Protection of information systems during audit testing

ISO 27002 Control 8.34

Control

Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management

Purpose

To minimize the impact of audit and other assurance activities on operational systems and business processes

Why is it important?

- Audit tests (especially technical tests) can risk system integrity and availability
- Restricting access and monitoring protects systems from accidental or malicious changes during the assessment
- Ensures the security requirements of devices used by auditors are verified

What should be planned ?

- Plan and agree on audit tests with appropriate management
- Restrict access to read-only access to software and data, or use an experienced administrator for execution
- Run tests that can affect system availability outside business hours
- Monitor and log all access for audit and test purposes

Small details

- If read-only access is unavailable, the test should be executed by an experienced administrator on behalf of the auditor
- The security requirements (antivirus, patching) of the devices used for accessing systems must be verified
- Only allow access other than read-only for isolated copies of system files
- Audit requests for access to systems and data must be agreed with appropriate management

Link with other frameworks

- NIST 800-53 rev5 : AU-5*
- NIST CSF 2.0 : PR.PS-04

Renaud Dardenne
Asphalia Consulting