

Thursday, August 30, 2018 3:13:48 PM

Ruud Leurs

<b>Requirement</b>	<b>Exercise Business Continuity Plans</b>
<b>Description</b>	<p>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.</p> <p>Exercises must be prepared and evaluated in an exercise report. Recommendations must be decided on succession and implemented within agreed timeline.</p>
<b>ID</b>	KSP-RE-570
<b>Version</b>	1.1
<b>Date</b>	August 16, 2018
<b>Rationale</b>	Determine BCM planning & process

<b>Requirement</b>	<b>Business Continuity Management Governance</b>
<b>Description</b>	Responsibilities for Business Continuity Management must be defined.
<b>Supplement</b>	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.
<b>ID</b>	KSP-RE-571
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Determine BCM planning & process
<b>Rationale</b>	Top Level Policy

<b>Requirement</b>	<b>BCM Planning</b>
<b>Description</b>	On a yearly basis, a BCM plan on segment and department level must be drafted.
<b>Supplement</b>	<p>Insight must be provided into the following activities:</p> <ul style="list-style-type: none"> <li>• Yearly cycle of the BCM Process</li> <li>• Yearly review of existing BCM documentation</li> <li>• By management approved Risk appetite</li> <li>• By management approved budget and required staff</li> <li>• Timelines</li> <li>• Stakeholder commitment</li> </ul>
<b>ID</b>	KSP-RE-572
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Determine BCM planning & process

<b>Requirement</b>	<b>BCM Process</b>
<b>Description</b>	A Business Continuity Management process must be implemented that will identify continuity risks and determine, implement and check, the mitigating measures where regulations require action or continuity risks exceed risk appetite.
<b>Supplement</b>	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 possible in the case that a calamity happens.
<b>ID</b>	KSP-RE-573
<b>Version</b>	1.1
<b>Date</b>	August 16, 2018
<b>Rationale</b>	Determine BCM planning & process

<b>Requirement</b>	<b>Business Continuity Framework reporting</b>
<b>Description</b>	On a quarterly basis the Business Continuity status of continuous delivery for all approved critical services, Service Components ("halfabricaten") 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.
<b>Supplement</b>	<p>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 use the same methodology and reporting methods, as prescribed by the CISO. The framework will encompass as well regulatory and KPN requirements.</p> <p>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.</p>
<b>ID</b>	KSP-RE-574
<b>Version</b>	1.1
<b>Date</b>	August 16, 2018
<b>Rationale</b>	Determine BCM planning & process

<b>Requirement</b>	<b>Determine Scope</b>
<b>Description</b>	<p>Determine what the scope of the service (that we deliver to customers) or Service Component (“halffabricaat”) or Application is. Determine and tune the scope of the object with the stakeholders, in order to be able to assess the risks.</p> <p>Determining the scope must be done in QCarbon or KSP-GL-591 ‘Scope Document’. The template is obligatory. The results must be delivered to CISO.</p>
<b>ID</b>	KSP-RE-564
<b>Version</b>	1.1
<b>Date</b>	August 16, 2018
<b>Rationale</b>	Determine BCM planning & process

Requirement	Evaluation of and defining requirements to Critical Services
<b>Description</b>	<p>On a yearly basis, the business critical services must be defined and evaluated and added on the Service overview list which is administered by CISO. The KPN impact classification of all services must be defined by means of the BCM Business Impact Assessment (BCM BIA) and reported tot CISO. CISO uses this information to complete the Critical Services overview which must be approved by executive management.</p> <p>The selection criteria for KPN's Critical Services are based on the impact a severe disruption of service may cause (as mentioned in the BCM BIA):</p> <ul style="list-style-type: none"> <li>• Financial impact: loss of sales <math>\geq</math> €6M and/or cost of recovery <math>\geq</math> €6M</li> <li>• Reputation damage: great loss of (potential) customers</li> <li>• Major social disruption</li> </ul> <p>The requirements regarding to the maximum impact a failure may have on the service are the following:</p> <ul style="list-style-type: none"> <li>• Max. 100.000 affected connections* caused by the failure,</li> <li>• <math>\leq</math> 4 hours outage for more than 10.000 affected connections*</li> <li>• Regional impact (max 100.000 connections*) for fixed and mobile services</li> <li>• Max. 1 regional incident per year (no repeating failures for the same customers)</li> </ul> <p>*connections: for Business customers the number of total connections affected are counted.</p> <p>Contractual agreement scan overrule above requirements.</p> <p>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 be also fulfil this requirement when the undying evidence and evaluation report are adequate; this is judged by the CISO.</p>
<b>Supplement</b>	Applying focus to the services with major impact because of financial, reputational of social importance.
<b>ID</b>	KSP-RE-575
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Determine BCM planning & process



Requirement	Business Impact Analysis (BIA)
Description	<p>Yearly, or in case of newly developed 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 .</p> <p>The classification of a Service must be done with BIA in QCarbon, the classification of a Service Component, an Application or a Building with the IA in QCarbon or with KSP-GL-590 BCM IA. These are mandatory tools.</p> <p>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.</p>
Related info	For Business customers an additional template is available with specified processes
ID	KSP-RE-565
Version	1.1
Date	August 16, 2018
Rationale	Determine BCM planning & process

<b>Requirement</b>	<b>Evaluating and defining Critical Buildings</b>
<b>Description</b>	<p>Each year, the classification for KPN Telecom buildings and data centers must be reassessed by means of the BCM Impact Analysis (KSP-GL-590). When the building is classified critical or high subsequently a risk assessment must be carried out by means of the BCM Risk Tool.</p> <p>The results must be reported to CISO for maintaining an overview approved by executive management.</p> <p>Critical buildings must be assessed annually on compliancy with the KPN Fit For Purpose (FFP). For each critical building a Building Continuity Plan (Building BC) must be developed and exercised.</p>
<b>Supplement</b>	<p>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.</p> <p>Datacenters, Regional Hubs, SQC, etc.</p>
<b>ID</b>	KSP-RE-576
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Determine BCM planning & process

Requirement	Risk Assessment
<b>Description</b>	<p>For Services, Service Components (Halffabrikaten), Applications 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.</p> <p>As inventory of BCM risks is the use of the threats in KSP-GL-714 BCM Threats list for Risk Assessment mandatory.</p> <p>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 Procurement Matrix (Shared Service Organisation).</p> <p>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.</p>
<b>ID</b>	KSP-RE-566
<b>Version</b>	1.1
<b>Date</b>	August 16, 2018
<b>Rationale</b>	Determine BCM planning & process

<b>Requirement</b>	<b>Invoke continuity plans</b>
<b>Description</b>	Continuity plans must be invoked in case of events/incidents impacting the availability of KPN services.
<b>Supplement</b>	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.
<b>Related info</b>	Business Continuity Plan (BCP), Service Continuity Plan (SCP), IT Chain Recovery Plan (CRP), Technical Recovery Plan (TRP) formats opgeleverd aan het CISO Office.
<b>ID</b>	KSP-RE-577
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Determine BCM planning & process

<b>Requirement</b>	<b>BCM Risk Acceptance</b>
<b>Description</b>	<p>Accepted Risks must be registered in the BCM Risk tool supplied by argumentation.</p> <p>The accepted Risks in the BCM Risk Tool must be approved by the responsible manager by the right level according to the procurement matrix.</p>
<b>Related info</b>	Procurement Matrix (Shared Service Organization Finance)
<b>ID</b>	KSP-RE-567
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Determine BCM planning & process

<b>Requirement</b>	<b>Corporate Crisis Management</b>
<b>Description</b>	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.
<b>Supplement</b>	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.
<b>Related info</b>	Corporate Crisis Management Plan (confidential)
<b>ID</b>	KSP-RE-578
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Determine BCM planning & process

Requirement	BCM Risk Mitigation
Description	<p>Identified risks which are assessed to be mitigated must be supplied with mitigating measures.</p> <p>The implementation of mitigating measures must be justified by the responsible Manager based on a business case.</p> <p>The implementation status of the mitigating measures must be actual and available.</p> <p>Risks which are mitigated must be approved by the responsible Manager to the level according to the Procurement Matrix.</p>
Related info	Procurement Matrix (Shared Service Organization Finance)
ID	KSP-RE-568
Version	1.0
Date	December 11, 2017
Rationale	Determine BCM planning & process

Requirement	Evaluation and defining NL Vital Services
Description	<p>Yearly the NL Vital Services must be evaluated and defined.</p> <p><b>Basic criterium</b> for a service in this category is that <b>the Government A vital service is specified by government defines the requirements completely or in a large extent.</b></p> <p>Beneath follow the criteria that each are a sufficient reason to classify the service as 'NL vitaal':</p> <ol style="list-style-type: none"> <li>1. Public Policy and (Inter)national Security agencies are operationalely dependent of the delivery of the service.</li> <li>2. The service requires screened personnel because of the processing of state secret labelled information.</li> <li>3. Loss of integrity may lead to great communication efforts of government.</li> <li>4. The service is crucial for communication during emergency or a crises.</li> <li>5. Last resort service when all other regular services are disrupted.</li> </ol> <p>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.</p> <p>Two examples of Vital Services are PKI (certificate services) and C2000 (parts T2000 and COV).</p> <p>The applicable requirements are defined by the specifications of government as specified in the contract.</p> <p>Bi-yearly a KWAS (Kwetsbaarheden Analyse Espionage) must be executed for NL Vital Services unless major changes or a specific incident require early action.</p>
Supplement	<p>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).</p> <p>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.</p>
ID	KSP-RE-579
Version	1.1
Date	August 16, 2018



<b>Rationale</b>	Determine BCM planning & process
------------------	----------------------------------

<b>Requirement</b>	<b>Business Continuity Plans</b>
<b>Description</b>	<p>Continuity plans must be created and stored in a central repository and delivered to CISO, and must at all times be accessible even if KPN internal (office) infrastructure is malfunctioning.</p> <p>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.</p> <p>The title (not the plan itself) and exercise and test dates of Continuity plans of MSPs must be delivered to CISO.</p>
<b>Related info</b>	Continuity Plans (Service Continuity Plan (SCP), Business Continuity Plan (BCP), Chain Recovery Plan (CRP), Technical Recovery Plan (TRP).
<b>ID</b>	KSP-RE-569
<b>Version</b>	2.0
<b>Date</b>	August 16, 2018
<b>Rationale</b>	Determine BCM planning & process

Requirement	Define and evaluate critical internal KPN business processes
<b>Description</b>	<p>1. Threat</p> <p>Define the NL Vital Services and critical internal KPN business processes information that (nearly) nowhere else is available, nor should be public and is interesting for other parties, because commercial, criminal or strategic advantage can be achieved.</p> <p>2. Policy within KPN</p> <p>Within KPN a KWAS must be applied on NL Vital Services and critical internal KPN business processes with a great risk of damage.</p> <p>3. What is a KWAS?</p> <p>A Vulnerability Analysis Espionage (Kwetsbaarheden Analyse Spionage, KWAS) is a mandatory kind of internal risk analysis in which interests, vulnerabilities, ways of working with information processing in coherence are assessed by personnel directly involved with the design, maintenance and implementation of a service.</p> <p>4. Way of working within KPN</p> <p>The KWAS must be done each two years for NL Vital Services and critical internal KPN Business processes, unless a great change or specific incident demands earlier action.</p>
<b>Supplement</b>	<p>1. Threat</p> <p>The Minister of National Affairs and Kingdom relations (Binnenlandse Zaken en Koninkrijksrelaties (BZK)) takes note that economical, strategic and technical-scientific (industrial) espionage is an actual threat implies for the Dutch National Safety. The AIVD confirms that KPN possesses information and infrastructure that can damage the national safety and may be of crucial importance of (foreign) organisations and persons with other intentions. The most important vulnerabilities (and therefore espionage risks) are:</p> <ul style="list-style-type: none"> <li>• Interception of telecommunication traffic</li> <li>• Increasing intertwining and complexity of computer systems</li> <li>• Connecting of data storage systems</li> <li>• Outsourcing of maintenance and data processing</li> </ul> <p>KPN is unwanted attractive as a source of information for such parties.</p>

	<p>2. Policy within KPN</p> <p>For the internal KPN processes a KWAS is of additional value because of the structural and periodical way it looks to vulnerabilities and risks from a specific perspective, in combination with the way of working to gather information.</p> <p>The Ministry of J&amp;V has in helpful tool for this published with the KWAS process. This process is included and processed in the tool developed by CISO to be able to register the findings.</p> <p>3. What is a KWAS?</p> <p>The KWAS leads to an insight in risks that will be presented to the responsible management team for risk acceptance or risk mitigation. The insights will be reviewed each two years. KPN CISO reports monthly the progression of the KWAS status in the CISO-management letter.</p> <p>4. Way of working within KPN.</p> <p>An analysis is the first time performed in about 3 sessions of 3 hours with KPN personnel where CISO acts as a process manager. Periodical KWAS reviews are subsequently performed by the teams itself in a session of about 3 hours, in which CISO participates as an advisor.</p>
<b>Related info</b>	<p>KSP-GL-587 - List KPN Critical Services</p> <p>KSP-GL-589 - List NL Vital Services</p> <p>KSP-RE-579 - Evaluation and defining NL Vital Services</p> <p>KSP-GL-716 - KWAS Tool</p>
<b>ID</b>	KSP-RE-717
<b>Version</b>	1.0
<b>Internal use</b>	Yes, internal use only
<b>Date</b>	August 16, 2018