ISO/IEC 27001:2013 Information security management systems
-Roles, responsibilities and segregation of duties-

Security category – 6.1. Internal organization

Control – 6.1.1. Information security roles and responsibilities
The responsibilities for information security have to be defined and allocated.

Roles and responsibilities for all personnel should be defined and clearly communicated.

Explain to individuals in the organization what is expected of them.

All staff should have a basic responsibility for security included in job descriptions and should understand their security responsibility.

Information security manager – ok, but not enough.

ISO/IEC 27001:2013 Information security management systems
-Roles, responsibilities and segregation of duties-

Control – 6.1.2. Segregation of duties
There should be measures in place so that duties and areas of responsibility that are in conflict be segregated.

Segregation - reduces opportunities for unauthorized or unintentional modification of misuse of assets.

Principles:
- initiation of an event should be separated from its authorization;
- no single person should be able to access, modify or use assets without authorization or detection

ISO/IEC 27001:2013 Information security management systems

-Roles, responsibilities and segregation of duties-

Dividing the job between 2 or more staff provides a system of verification of one by the other (ex. 2 keys or passwords).

Barings bank collapse – classical example of a lack of segregation of duties (https://en.wikipedia.org/wiki/Barings_Bank)

Segregation of duties – more difficult to implement for small companies (if its not possible record all activities and to review the records independently to identify suspicious or unauthorized activity)