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

purpose

owner

title / codification

director / IS manager / project leader

* achieve ISMS objectives
* establish information security risk criteria
* identify, analyze and assess IS risks
* improve the overall performance of the company

assess risks /

M 22

downstream processes

upstream processes

risks

* treat risks
* establish process ownership
* communicate
* satisfy requirements
* 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

activities

inputs

outputs

* 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
* context of the organization
* requirements of interested parties
* necessary resources
* conditions (normal and abnormal)
* any identified risk
* IT purchases
* risk acceptance criteria
* list of risks
* risk levels
* list of risk owners
* staff awareness

indicators

procedures / documents

customers

resources

identified risks, assessed risks

all staff and processes, interested parties

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

direction, department managers, process owners, risk owners