Information security during disruption

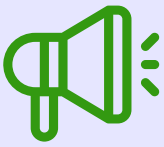
ISO 27002 Control 5.29

Control

The organization should plan how to maintain information security at an appropriate level during disruption

Purpose

To protect information and other associated assets during disruption



What are the main risks ?

- Consequences of loss of confidentiality, integrity, and availability being overlooked during disruption
- Failure to restore information security at the required level or in the required time frame

Which topics should be addressed ?

- Requirements for adapting information security controls during disruption
- Plans to maintain or restore the security of information of critical business processes
- Security of information being restored at the required level and in the required time frames
- Consequences of loss of confidentiality and integrity of information (these should be considered and prioritized in addition to availability)

How is it achieved ?

By having the BCP and DRP adapted to :

- Determine the requirements for adapting existing information security controls during disruption
- Develop, implement, test, review, and evaluate plans to maintain or restore information security
- Implement and maintain compensating controls for controls that cannot be maintained during disruption

Link with other frameworks

- NIST 800-53 rev5 : CP-2, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13
- NIST CSF 2.0 : GV.OC-04, ID.IM-02, ID.IM-04, PR.AA-02, PR.DS-11, PR.IR-03

Renaud Dardenne
Asphalia Consulting