Access Governance

From information to cyber and even physical, the core questions anchoring all security issues are: who is granted access to an object and why are they given the right to do so?

The task of determining who is given the ability to carry out actions is not necessarily complicated. It can often follow a certain logic. For example, a property owner determines who can enter the premises. If the owner rents out the property, the tenant could also grant access to others within the contract conditions. This relatively simple principle can be easy replicated. However, when applied to other contexts such as information and data systems, it proves to be much more complex. When discussing information, there is a clear case of multiple owners and multiple types of owners and users, meaning that the 'Who, What, and Why' has deeper implications.

In the field of information security, questions surrounding access are key. Often it is not clear who determines the access policy, who manages the security of the crown jewels. There are various information owners within organizations, and they all have a say – and a stake - in deciding who can access what.

This complexity leads to a multitude of problems, perhaps the most well- known being, individuals who have too many authorizations. Perhaps they are given authorizations because they are long-term employees, or because an organization enacts the authorization because it is 'necessary', which can lead to higher risk of data breaches. Another problem is that people begin to feel that, under the guise of enforcing segregation of duties (SoD), the ease with which they can work becomes limited, and that they should be allowed to simply act without undergoing yet another access request process. This aspect of control is unfortunately often not well developed because the concept of SoD is not well understood… Control and governance are fundamentally about ownership issues.

Governance is about ownership

In the model below five types of owners are shown. Let's deal with them one by one. The fact that this overview starts with an ICT owner is perhaps a symptom of an Access Governance problem, in a broad sense. In every organization the ownership of ICT can be identified. But Access Governance is not an ICT problem. Another party should own the problem.

Ownership role	Explanation
Manager / Director ICT Infrastructure owner	The ICT Director owns all ICT components, such as servers, PCs, networks, mobile devices. These components are mainly used to host information systems and provide services for the performing business tasks. Access is usually reserved for ICT administrators, but functional managers and 'ordinary users' also have access to various ICT components, such as disk space, shares.
System owner	System owners are responsible for the implementation of information systems and services that are used within the primary business processes. And in this case the System Owner in the 'Business' is the owner we need, not the ICT equivalent. The system owner ensures acceptance of a system that is taken into production and for life cycle management of a 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 can also be seen as a system owner. Operational management on behalf of the system owner takes place by a Functional Administrator.

Process owner	The business 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 with respect to persons who can perform tasks within the process. But also requirements regarding, for example, segregation of duties. They don't care about the identity, just about quality of execution.
Line manager	The line manager is the resource owner, who assigns his employees to perform tasks within the business processes. The line manager determines which employee can or may perform which tasks. In this respect, the requirements both from the viewpoint of work division (as little as possible under- or overloading) must be met as much as possible and from the demands of the process owner because of the quality criteria for the performer.
Data owner	The data owner is a special and can never be unambiguously determined on the basis of company criteria. Is it the person who pays for the processing of the data, the person who has the budget, or is it the person who owns the data? In terms of access, it can be said that the data owner supervises compliance with laws and regulations, such as retention or destruction, but also consent and limitation of use based on the goals of registration.

These different owners also maintain relationships with each other. The best known is the relationship between the system owner and the ICT boss: the Service Level Agreement, in which both agree on how a system is managed within the infrastructure, how it is funded and how it can be used.

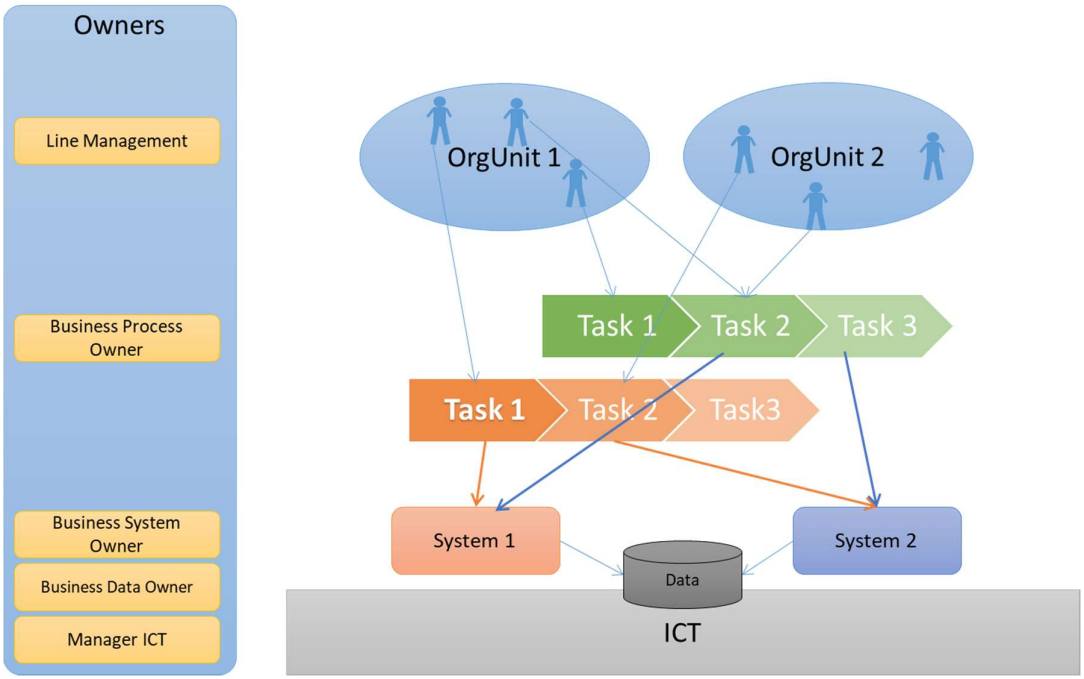

Figure 1 Access Governance model

Owners in detail

Several of these types of owners exist in many organizations. The line manager, the ICT owner and the System Owner are roles that occur everywhere in one form or another. Maybe they are not always categorized as such, but the nature of the role is comparable.

The data owner is special, partly because in many cases data is processed by several people. It does not mean that someone who processes the data itself is also an 'owner'. Within organizations, not all individuals thought to be ‘data owners’ are given the label. And while this is not of the utmost importance, it is relevant that someone must be responsible for the reliability of the data – quality standards are far too important to fall by the wayside.

The owner of a business process is perhaps most critical, primarily because it is a challenge to find the actual ‘owner’ in many organizations. For some processes it is possible to identify who *should* be the owner, but taking on the role is not always easy, largely because this individual becomes accountable for the quality of a process: defining the different steps and, critically reviewing performance, assigning duties, and controlling quality during and after the processing. Unfortunately, this rarely happens in practice.

A process owner can also have conflicting points of interest with the line manager; the former seeks high caliber qualitative input, and the latter is primarily responsible for efficiency of deployment - that can collide. To illustrate the problem, the responsibilities of data owners is outlined below:

Ownership role	Responsibilities
Manager / Director ICT Infrastructure owner	• Compliance with the SLA with System Owner • Ensuring the sound deliverance of IT security • Providing access to ICT components and facilities
System owner	• SLA with ICT • Acceptance of an information system for taking into production • Change management (Requirements analysis, management of a change request) • Implementation of an authorization model; user management; system rolls • Budget for operating the system
Process owner	• Defining quality criteria for process execution, inputs and outputs • Establish management controls such as separation of duties and implementing monitoring systems • Process KPIs • CIA risk classification (Confidentiality, Integrity and Availability) • Data contracts • Authorization models in consultation with line managers and system owners
Line manager	• HR tasks such as assessing employees • Establish and facilitate career path with appropriate tasks • Managing employee workloads • Ensuring that billable hours are met
Data owner	• Maintaining laws and regulations regarding data (eg limitation of use based on consent, retention and deletion of data) • Drafting of data contracts (eg. transfer of data between processes and systems)

Authorizations and roles

In theory, each of these five owners must contribute to determining who gains access to data. However, in the vast majority of organizations that does not happen as it should. Explicitly identifying an owner's roles is of vital importance if control over access is to be maintained.

Granting access according to the concept of Role Based Access Control (RBAC) – whereby an employee gets a role in the organization and thereby authorizations in applications and systems - is often also problematic. This concept seems simple, but if we take a closer look, it is not as transparent as we may assume. In practice, roles are defined by a line manager (we tend to call these roles business roles, or organization roles) and by a system owner. In one way or another, the business role must then be linked to the system role. But why someone gets a business role, or why a system role is linked to a business role, or even why authorizations are in a system role. The legitimacy for granting authorizations to employees is an underexposed problem.

In practice, problems faced when implementing Segregation of Duties (SoD), can be solved by ensuring that conflicting roles ("toxic roles") are not given to the same person. But again, it is not always clear what roles are conflicting. Only the process owners can separate the roles. In the lack thereof, one must conclude that the organization is simply not in control.
For example, in many organizations a system owner ('Asset owner') is responsible for defining the SoD rules in a system. But a system owner does not determine how a business process should work and what the process risks are; additionally, a process can work across multiple systems, so defining SoD rules within a single system may even not be relevant at all.
The process owner must therefore be able to say something about the content of roles and their allocation when determining the authorization structure. Unfortunately, that is rarely the case because in most organizations process ownership not explicitly identified. And even more rarely does a process owner understand how to define quality requirements (like SoD rules) for the process.

IAM solutions

Many organizations have already taken steps towards automating the identity management process and the RBAC principle. Most modern IAM solutions offer advanced authorization management facilities and reporting options to gain control. But in practice these features are not used very effectively and governance is inadequate (even though these IGA solutions are called governance solutions).
Within IAM solutions, roles can be modeled (for example on the basis of 'role mining' by which existing, frequently occurring combinations of authorizations are included in roles), and these solutions are also able to define segregation of duties rules so that conflicting authorizations cannot be assigned to the same employee. Unless, for example, a line manager overrides such a decision.
But this same problem arises again as already described: an IAM solution could enforce segregation of duties, but first someone must define the rules of separation. If it is not known who has set the rule -and in many cases there is no ‘owner’of an SoD rule- then the rule is not formally valid, meaning that the organization is once again not in control. Governance is then merely symbolic and ineffective, becoming a 'check mark' from the compliance perspective.

Taking action

- Assign owners to business processes.
- Define a risk profile for each business process.
- Have the process owner of critical processes determine the quality criteria, such as rules for the context (such as time or location, type of device) and competences (such as training, experience).
- Process owners must determine the task separation rules.
- process owners must validate the existing business and system roles.

- Assess each SoD rule separately: who is the owner and why has the rule been defined? If those questions cannot be answered, the rule should be removed. The only one who can oppose this, can be considered as the owner ...
- As indicated earlier, there are owners who wear different hats; however, decisions surrounding must be explicit. Which role, which hat, has the owner used to define the rule?
- Provide a process for validation of established and changed role models.

Conclusion

Executing all these actions does not necessarily lead to good governance. Governing access is not a process, but a ceaseless responsibility. Moreover, in this paper we have not paid attention to data quality, login, federation, audit or maturity of the organization.
For the individual faced with the task of purchasing an IAM solution or setting up RBAC, this must be a painful observation. But perhaps it helps to look at the access issue from this point of view in order to implement sustainable, long-term access controls.

And if this article does not help enough ...

Nixu helps organizations with their security needs. In the field of IAM, we carry out problem analyses and draft the architecture necessary for systematic implementation within the organization. We also help clients manage IAM solutions by provide 24-hour support.

About the author

This article is written by André Koot. He has 25 years of experience in information security and is a renowned expert in Identity and Access management. He is Practice Lead for IAM at Nixu and independently leads a 4-day IAM training via IMF-online. André can be contacted via andre.koot@nixu.com and via his Twitter handle, @meneer.