Segregation of duties

ISO 27002 Control 5.3

Control

Conflicting duties and conflicting areas of responsibility should be segregated

Purpose

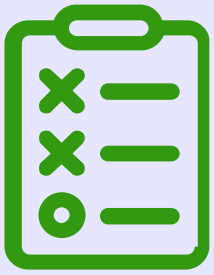
To reduce the risk of fraud, error and bypassing of information security controls

Why is it important ?

- to separate conflicting duties between different individuals in order to prevent one individual from executing potential conflicting duties on their own
- To avoid the possibility of collusion

In which area is it typically defined ?

- Change Management
- Procurement
- Access Management
- IT development *Vs* IT Operations
- Business *Vs* Risk Management *Vs* Internal Audit



How exactly can it be achieved ?

- List all the roles in the organization
- Create a diagonal matrix to represent all the combinations
- Identify the incompatible roles and tasks
- Forbid the carrying of incompatible duties
- Accept exceptions when necessary
- Define compensating controls when needed
- Implement controls like : from 4-eyes principles, temporary accesses, or monitoring

Link with other frameworks

- NIST 800-53 rev5 : NA
- NIST CSF 2.0 : NA

Renaud Dardenne
Asphalia Consulting