**7 Types of Identity Management Access Controls**

According to the [Verizon 2020 Data breach Investigations report](https://enterprise.verizon.com/resources/reports/dbir/), brute force attacks and the use of stolen or lost credentials are the root cause for more than 80% of breaches. This makes having a strong information security program an essential capability for organizations today. Identity and Access Management is a vital part of information security because it provides a central platform and framework to manage the [user Identity Lifecycle](https://www.idenhaus.com/iam-managing-user-access-across-lifecycle/). One of the core benefits of IAM is that it supports a range of access control models that tie into the organization’s [governance policies](https://www.idenhaus.com/seven-goals-identity-governance-success/). IAM technologies manage security administration and monitor the status of user accounts and activities within the organization. Privilege misuse is one of the prevalent threat actors that still persists in most ransomware attacks. In this blog, we discuss the various security controls that are defined for information systems and the publications available that provide recommendations to mature your organization’s cybersecurity posture.

**7 Types of Access Controls:**

The term describes a variety of protection mechanisms to prevent unauthorized access to a computer system or network. These controls can be implemented in several ways and the effectiveness of the control depends on the data regulations set by the company.

**1. Mandatory Access Control:** This is a system-enforced access control that is based on a subject’s clearance and an object’s labels. It is usually associated with multilevel security labels such as Top Secret, Confidential, and Secret.

**2. Discretionary Access Control:** This is a type of access control that restricts access to objects based on the identity of subjects and groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission.

**3. Rule Based Access Control:** In this model, access rules are pre-defined (for example, via an ACL) and are evaluated to determine access permissions. Rule-based access defines specific and detailed situations in which a subject can or cannot access an object, and what that subject can do once access is granted. While the rule-based model offers a straightforward way to manage access control permissions, it is a very complex and unproductive control if you need to manage access at a more granular level. In summary, rule-based controls enforce rules on all the users equally, for more granular applications the role-based controls lose their usefulness.

**4. Physical Access Control:** Physical access controls restrict access to a physical space within an organization. This type of access control limits access to rooms, buildings and physical IT assets. One benefit of implementing these controls, is that you have a record of everyone who is entering and leaving restricted areas.

Examples of physical access control include badge card readers or fob controlled doors that require the user to present a valid physical credential to enter a room or facility. These readers only give access to workers with the right credentials.

**5. Role Based Access Control:** This is a type of control that uses a [user’s role](https://www.idenhaus.com/understanding-role-based-access-control-rbac/) as a basis to restrict access. Custom roles are usually created such that the least privilege policy is maintained, and the access is revoked when no longer needed.

**6. Attribute Based Access Control:** This is a form of access control that governs the access based on the attributes. These can be user attributes, resource of object attributes, and environmental attributes.

**7. Policy Based Access Control:** This is a strategy used to [manage access based on the policies](https://www.idenhaus.com/what-is-policy-based-access-control-pbac/) which determine what access role each person must have.

NIST 800 series publication is one of the best publications to refer for controls and security requirements that need to be set for each control family.

The [NIST 800-53](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf) provides a list of controls that support the development of secure and resilient federal information systems and the [NIST 800-171](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf) publication provides recommendations for protecting the confidentiality of controlled unclassified information (CUI). They are divided into 14 control families which consist of security controls that help in maintaining the integrity, confidentiality, and availability of information systems.

**Identity Management best practices:**

Listed below are the best practices to maintain the integrity of user and device identities based on the security controls:

* Perform a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis based on the risk appetite of your company
* Least Privilege – be aware of any ‘allow all’ type or roles and where/when those are being used
* Protect root level of access and restrict privilege abuse
* Detail and assess the out of the box roles before assigning these
* Control groups for permission assignments and monitor the access
* Be sure to have good password policies configured into applications and processes
* Have clear and communicated policies that govern which identities and roles can access which resources
* Use compliance as code and policies as code to prevent excessive privileges being created as a result of development
* Build an inventory of identities – this should include APIs, services/service accounts, 3rd parties, BOTS, and devices
* Adopt a [zero-trust architecture](https://www.idenhaus.com/leveraging-zero-trust-with-identity-at-the-core/) approach
* Remove unused credentials
* Engage with an Identity Solutions provider to conduct an [Identity Management Assessment](https://www.idenhaus.com/iam-assessment/) for your organization

Identity Management improves the security of an organization by reducing users with excessive or toxic privileges by as much as 60% per Forrester Research. Companies must invest the time and effort in identifying and implementing the proper identity management access controls needed for their organization to safeguard their IT systems. [Proper planning](https://www.idenhaus.com/6-reasons-to-get-started-with-iam-roadmap/) is critical to a successful IAM project. [Contact Idenhaus today](https://www.idenhaus.com/contact/) for help getting your IAM project done right, the first time around.