Access control

ISO 27002 Control 5.15

Control

Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements

Purpose

To ensure authorized access and to prevent unauthorized access to information and other associated assets

What aspects should be considered ?

- Both logical and physical access
- Include both human and non-human entities
- Access to data / generic IT resources / applications
- Define first a global access policy, then provide specifics in a procedure

What topics should be in the access policy ?

- Alignment between access and information classification
- Relations between identification, authentication, and access
- The global lifecycle of access : join / work / leave
- The roles and responsibilities in the access process : the roles of management and business owners
- A reference to the least privilege principle and the segregation of duties
- The main type of access control to implement : RBAC / MAC / …

What specific details are important ?

- The universal process of access request, access approval, and access provisioning
- The access logging mechanisms
- The monitoring activities
- Ensuring that privileged access rights are restricted
- Consistency between your organization's access rights and physical security requirements
- How cloud based access are managed

Link with other frameworks

- NIST 800-53 rev5 : AC-1, AC-3, AC-6
- NIST CSF 2.0 : PR.AA-02, PR.AA-05, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01

Renaud Dardenne
Asphalia Consulting