Information security awareness, education and training

ISO 27002 Control 6.3

Control

Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function

Purpose

To ensure personnel and relevant interested parties are aware of and fulfil their information security responsibilities

Why is it important?

- It ensures technical teams maintain the skills required for configuring and maintaining security levels
- It ensures compliance with applicable security rules and obligations
- It uses lessons learned from information security incidents to reduce the likelihood of future incidents

What is important ?

- Apply it to both internal and external people
- Frequency of awareness and training
- Diversification of media support
- Management Commitment
- Reminder of standards, law and regulations
- Incident notification procedure
- Point of contact in the event of a security incident

Which proofs are needed ?

- Documented programme and plan
- Records showing initial and periodic awareness conducted
- Records of assessment results (e.g., quiz scores) to test knowledge transfer
- Documentation showing the awareness program incorporates lessons learnt from information security incidents

Link with other frameworks

- NIST 800-53 rev5 : AT-2, AT-3, CP-3, IR-2, PM-13
- NIST CSF 2.0 : PR.AT-01, PR.AT-02

Renaud Dardenne
Asphalia Consulting