

Manage assets R 55

type	realization process
purpose	<ul style="list-style-type: none"> • identify the assets of the organization • preserve assets • assign a manager (owner) for each asset
owner	information security manager
risks	<ul style="list-style-type: none"> • not identifying and inventorying certain assets • failing to assess the risks associated with the assets • not understanding the requirements of interested parties • not taking into account the identified risks • not attribute assets to persons • fail to preserve assets • do not manage incidents • not have all the licenses of the software used • not having an exhaustive inventory of assets
upstream processes	<ul style="list-style-type: none"> • plan the ISMS • assess risks • treat risks • acquire and maintain infrastructure • implement information security • buy
downstream processes	<ul style="list-style-type: none"> • maintain equipment • manage the ICT chain • manage incidents • manage configuration • manage changes • improve
inputs	<ul style="list-style-type: none"> • available assets • identified risks • returned assets • new assets
activities (sub-processes)	<ul style="list-style-type: none"> • identify the assets of the organization: <ul style="list-style-type: none"> ○ material ○ software ○ virtual machines ○ facilities ○ records • keep the inventory of assets up to date (changes, new assets) • assign the owner and location of the asset in the inventory • manage the return of assets (end of contract or change of position) • establish the links between the different assets • set restrictions for each asset • classify the assets according to their importance: <ul style="list-style-type: none"> ○ most critical ○ most expensive to protect ○ most expensive to replace
outputs	<ul style="list-style-type: none"> • inventory of assets • instructions concerning certain assets
resources	technical and IT resources, licenses
indicators	<ul style="list-style-type: none"> • information availability rate • incident rate
procedures / documents	access rights, ICT chain, access restrictions, incidents, access restrictions, vulnerability management / registration and deregistration, access distribution, incident register
customers	all staff

Glossary:

ICT: information and communication technology

title / codification
manage assets / R 55

purpose
<ul style="list-style-type: none"> • identify the assets of the organization • preserve assets • assign a manager (owner) for each asset

owner
information security manager

upstream processes
<ul style="list-style-type: none"> • plan the ISMS • assess risks • treat risks • acquire and maintain infrastructure • implement information security • buy

risks
<ul style="list-style-type: none"> • not identifying and inventorying certain assets • failing to assess the risks associated with the assets • not understanding the requirements of interested parties • not taking into account the identified risks • not attribute assets to persons • fail to preserve assets • do not manage incidents • not have all the licenses of the software used • not having an exhaustive inventory of assets

downstream processes
<ul style="list-style-type: none"> • maintain equipment • manage the ICT chain • manage incidents • manage configuration • manage changes • improve

inputs
<ul style="list-style-type: none"> • available assets • identified risks • returned assets • new assets

activities
<ul style="list-style-type: none"> • identify the assets of the organization: <ul style="list-style-type: none"> ○ material ○ software ○ virtual machines ○ facilities ○ records • keep the inventory of assets up to date (changes, new assets) • assign the owner and location of the asset in the inventory • manage the return of assets (end of contract or change of position) • establish the links between the different assets • set restrictions for each asset • classify the assets according to their importance: <ul style="list-style-type: none"> ○ most critical ○ most expensive to protect • most expensive to replace

outputs
<ul style="list-style-type: none"> • inventory of assets • instructions concerning certain assets

resources
technical and IT resources, licenses

indicators
information availability rate, incident rate

procedures / documents
access rights, ICT chain, access restrictions, incidents, access restrictions, vulnerability management / registration and deregistration, access distribution, incident register

customers
all staff