Use of privileged utility programs

ISO 27002 Control 8.18

Control

The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled

Purpose

To ensure the use of utility programs does not harm system and application controls for information security

Why is it important?

- Most information systems have utility programs capable of overriding system controls (e.g., diagnostics, patching tools)
- Tight control reduces the risk of malicious or accidental misuse
- Logging all usage ensures accountability

What are the sub controls ?

- Limitation of the use of utility programs to the minimum practical number of trusted, authorized users
- Using unique identification, authentication, and authorization procedures for utility programs
- Removing or disabling all unnecessary utility programs
- Logging of all use of utility programs

What are the risks if badly implemented ?

- Harm to system and application controls due to misuse of utility programs
- Unauthorized access or changes if controls are overridden
- Failure of accountability if use is not logged
- Excessive risk if utility programs are available to users requiring segregation of duties

Link with other frameworks

- NIST 800-53 rev5 : AC-3, AC-6
- NIST CSF 2.0 : PR.AA-02, PR.AA-05

Renaud Dardenne
Asphalia Consulting