

Screening

ISO 27002 Control 6.1

Control

Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks

Purpose

To ensure all personnel are eligible and suitable for the roles for which they are considered and remain eligible and suitable during their employment



Why is it important?

- Proper screening is a prerequisite for assigning trust, especially for roles involving access to confidential information
- Periodic verification confirms ongoing suitability of personnel, depending on the criticality of their role

How can it be achieved ?

- Internal and external people are in scope
- By defining a selection procedure
- Checking references
- Checking the resume / Curriculum vitae
- Ensuring the correct qualification and certification
- Verifying the identity
- Background checks / criminal record for specific positions
- Screening must be proportional to the risks and the classification of information to be accessed



Which proofs are needed ?

- Documented screening process and procedures
- Records showing the completion of satisfactory references
- Confirmation records of academic and professional qualifications
- Documentation of the criteria and limitations for verification reviews
- Documentation of repeated checks performed periodically.

Link with other frameworks

- NIST 800-53 rev5 : PS-3, SA-21
- NIST CSF 2.0 : GV.RR-04, PR.DS-01, PR.DS-02, PR.DS-10



Renaud Dardenne
Asphalia Consulting