Change management

ISO 27002 Control 8.32

Control

Changes to information processing facilities and information systems should be subject to change management procedures

Purpose

To preserve information security when executing changes

Why is it important?

- Inadequate control of changes to information processing facilities and information systems is a common cause of system or security failures
- Formal procedures mitigate risks related to system integrity and availability
- Ensures all related documentation and continuity plans are updated following a change

What are the good attributes ?

- Change Process
- Planning
- Impact assessment
- Tests in non production environment
- Deployment plan
- Rollback procedure
- Change registering tool
- Approval of the change
- Update DRP / CMDB after change

Best practices

- Integrating change control procedures for ICT infrastructure and software
- Planning and assessing the potential impact of changes considering all dependencies
- Documenting and testing fall-back procedures

Link with other frameworks

- NIST 800-53 rev5 : CM-3, CM-5, SA-10, SI-2
- NIST CSF 2.0 : ID.RA-07, PR.PS-01

Renaud Dardenne
Asphalia Consulting