Identity management

ISO 27002 Control 5.16

Control

The full life cycle of identities should be managed

Purpose

To allow for the unique identification of individuals and systems accessing the organization's information and other associated assets and to enable appropriate assignment of access rights

Why is it important?

- To make sure that people can be held accountable for their actions and to prevent impersonation. It is a pre-requisite for later authentications and access controls.

What are the main principles ?

- One person = One identity
- Strictly control shared identities
- Strictly control non-personal accounts
- Identities should be provisioned based on a process initiated by human resources or procurement
- Keep records of all significant events
- Manage third-party identities

What are the main risks ?

- Having privileged users using their regular identity to perform administrative tasks
- Sharing identities amongst people
- Not having a person designated as accountable for the generic users
- Forgetting to disable an identity on time
- Lack of logging / alerting for suspect behaviors of identities
- Having identities defined in multiple systems that

Link with other frameworks

- NIST 800-53 rev5 : AC-2, IA-2, IA-4, IA-5, IA-8
- NIST CSF 2.0 : PR.AA-01, PR.AA-05

Renaud Dardenne
Asphalia Consulting