Physical security monitoring

ISO 27002 Control 7.4

Control

Premises should be continuously monitored for unauthorized physical access

Purpose

To detect and deter unauthorized physical access

Why is it important?

- It acts as a preventive and detective measure against unauthorized physical access or suspicious behavior
- Monitoring systems must be protected from unauthorized access to prevent compromise or disabling
- It ensures compliance with local laws regarding surveillance and retention of PII/video data

How can it be implemented ?

- Monitor physical premises continuously using surveillance systems (guards, intruder alarms, video systems)
- Install and periodically test intruder alarms (contact, sound, or motion detectors)
- Protect monitoring systems from unauthorized access (e.g., accessing video feeds or remote disabling)
- Ensure monitoring and recording complies with local laws and regulations, including PII protection and video retention periods

Which recurrent activities need to be carried out ?

- Access to buildings housing critical systems is continuously monitored
- Alarms and detectors are regularly tested
- Monitoring system designs are kept confidential

Link with other frameworks

- NIST 800-53 rev5 : AU-6(6)*, PE-3, PE-3(3), PE-6, PE-6(1), PE-6(4)*
- NIST CSF 2.0 : GV.OC-04, GV.OC-05, PR.AA-06, PR.AT-02, PR.IR-02

Renaud Dardenne
Asphalia Consulting