Information backup

ISO 27002 Control 8.13

Control

Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup

Purpose

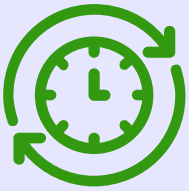
To enable recovery from loss of data or systems

Why is it important?

- Backups are crucial for integrity and availability
- Ensures recovery meets the required objectives and time frames
- Regular testing verifies media integrity and restoration procedures
- Remote storage prevents data loss from disasters at the main site

What does it imply ?

- Producing accurate and complete records of backup copies and documented restoration procedures
- Storing backups in a safe and secure remote location at a sufficient distance to escape disaster
- Regularly testing backup media (on a test system) to ensure reliability for emergency use
- Protecting backups by means of encryption where confidentiality is important
- Monitoring the execution of backups and addressing failures of scheduled backups



What should not be forgotten ?

- Offsite/cloud backup storage
- 3-2-1 backup rule implementation
- Encrypted backup data
- Immutable/air-gapped backups
- Regular backup testing and restoration drills
- Versioned backups with retention policies
- Automated backup scheduling and monitoring

Link with other frameworks

- NIST 800-53 rev5 : CP-9
- NIST CSF 2.0 : PR.DS-11

Renaud Dardenne
Asphalia Consulting