Overview of selected KPN Security Policies

Creation date: Thursday, May 9, 2019 9:30:59 AM

Selected by: Ruud Leurs

Requirement	**Mass disruption affects maximum 100.000 customers**
Description	The impact of a critical service must be limited to a maximum of 100.000 customers per incident in the KPN Domain. Design and implementation should be adequate to the extent that with an incident, the impact is never larger than 100.000 customers, unless there is a near-realtime switch to a redundant element with adequate capacity.
ID	KSP-RE-557
Version	1.0
Date	December 11, 2017
Rationale	BCM services

Requirement	**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 in the service, service component, application or building occur. The dates of the planned excercises and tests must be delivered to CISO beforehand. Exercises must be evaluated in an exercise report and delivered to CISO. Recommendations must be decided on succession and implemented within the timeline as stated in the report. For continuity plans of Managed Service Providers (MSP) related to their own services to KPN, also the dates of the planned excercises and tests and related reports must be delivered to CISO. If the continuity plans are related solely to the assets of the MSP itself, then only the dates of the planned excercises or tests and the final results need to be shared with CISO.
ID	KSP-RE-570
Version	1.3
Date	February 1, 2019
Rationale	BCM services
Rationale	BCM service components
Rationale	BCM applications
Rationale	BCM buildings

Requirement	**Determine Scope**
Description	For each Service, Service Component (“halffabricaat”) or Application must the scope (for which the risks must be evaluated) be determined in QCarbon, in accordance with KSP-GL-591 ‘Scope Document’. The use of QCarbon or the template is obligatory. The results must be delivered to CISO.
ID	KSP-RE-564
Version	1.2
Date	November 2, 2018
Rationale	BCM services
Rationale	BCM service components
Rationale	BCM applications
Rationale	BCM buildings

Requirement	**Defining KPN Critical Services and related requirements**
Description	The **selection criteria** for KPN Critical Services are based on the impact that a severe disruption of the service may cause conform the KPN Impact in the BCM Business Impact Analyses: Financial impact: loss of sales $\geq$ €6M and/or cost of recovery $\geq$ €6M; Reputation damage: great loss of (potential) customers; Major social disruption (1-1-2 unreachability always highest impact). The requirements regarding the **maximum impact** of a a failure of a KPN Critical Service are: Max. 100.000 affected connections* caused by the failure; $\leq$ 4 hours outage for more than 10.000 affected connections*; Regional impact (max 100.000 connections*) for fixed and mobile services; Max. 1 regional incident per year (no repeating failures for the same customers); Connections: for business customers the number of total connections affected are counted. For the KPN Critical Services the operation of the **BCM Architecture Guidelines** (KSP-GL-582) is mandatory. Contractual agreements can overrule the above requirements by having to meet more stringent requirements. For KPN Critical Services **each three years a table-top chain exercise** must be done. This to check the correct and timely interoperability of continuity plans and crisis management in all involved parts of the organization. A real incident invoking these plans and crisis management process may also fulfil this requirement when the underlying evidence and evaluation report are adequate. This is judged by the CISO Office. The list KPN Critical Services is prepared annually by the CISO Office for approval by KPN topmanagement, and published in the KPN Security Policy (KSP-GL-587).
Supplement	Applying focus to the services with major impact because of financial, reputational or social importance.
ID	KSP-RE-575
Version	1.3
Date	May 3, 2019

Rationale	BCM services

Requirement	**Business Impact Analysis (BIA)**
Description	Yearly, or in case of newly developed (innovcation) or significantly changed functionality, must be determined what the impact of prolonged unavailability is due to a worst case scenario of a Service, Service Component, Application or a Building from a customer, society as well as a KPN point of view . The classification of a Service must be done with BIA in QCarbon, the classification of a Service Component, an Applcation or a Building with the IA in QCarbon or with KSP-GL-590 - BCM IA. These are mandatory tools. The tools must be filled in by the responsible Product Manager of the Service or Service Component or the owner of the Application or Building, and be approved by the responsible manager. Hereafter the completed tool must be send to CISO.
Related info	For Business customers an additional template is available with specified processes
ID	KSP-RE-565
Version	1.2
Date	November 2, 2018
Rationale	BCM services
Rationale	BCM service components
Rationale	BCM applications
Rationale	BCM buildings

Requirement	**Risk Assessment**
Description	For Services, Service Components (Halffabrikaten) and Applications, High or Critical (Medium if Telecom Law relevant), and for critical or high classified Buildings according to BIA/IA output, yearly a Risk Assessment must be performed to have an actual overview of risks, identified Single Points of Failure (SPoFs) and environmental risks. As inventory of BCM risks is the use of the threats in KSP-GL-714 - BCM Threats list for Risk Assessment mandatory. The identified risks must be evaluated by the responsible Asset owner or Manager to define whether the risks have to be mitigated by taking measures or by accepting risks according to the Procuration Matrix (Shared Service Organisation). The BCM Risk Tool or QCarbon must be filled in and approved by the responsible manager. The completed BCM Risk Tool must be send to CISO.
ID	KSP-RE-566
Version	1.2
Date	November 2, 2018
Rationale	BCM services
Rationale	BCM service components
Rationale	BCM applications
Rationale	BCM buildings

Requirement	**BCM Risk Acceptance**
Description	Risks may only be accepted by the responible manager who, according to the procuration matrix, is allowed to sign for the amount of money of the worst case impact of the risk, together with an mandatory argumentation for the reason of accepting the risk.
Related info	Procuration Matrix (Shared Service Organization Finance)
ID	KSP-RE-567
Version	1.1
Date	November 2, 2018
Rationale	BCM services
Rationale	BCM service components
Rationale	BCM applications
Rationale	BCM buildings

Requirement	**BCM Risk Mitigation**
Description	Identified risks 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. Mitigatation measures must be approved by the responsible Manager to the level according to the Procuration Matrix.
Related info	Procuration Matrix (Shared Service Organization Finance)
ID	KSP-RE-568
Version	1.1
Date	November 2, 2018
Rationale	BCM services
Rationale	BCM service components
Rationale	BCM applications
Rationale	BCM buildings

Requirement	**Defining NL Vital Services and related requirements**
Description	Basic criterium for a service in this category is that the government defines the requirements completely or in a large extent. Additionally the service has to meet one or more of the following criteria: Public Order and (Inter)national Security agencies are operationaly dependent of the delivery of the service. The service requires screened personnel and is used for the processing of state secret labelled information. Loss of integrity may lead to great communication stroke of government. The service is crucial for communication during emergency or a crises. The service is a last resort service when all other regular services are disrupted. For the NL Vital Services the operation of the BCM Architecture Guidelines (KSP-GL-582) is mandatory. The other requirements are defined by the specifications of the government as described in the contract. Every two years a KWAS (Dutch: Kwetsbaarheden Analyse Spionage, English: vulnerability analsysis espionage) must be executed for the NL Vital Services, unless major changes or a specific incidents require a direct review. The confidential list NL Vital Services is prepared annually by the CISO Office for approval by KPN topmanagement, and is maintained by the CISO Office.
Supplement	A vital Service is a service that is of crucial importance for Public Order and (Inter)national Safety of the Dutch society. Not only availability, but confidentiality of information processed in the service is important: based on a specific directive classified information defined in law and legislation (wet op het staatsgeheim, VIR-BI, ABDO and others). A vital classification is focused on quite different aspects than a critical classification because of the impact to society versus the impact on KPN Business.
ID	KSP-RE-579
Version	1.2
Date	May 3, 2019
Rationale	BCM services

Requirement	**Business Continuity Plans**
Description	Continuity plans must be registered and stored in the central repository QCarbon, and must at all times be accessible even if the KPN internal (office) infrastructure is malfunctioning. This can be done by e.g. store a copy on a local pc and/or USB stick or a latest version print-out on the places where needed. Continuity plans must be reviewed on topicality at least annually or after a major change or disturbance and updated if needed. Also continuity plans from Managed Service Providers (MSP) that are related to delivery of services to KPN must be registered and stored in the central repository QCarbon, unless they are solely related to the assets of the MSP. In that case, only the header or title of the plans must be registered in QCarbon.
Related info	Continuity Plans (Service Continuity Plan (SCP), Business Continuity Plan (BCP), Chain Recovery Plan (CRP), Technical Recovery Plan (TRP)), KSP-GL-583 - BCM Handbook, KSP-RE-570 - Practising Continuity Plans.
ID	KSP-RE-569
Version	2.2
Date	February 1, 2019
Rationale	BCM services
Rationale	BCM service components
Rationale	BCM applications
Rationale	BCM buildings

Requirement	**Business Continuity Requirement Management**
Description	Yearly, or in case of newly developed or significantly changed functionality, the services, service components and applications and their continuity requirements must be reviewed or determined by the service, service component or application owner. Business Continuity requirements must reflect customer, contractual, regulatory, internal quality requirements and social demands.
Supplement	The requirements for (critical) services, service components and applications regarding availability and maximum impact of severe incidents must be set by executive management. These requirements can be: maximum impacted customers from one failure, maximum unavailability, maximum dataloss, regional or nationwide impact.
ID	KSP-RE-581
Version	1.2
Date	May 3, 2019
Rationale	Implementing changes
Rationale	BCM services
Rationale	BCM service components
Rationale	BCM applications

Requirement	**Vulnerability Analysis Industrial Security (KWAS)**
Description	A Vulnerability Analysis Industrial Security (KWAS) is mandatory to NL Vital services and critical internal KPN business processes. It is performed every two years unless a major change or a specific incident requires analysis earlier.
Supplement	KPN has certain information and networks that are (almost) nowhere else available, should not be public and are attractive to other parties to obtain commercial, criminal or strategic advantage. KPN is therefore undesirably attractive as a source of information for such parties.
ID	KSP-RE-722
Version	1.0
Internal use	Yes, internal use only
Date	November 2, 2018
Rationale	BCM services
Rationale	BCM processes