Access rights

ISO 27002 Control 5.18

Control

Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control

Purpose

To ensure access to information and other associated assets is defined and authorized according to the business requirements

Access rights granting

- One process for all users – no exception
- Access authorization from the owner of the information system
- Access authorization from the line manager
- Access based on business requirements
- A record of all access right granting should be kept
- Consider active monitoring of the tools used for the access provision
- Use access rights group definition to ensure homogenous access across team members

Access rights revocation / adjustments

- Both for internal and external users
- At least upon job termination or job modification
- Temporary access rights should always have an automatic expiration date
- An emergency access revocation process should be defined for exceptional cases
- Do not forget to adapt physical access rights

Access right review

- Review by business owners
- At predefined intervals
- Privileged access should be reviewed more often
- What is permitted and prohibited
- The monitoring activities
- Access restrictions

Link with other frameworks

- NIST 800-53 rev5 : AC-2
- NIST CSF 2.0 : PR.AA-01, PR.AA-02, PR.AA-05

Renaud Dardenne
Asphalia Consulting