Overview of selected
KPN Security Policies

Creation date: Wednesday, November 7, 2018 3:45:37 PM

Selected by: Ruud Leurs

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. Exercises must be prepared and evaluated in an exercise report. Recommendations must be decided on succession and implemented within the timeline as stated in the report.
ID	KSP-RE-570
Version	1.2
Date	November 2, 2018
Rationale	Determine BCM planning & process

Requirement	**Business Continuity Management Governance**
Description	Responsibilities for Business Continuity Management must be defined.
Supplement	Without a clear understanding of roles and responsibilities it will be practically impossible to implement regulatory, customer and KPN Business requirements for business continuity in a consistent manner.
ID	KSP-RE-571
Version	1.0
Date	December 11, 2017
Rationale	Determine BCM planning & process
Rationale	Top Level Policy

Requirement	**BCM Planning**
Description	On a yearly basis, a BCM plan on segment and department level (each unit delivering a monthly Management Letter) must be drafted.
Supplement	Insight must be provided into the following activities: • Yearly cycle of the BCM Process; • Yearly review of existing BCM documentation; • By management approved Risk appetite; • By management approved budget and required staff needed for the realization of th BCM plan; • Timelines; • Commitment from stakeholders of the delivered services outside the unit.
ID	KSP-RE-572
Version	1.1
Date	November 2, 2018
Rationale	Determine BCM planning & process

Requirement	**BCM Process**
Description	A Business Continuity Management process must be implemented for services, service components, buildings and applications that will identify continuity risks and determine, implement and check, the mitigating measures where regulations require action or continuity risks exceed risk appetite.
Supplement	To have insight in the BCM risks of services, service components, buildings and applications. This enables the organization to realize a comprehensive framework of mitigating measures to prevent situations that threaten the continuity of the organization and minimize the resulting harm as much as possibe in the case that a calamity happens.
ID	KSP-RE-573
Version	1.2
Date	November 2, 2018
Rationale	Determine BCM planning & process

Requirement	**Business Continuity Framework reporting**
Description	On a quarterly basis the Business Continuity status of continuous delivery for all approved critical services, service components (“halffabricaten”) and critical applications must be reported by the service owner or application owner to CISO. All reporting units must use the same Business Continuity Framework.
Supplement	To compile an corporate BCM status overview for KPN, and in order to report both internally and externally in a consistent manner, it is mandatory that all reporting units (that deliver a monthly Management Letter) use the same methodology and reporting methods, as prescribed by the CISO. The framework will encompass as well regulatory and KPN requirements. The BCM status of continuous delivery for all approved critical services, critical service components and critical applications must be reported quarterly to CISO, including BCM BIA or IA ((Business) Impact Analysis) status, BCM RT (Risk Tool) status, status of the risk mitigating measures and the Continuity Plan test execution and results status.
ID	KSP-RE-574
Version	1.2
Date	November 2, 2018
Rationale	Determine BCM planning & process

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	Determine BCM planning & process

Requirement	**Evaluation of and defining requirements to Critical Services**
Description	On a yearly basis, the business critical services must be defined and evaluated. To accomplish this the KPN impact classification of all services must be defined by means of the BCM Business Impact Assessment (BCM BIA) and reported to CISO. CISO uses this information to complete the proposal Critical Services overview in Q4 which must be approved by executive management in OLT and CCLT. The selection criteria for KPN’s Critical Services are based on the impact that a severe disruption of service may cause (as mentioned in the BCM BIA): • Financial impact: loss of sales ≥ €6M and/or cost of recovery ≥ €6M; • Reputation damage: great loss of (potential) customers; • Major social disruption (1-1-2 unreachability always highest impact). The requirements regarding to the maximum impact a failure may have on the service are the following: • Max. 100.000 affected connections* caused by the failure; • ≤ 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 Contractual agreement scan overrule above requirements. For critical services, each three years a table-top chain exercise must be held 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.
Supplement	Applying focus to the services with major impact because of financial, reputational or social importance.
ID	KSP-RE-575
Version	1.1
Date	November 2, 2018
Rationale	Determine BCM planning & process

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	Determine BCM planning & process

Requirement	**Evaluating and defining Critical Buildings and their requirements.**
Description	Each year, the classification for KPN Telecom buildings and data centers must be reassessed by means of the BCM Impact Analysis. CISO maintains an overview of critical Buildings. Critical buildings must be assessed annually on compliancy with the requirements critical buildings. For each critical building a Continuity Plan must be developed and yearly exercised/tested.
Supplement	Several (technical) KPN buildings are used by many critical services. If such a building, or a part of it, fails this will potentially impact many customers for a prolonged period of time. Examples of technical buildings can be: Datacenters, Core-locations, Regional Hubs, Networkmanagement centers.
ID	KSP-RE-576
Version	1.1
Date	November 2, 2018
Rationale	Determine BCM planning & process

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	Determine BCM planning & process

Requirement	**Invoke continuity plans**
Description	Continuity plans must be invoked in case of events/incidents impacting the availability of KPN services.
Supplement	Continuity Plans are created and maintained and exercised yearly to make sure that the organization is prepared when a major incident occurs. Continuity Plans When serious incidents occur, the prepared continuity plans, if available, must be used to mitigate the impact.
Related info	Business Continuity Plan (BCP), Service Continuity Plan (SCP), IT Chain Recovery Plan (CRP), Technical Recovery Plan (TRP) formats opgeleverd aan het CISO Office.
ID	KSP-RE-577
Version	1.0
Date	December 11, 2017
Rationale	Determine BCM planning & process

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	Determine BCM planning & process

Requirement	**Corporate Crisis Management**
Description	For crisis situations threatening the company as a whole, or as directed by the government, the executive management must be able to manage these situations, and must be trained yearly.
Supplement	Severe crisis may be of great danger for the continuity of KPN as a whole. Besides that KPN must, because of law and regulation, be prepared to crisis situations issued and directed by government. Furthermore KPN, as a Telco, has great responsibilities towards society.
Related info	Corporate Crisis Management Plan (confidential)
ID	KSP-RE-578
Version	1.0
Date	December 11, 2017
Rationale	Determine BCM planning & process

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	Determine BCM planning & process

Requirement	**Evaluation and defining NL Vital Services**
Description	Yearly the NL Vital Services must be evaluated and defined. **Basic criterium** for a service in this category is that **the Government A vital service is specified by government defines the requirements completely or in a large extent**. Beneath follow the criteria that each are a sufficient reason to classify the service as ‘NL vitaal’: 1. Public Policy and (Inter)national Security agencies are operationalely dependent of the delivery of the service. 2. The service requires screened personnel because of the processing of state secret labelled information. 3. Loss of integrity may lead to great communication efforts of government. 4. The service is crucial for communication during emergency or a crises. 5. Last resort service when all other regular services are disrupted. CISO prepares, based on above requirements, the list of vital services to be approved by executive management. These services get an annotation in this list of NL vital services. However services can be as well KPN Critical as NL Vital for the Dutch society. Two examples of Vital Services are PKI (certificate services) and C2000 (parts T2000 and COV). The applicable requirements are defined by the specifications of government as specified in the contract. Bi-yearly a KWAS (Kwetsbaarheden Analyse Espionage) must be executed for NL Vital Services unless major changes or a specific incident require early action.
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	1.1
Date	August 16, 2018

Rationale	Determine BCM planning & process

Requirement	**Business Continuity Plans**
Description	Continuity plans must be created and stored in a central repository and registered in QCarbon, and must at all times be accessible even if KPN internal (office) infrastructure is malfunctioning. Continuity plans must be reviewed, exercised and tested at least annually or after a major change and updated if needed. Exercise and test planning and results must be reported to CISO. The title (not the plan itself) and exercise and test dates and results of Continuity plans of MSPs must be delivered to CISO.
Related info	Continuity Plans (Service Continuity Plan (SCP), Business Continuity Plan (BCP), Chain Recovery Plan (CRP), Technical Recovery Plan (TRP))
ID	KSP-RE-569
Version	2.1
Date	November 2, 2018
Rationale	Determine BCM planning & process

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