Assess risks M 22

type	management process
purpose	• achieve ISMS objectives • establish information security risk criteria • identify, analyze and assess IS risks • improve the overall performance of the company
owner	director / IS manager / project leader
risks	• not taking into account the business context • not understanding the requirements of interested parties • not identifying the risks • not analyzing the risks • not assessing the risks • not establishing the risk acceptance criteria • not keeping the risk acceptance criteria up to date • failing to identify the risk owners • not reviewing the indicators
upstream processes	• carry out FMEA • plan the ISMS
downstream processes	• treat risks • establish process ownership • communicate • satisfy requirements
inputs	• context of the organization • requirements of interested parties • necessary resources • conditions (normal and abnormal) • any identified risk • IT purchases
activities (sub-processes)	• establish the risk acceptance criteria • identify the risks • assign risks to owners • analyze the risks • assess the risks • make staff aware of the risks • communicate • retain documented information on risk assessment
outputs	• risk acceptance criteria • list of risks • risk levels • list of risk owners • staff awareness
resources	direction, department managers, process owners, risk owners
indicators	• identified risks • assessed risks
procedures / documents	continual improvement, communication, internal audits, training, planning, change management, purchasing, process control, data analysis, inspection / strategic plan, policy, objectives, indicators, list of risks, action plans, list of processes, process sheets, customer satisfaction survey, change requests, reports, FMEA
customers	all staff and processes, interested parties

Glossary:

- ISMS: information security management system
- IS: information security
- IT: information technology
- FMEA: failure mode and effect analysis

title / codification	purpose	owner
assess risks / M 22	• achieve ISMS objectives • establish information security risk criteria • identify, analyze and assess IS risks • improve the overall performance of the company	director / IS manager / project leader

upstream processes	risks	downstream processes
• carry out FMEA • plan the ISMS	• not taking into account the business context • not understanding the requirements of interested parties • not identifying the risks • not analyzing the risks • not assessing the risks • not establishing the risk acceptance criteria • not keeping the risk acceptance criteria up to date • failing to identify the risk owners • not reviewing the indicators	• treat risks • establish process ownership • communicate • satisfy requirements

inputs	activities	outputs
• context of the organization • requirements of interested parties • necessary resources • conditions (normal and abnormal) • any identified risk • IT purchases	• establish the risk acceptance criteria • identify the risks • assign risks to owners • analyze the risks • assess the risks • make staff aware of the risks • communicate • retain documented information on risk assessment	• risk acceptance criteria • list of risks • risk levels • list of risk owners • staff awareness

resources	indicators	procedures / documents	customers
direction, department managers, process owners, risk owners	identified risks, assessed risks	continual improvement, communication, internal audits, training, planning, change management, purchasing, process control, data analysis, inspection / strategic plan, policy, objectives, indicators, list of risks, action plans, list of processes, process sheets, customer satisfaction survey, change requests, reports, FMEA	all staff and processes, interested parties