Catalogue of threats & vulnerabilities

This list of threats and vulnerabilities can serve as a help for implementing risk assessment within the framework of ISO 27001 or ISO 22301. This list is not final – each organization must add their own specific threats and vulnerabilities that endanger the confidentiality, integrity and availability of their assets.

Threats

Threat	Vulnerabilities
Below is a list of threats – this is not a definitive list, it must be adapted to the individual organization: • Access to the network by unauthorized persons • Bomb attack • Bomb threat • Breach of contractual relations • Breach of legislation • Compromising confidential information • Concealing user identity • Damage caused by a third party • Damages resulting from penetration testing • Destruction of records • Disaster (human caused) • Disaster (natural) • Disclosure of information • Disclosure of passwords • Eavesdropping • Embezzlement • Errors in maintenance • Failure of communication links • Falsification of records • Fire • Flood • Fraud • Industrial espionage • Information leakage • Interruption of business processes	Below is a list of vulnerabilities – this is not a definitive list, it must be adapted to the individual organization: • Complicated user interface • Default passwords not changed • Disposal of storage media without deleting data • Equipment sensitivity to changes in voltage • Equipment sensitivity to moisture and contaminants • Equipment sensitivity to temperature • Inadequate cabling security • Inadequate capacity management • Inadequate change management • Inadequate classification of information • Inadequate control of physical access • Inadequate maintenance • Inadequate network management • Inadequate or irregular backup • Inadequate password management • Inadequate physical protection • Inadequate protection of cryptographic keys • Inadequate replacement of older equipment • Inadequate security awareness • Inadequate segregation of duties • Inadequate segregation of operational and

• Loss of electricity • Loss of support services • Malfunction of equipment • Malicious code • Misuse of information systems • Misuse of audit tools • Pollution • Social engineering • Software errors • Strike • Terrorist attacks • Theft • Thunder-stroke • Unintentional change of data in an information system • Unauthorized access to the information system • Unauthorized changes of records • Unauthorized installation of software • Unauthorized physical access • Unauthorized use of copyright material • Unauthorized use of software • User error • Vandalism	testing facilities • Inadequate supervision of employees • Inadequate supervision of vendors • Inadequate training of employees • Incomplete specification for software development • Insufficient software testing • Lack of access control policy • Lack of clean desk and clear screen policy • Lack of control over the input and output data • Lack of internal documentation • Lack of or poor implementation of internal audit • Lack of policy for the use of cryptography • Lack of procedure for removing access rights upon termination of employment • Lack of protection for mobile equipment • Lack of redundancy • Lack of systems for identification and authentication • Lack of validation of the processed data • Location vulnerable to flooding • Poor selection of test data • Single copy • Too much power in one person • Uncontrolled copying of data • Uncontrolled download from the Internet • Uncontrolled use of information systems • Undocumented software • Unmotivated employees • Unprotected public network connections • User rights are not reviewed regularly