

Acknowledgments

This article is based on a whitepaper written in 2018 by André Koot published earlier by Nixu Oyj. An earlier version of that whitepaper, written by André Koot and Jacoba Sieders, was published in 2012 by IDNext.eu in the whitepaper “From Mindmap to Roadmap”.

The author wishes to thank Lori Robinson, VP, Identity and Access Management at Salesforce; Mary McGee, Director, Identity Management and Security Services at Duke University; Graham Williamson, Internet Commerce Australia, for reviewing and helping to structure and scope the article.

And also, thanks to Heather Flanagan, Principal editor at IDPro, not only a great editor but also an expert clarifier.