Information security event reporting

ISO 27002 Control 6.8

Control

The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner

Purpose

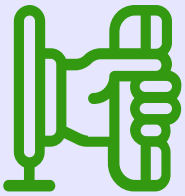
To support timely, consistent and effective reporting of information security events that can be identified by personnel

Why is it important?

- Timely reporting is crucial for effective information security incident management
- It ensures potential incidents, vulnerabilities, and control weaknesses are brought to attention quickly
- Unauthorized testing of vulnerabilities can cause damage to systems or corrupt digital evidence

The process should address :

- Security Event Reporting Process
- Communication of the process to internet and external staff
- Definition of the point of contact in the event of a security event
- Example of security events
- Privacy breach, policy non-compliance, unapproved system change, malfunction, vulnerability
- Prohibition of proving vulnerabilities



What could go wrong with it?

- Delay in response or failure to contain an incident due to late reporting
- Individual legal liability for users who test vulnerabilities
- Damage or corruption of digital evidence (5.28) if unauthorized actions are taken
- Personnel should try to determine the cause or severity before reporting (reporting must be timely to minimize effect)

Link with other frameworks

- NIST 800-53 rev5 : AU-6, IR-6, SI-2
- NIST CSF 2.0 : PR.AA-02, PR.AA-05

Renaud Dardenne
Asphalia Consulting