Access Control in Information Security

Access control is a part of everyday life and is also an integral component of IT and data security for businesses.

It’s a broad term that describes a variety of ways to control who has access to organization’s resources.

Access controls also help you stay compliant with various industry standards and regulations. By restricting access to sensitive systems or data, you’re limiting the potential risks associated with data exposure.

Access control in information security is about determining who gets access to what, when, how (files, directories, applications, etc.).

Access control is a broad term that describes policies and methods that ensure only verified individuals can physically or virtually touch items that they have permission to access. This process involves restricting access or granting permissions that allow someone to do something to a protected item. This includes having permissions to do any of the following to protected items (digital or physical resources):

- Access,
- Read,
- Modify,
- Communicate,
- Delete or otherwise destroy.

Access controls requires an in-depth understanding of the relationship between two specific terms: *subjects* and *objects*.

“Subjects are usually people or groups. Objects are usually files or directories. The key is, subjects access objects, and so access controls regulate how subjects access objects.”

Objects could be resources that you want to protect from unauthorized access, use, or disclosure. And the subject is the user (or group of users or even non-person entities such as applications or services) that the access controls apply to. So, access controls (in a more technical sense) are the tools, policies, models, and mechanisms that enable you to grant or restrict access to your organization’s digital or physical resources. This includes everything from restricting or granting access to specific files and databases to IT systems and physical locations.

Access control is a way for you to ensure that only the individuals (or groups) you choose have access to your sensitive data, applications, technologies, and critical infrastructure.

Basically, these types of physical and logical restrictions prevent unauthorized individuals from doing things they shouldn’t with your sensitive systems or data. Furthermore, they also help to prevent inadvertent exposure or disclosure of sensitive items.

Authorization and Authentication

Authentication and authorization are key components of information security, cybersecurity, and access control. They’re also integral to identity and access management.

- **Authentication** is all about proving or verifying that someone is who they claim to be. This differs from identification, which is when you (or someone else) claims to be you, but that claim isn’t verified. Authentication involves verifying someone’s identifying information (for example, a username and password) against the information you have on file. This process prevents Carrie in customer service from pretending to be Harry from Human Resources to access systems she doesn’t need access to.
- **Authorization** refers to granting someone the ability to access, use, or modify some type of asset or resource. So, once they’re logged in or otherwise authenticate themselves, this

next part of the process will determine whether or not they have the system permissions or privileges to do what they're trying to do.

So, let's consider an example. Let's say I want to access one of my company's intranet sites to access some marketing related files.

- *Identification* would be me typing in my username in the login field for the page.
- *Authentication* would be me typing in my corresponding password (or using a PKI-based passwordless authentication method such as a client authentication certificate) to prove my identity so that I can access the site.
- And *authorization* would be the permissions or access privileges that my director or our sysadmin set for me. These access controls determine what I can do to any files once I've proven my identity and logged in to the system.

Types of Access Control Systems

Access control systems can be logical or physical in nature and fall within three sub-categories:

- **Technical control systems**,
- **Administrative control systems**, and
- **Physical control systems**.

Organization requiring employees to use an ID badge to access specific areas, such as server room is an example of physical access control because it prevents just *anyone* from meandering in. An example of administrative access control is limiting which of the employees — or groups of employees — can make changes to specific files. A technical form of access control would be limiting which IP addresses (or ranges of IP addresses) can access your network through your firewall.

Some examples of virtual and physical access control systems include:

- Login credentials (such as usernames and passwords).
- PINs and one-time passwords (OTPs).
- Virtual private network (VPN) access to internal networks.
- Physical access cards, FOBs, tokens, locks, and keys.
- Security guards with access lists.
- Biometric readers (such as for facial, retinal, and fingerprint scans).
- Digital authentication certificates and digital keys.

While access controls may seem inconvenient or cumbersome, they're integral to the security an organization. They can help to prevent sensitive data from being exposed as the result of human error or an employee going rogue by limiting who has access to it.

Access Control Lists

An access control list, much like the name would imply, is a list of privileges or permissions that authorize or deny access for specific people or groups to specific objects. ACLs consist of various access control entries (ACEs), which specify the subject and any privileges they have for specific objects.

ACLs serve different functions in terms of how and where they're used and are central to several different access control models. In the meantime, here are just a few quick examples of common access control lists:

- Filesystem Access Control Lists,
- Active Directory Access Control Lists, and
- Network Access Control Lists.

Access Controls in an Organization

File-Sharing Platforms like SharePoint and Google Docs

If you use these types of file-sharing platforms, you're already familiar with this type of access control. Whenever you create or share a document, you can choose to either keep control to Recall when lastly someone sent you a link to their Google doc file. You might have been required to request access to gain permission to see and edit it.

Windows Active Directory

You can set up folder permissions for groups and individuals in Active Directory:

These permissions can be set for specific objects or groups of objects.

Linux Access Controls

You can also can also use access controls for filesystems in Linux. This process involves the use of Linux ACLs to grant permissions to one of three options: users, groups, or others. The level of access that each of these permission categories could have includes read, write, and execute.

WordPress Access Controls

In WordPress, you also have the option of implementing access control. You may give a few users Administrator access, which allows them to give other users access, whereas you may only give some editors author access.

You can also use WordPress plugins like the Advanced Access Manager (AAM) to set more specific, granular access controls.

Access Control Models

There are actually several models or varieties of access control to choose from in information security to determine user access.

1. Discretionary Access Control (DAC)

Discretionary access control enables a file or system owner to control, grant, or limit others' permissions. For example, think of when you create a Google Sheets spreadsheet in Google Drive. As the file owner, you can choose to grant access to specific individuals to either access, read, or modify the document. You can also set it so that anyone with a link can access the document or open the document up to the public.

DACs, which are commonly used for operating systems, rely upon access control lists (ACLs). These lists generally specify individuals (or groups of individuals) along with their access permission levels. Discretionary access controls are also more flexible and less restrictive with the next type of access control we're going to talk about. However, they're also the least secure method as well because access control is left up to the file or system owner.

Of the different control access models, DACs are the least restrictive and are commonly used.

2. Mandatory Access Control (MAC)

Unlike DAC, **mandatory access control** is nondiscretionary and is simply based on the decisions of a central authority such as a security administrator. The file owners and users themselves have little to no say in who can access their files.

MAC relies on labels (such as confidential, secret, top secret, etc.) and clearances to associate any programs or levels of access with users. Documents receive labels that determine which levels of clearance you need to have to access, modify, or disclose them.

An administrator can set these levels of access for individuals and groups of users, which the users themselves can't change. This model of access control is the most restrictive.

3. Role-Based Access Control (RBAC)

Role-based access control gives access permissions based on user roles. Role is the functions that an employee performs. Users may have one or more roles and may be assigned one or more permissions as a result. Doing this gives users who have those roles access to the info they need to do their jobs without affording them access to information that they don’t need. RBAC is a broader form of access control than, say, MAC.

In Windows, for example, you can use Groups to set RBAC.

4. Attribute-Based Access Control (ABAC)

It represents a point on the spectrum of logical access control from simple access control lists to more capable role-based access, and finally to a highly flexible method for providing access based on the evaluation of attributes.

ABAC helps us to link people or groups with the types of data that they can use within specific parameters. It supports the use of Boolean logic to create more granular policies that are also more flexible.

Attributes could be specific characteristics or specifications that are applied to either subjects (subject attributes) or objects (object attributes). Some examples of subject attributes include management levels, employee IDs, organizational roles.

Some examples of how you can use this type of access control include:

- Restricting access to your network or specific systems before 9 a.m. or on the weekends.
- Limiting the ability to edit a document to the file owner.
- Giving permissions to a specific class of employee to read or modify files within a specific folder.
- Restricting access to software to employees within a specific team.

Significance of Access Control

- Limit liability and damage from attacks
- Carry out anomaly tracking, and
- Increase accountability.

The Challenges of Controlling Access for Organizations & Businesses

There’s a Perception That Access Controls Limit Efficiency