Independent review of information security

ISO 27002 Control 5.35

Control

The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur

Purpose

To ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security

Why is it important?

- It provides objective assurance on whether the approach to managing information security is effective
- It ensures controls and policies remain relevant in response to internal and external changes (laws, regulations, threats)

How is it achieved ?

- Internal audit department
- External audit - regulators
- Penetration tests :
  - External
  - Internal
  - Physical
  - Black box / grey box / white box

By who and how often ?

- A yearly plan must be documented
- Independent reviews are conducted at planned intervals
- Results are reported to management and top management
- If deficiencies are found, management initiates corrective actions
- Using reviewers who are competent and independent
- Opportunities for improvement and the need for changes to policies and controls

Link with other frameworks

- NIST 800-53 rev5 : CA-2(1)
- NIST CSF 2.0 : na

Renaud Dardenne
Asphalia Consulting