ICT readiness for business continuity

ISO 27002 Control 5.30

Control

ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements

Purpose

To ensure the availability of the organization's information and other associated assets during disruption

Who should be involved ?

The whole company :

- Personnel with the necessary responsibility, authority and competence
- Management
- Facilities / Legal / Compliance / Risks / Procurement / IT / ...

What needs to be done ?

- A Business Impact Analysis (BIA)
- Define the RTO (Recovery Time Objective) and RPO (Recovery Point Objective)
- Defining a strategy to identify which disasters will be covered
- Creating the Business Continuity Plan (BCP)
- Creating the Disaster Recovery Plan (DRP)
- Testing the BCP and the DRP

Details are important

- Implementing redundancy alone does not constitute ICT readiness
- Crisis management should trigger the BCP or DRP invocation
- The selected continuity strategies should cover options for before, during, and after disruption

Link with other frameworks

- NIST 800-53 rev5 : CP-2(1)*, CP-2(8)*, CP-4*, CP-4(1)*
- NIST CSF 2.0 : NA

Renaud Dardenne
Asphalia Consulting