Privileged access rights

ISO 27002 Control 8.2

Control

The allocation and use of privileged access rights should be restricted and managed

Purpose

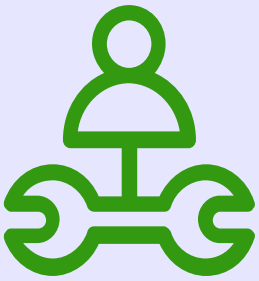
To ensure only authorized users, software components and services are provided with privileged access rights

Why is it important?

- Privileged access rights allow users to override system or application controls
- Restricting allocation ensures alignment with the minimum requirement for functional roles
- Logging privileged access ensures accountability for audit purposes

What should we take care of ?

- Privileged User List
- Explicit permission of usage
- Expiration of privileged accounts
- Different logins for normal and privileged activities
- MFA
- Ban generic accounts
- Time-limited privileged access
- Logging
- Working with groups/roles



What are the best practices ?

- Allocating privileged access rights as needed and on an event-by-event basis
- Regularly reviewing users working with privileged access rights
- Restricting the use of generic administration user IDs

Link with other frameworks

- NIST 800-53 rev5 : AC-2, AC-3, AC-6, CM-5
- NIST CSF 2.0 : PR.AA-02, PR.AA-05, PR.DS-02, PR.DS-10

Renaud Dardenne
Asphalia Consulting