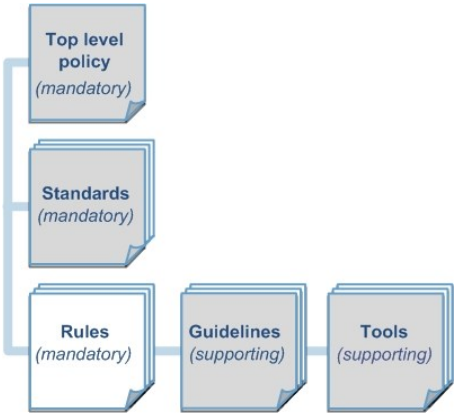
KPN Security Policy

KSP – Rule

Title	**Business Continuity Management**
ID	**KSP-FA09-RL01**
Funct. Area	09 – Business Continuity
Date	3 February 2017
Version	v3.2
Status	Approved
Owner	CISO



Summary

This document describes the steps that must be taken to identify potential threats to an organization and the impact to business operation that those threats, if realized, might cause. Furthermore it describes the requirements that must be implemented to comply to law and regulation and to protect KPN Business and client interest.

To be consistent throughout the organisation, all reporting units must use the same tools and methods as defined or referenced in the KPN Security Policy.

Version history

Version	*Date*	*Comments*
v1.0	17 September 2013	Approved in SSM
v1.1	9 October 2013	Updated based on consistency check
v2.0	1 August 2014	Update based on feedback from Q4 2013 and Q1 2014
v2.1	14 August 2014	Update based on feedback and required additions
v3.0	1 January 2015	Policy review for KSP-FA09 as of 1/1/2015
v3.1	20 July 2015	Update based on adjusted tooling
v3.2	3 February 2017	Added the Scope Document to process

ID	KSP-FA09-RL01-R01
Titel	Determine Scope
Omschrijving	Determine what the scope of the service (that we deliver to customers) or “halffabricaat” is. Determine and tune the scope of the object with the stakeholders, in order to be able to assess the risks. Determining the scope must be done in KSP-FA09-TL09 ‘Scope Document’. The template is obligatory. The results must be delivered to CISO.
Gerelateerde documenten	KSP-FA09-TL09 - Scope document

ID	KSP-FA09-RL01-R02
Title	Business Impact Analysis (BIA)
Description	Yearly, or in case of newly developed or significantly changed functionality, a (Business) Impact Analysis (BCM BIA) must be performed to identify the impact of prolonged unavailability, due to a worst case scenario, of a service of a building from a customers, society as well as a KPN point of view. Therefor the KSP-FA09-TL01 BCM BIA and the KSP-FA09-TL08 BCM IA are mandatory tools. The tools must be filled in by the responsible Product Manager or owner of the building, and be approved by the responsible manager. Hereafter the completed tool must be send to CISO.
Relating document	KSP-FA09-TL01 - BCM Business Impact Analysis (BCM BIA) KSP-FA09-TL08 - BCM Impact Analysis (BCM IA) For Business customers an additional template is available with specified processes

ID	KSP-FA09-RL01-R03
Title	Risk Assessment
Description	For services, “halffabricaten” or buildings , High or Critical (Medium if Telecom Law relevant), according to BIA output, yearly a Risk Assessment must be performed to have an actual overview of risks, identified Single Points of Failure (SPoFs) and environmental risks. The identified risks must be evaluated by the responsible Service owner or Manager to define whether the Risks has to be mitigated by taking measures or by accepting Risks according to the Procuration Matrix (Shared Service Organisation). The BCM Risk Tool must be filled in and approved by the responsible Manager. The completed BCM Risk Tool must be send to CISO.
Relating document	KSP-FA09-TL01 - BCM Business Impact Analyses (BCM BIA) KSP-FA09-TL02 - BCM Risk Tool (BCM RT) KSP-FA09-TL08 - BCM Impact Analysis (BCM IA)

ID	KSP-FA09-RL01-R04
Title	BCM Risk Acceptance
Description	Accepted Risks must be registered in the BCM Risk tool supplied by argumentation. The accepted Risks in the BCM Risk Tool must be approved by the responsible manager by the right level according to the procuration matrix,
Relating document	KSP-FA09-TL02 - BCM Risk Tool (BCM RT) Procuration Matrix (Shared Service Organization Finance)

ID	KSP-FA09-RL01-R05
Title	BCM Risk Mitigation
Description	Identified risks which are assessed to be mitigated must be supplied with mitigating measures. The implementation of mitigating measures must be justified by the responsible Manager based on a business case. The implementation status of the mitigating measures must be actual and available. Risks which are mitigated must be approved by the responsible Manager to the level according to the Procuration Matrix.
Relating document	KSP-FA09-TL02 - BCM Risk Tool (BCM RT) Procuration Matrix (Shared Service Organization Finance)

ID	KSP-FA09-RL02-R06
Title	Business Continuity Plans
Description	Continuity plans must be created and stored in a central repository, and must at all times be accessible even if KPN internal (office) infrastructure is malfunctioning. Continuity plans must be reviewed at least annually and updated if needed.
Relating document	Continuity Plans (Service Continuity Plan (SCP), Business Continuity Plan (BCP), Chain Recovery Plan (CRP), Technical Recovery Plan (TRP).

ID	KSP-FA09-RL01-R07
Title	Exercise Business Continuity Plans
Description	All continuity plans (SCPs/BCPs/CRPs/TRPs) and all technical solutions that are created to mitigate continuity risks must be exercised at least once a year or when major changes occur. Exercises must be prepared and evaluated in an exercise report. Recommendations must be decided on succession and implemented within agreed timeline.
Relating document	KSP-FA09-GL02 - BCM Handboek

ID	KSP-FA09-RL01-R08
Title	Reporting Incidents
Description	Be Alert incidents with orange or red classification on Telecom Law relevant services must be registered by SQC to AT website within 24 hours and to CISO. When needed follow-up messages must be registered when classification changes or when updates are available.
Relating document	N/A