ISO/IEC 27001:2013 Information security management systems
- Information security risk assessment-

The organization is required to develop and apply a risk assessment process.

1. Start from information assets and try to identify the threats and vulnerabilities related to the assets

2. Evaluate impact if the confidentiality, integrity or availability of the information are compromised

3. Calculate the likelihood (or probability) of an event happening

4. Estimate the level of risk as a combination of impact and likelihood

5. Assign risk owners

6. Define what is considered acceptable risk and what is not acceptable

ISO/IEC 27001:2013 Information security management systems

- Information security risk assessment-

Asset	Threat	Vulnerabilities	Impact	Likelihood (probability)	Risk level	Acceptable? Y/N	Risk Owner
Information stored on mobile devices	Theft	No access security control (password or Touch ID). No settings for installed for remote wiping of data	Estimation of the damages	How probable is this to happen	Impact x Likelihood		

ISO/IEC 27001:2013 Information security management systems
- Information security risk assessment-

Estimation of impact, likelihood and risk level:

Qualitative – use levels (ex. "high", "low", "medium“)
Quantitative - use numbers
Semi-quantitative - using numerical ratings to generate a level

Establish criteria:
Acceptable risk / Not acceptable risk

Risk owners- persons (structures) who are accountable for the management of the management of the risk

ISO/IEC 27001:2013 Information security management systems
- Information security risk assessment-

Risk assessment is subjective!

…but you should create a list of risks as comprehensive as possible

ISO standards on risk assessment:
ISO 31000, IEC 31010, ISO/IEC 27005

Risk assessment should be documented