Overview of selected KPN Security Policies

Creation date: Tuesday, March 6, 2018 12:49:42 PM

Selected by: Ruud Leurs

Requirement	Capacity
Description	When the (B)IA classification is high or critical, the average demanded processing capacity must be guaranteed. The average demanded processing capacity is the average load measures at the hour with the highest load in one week, measured over multiple years. This average demanded processing capacity should always be available, despite disruptions and peak load moments. This applies to transport layers, procesing capacity, storage, cpu power, cooling etc.
ID	KSP-RE-550
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Capacity (specific overload)**
Description	An overload of a platform may not be the cause of an disruption (not during normal situations, nor during incidents).
ID	KSP-RE-551
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Network monitoring**
Description	Networks must be monitored for capacity, availability and malicious activities. Events must be handled as per the incident management process.
Supplement	Monitoring is essential to be able to see what is happening on a network. Without monitoring, network management departments are “blind” and are not in control of a network. Monitoring a network link for over-usage or being able to detect a virus outbreak on the network.
ID	KSP-RE-530
Version	1.0
Date	December 11, 2017
Rationale	BCM
Rationale	Logging
Rationale	The examination of security, safety and integrity incidents
Rationale	Reporting security incidents

Requirement	**Capacity (specific provisioning)**
Description	The provisioning proces should always deliver adequate capacity to comply to the demand.
ID	KSP-RE-552
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	Continuity impact
Description	The project must determine whether continuity plans have to be written or updated, and these plans must be fully tested before implementation; all conform the Business Continuity policy (KSP-RA-529 and underlying requirements).
ID	KSP-RE-531
Version	1.0
Date	December 11, 2017
Rationale	BCM
Rationale	Determine BCM planning & process
Rationale	Implementing changes
Rationale	Law and regulation

Requirement	**Capacity (specific limitation)**
Description	The limitation of the capacity should be known. This must include limitations posed by licences and the influence of one element to the other.
ID	KSP-RE-553
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Proactively detecting disruptions**
Description	Disruptions must be detected as soon as possible, near realtime. Disruptions or performance degradation in systems, networks and services must be detected in the earliest stage possible.
ID	KSP-RE-532
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Capacity (specific utility)**
Description	Utility processes (e.g. power, airco, building) must also contain adequate capacity. The TI should not exceed the set capacities of utility processes.
ID	KSP-RE-554
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Data: complete and correct**
Description	Data that is necessary for the continuous delivery of the service and data that is necessary for incidentmanagement, must be complete, correct and up-to-date.
ID	KSP-RE-533
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Capacity (specific continuous delivery)**
Description	The capacity to deliver continuously may not be disrupted by the provisioning process and assurance of data.
ID	KSP-RE-555
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Data is available**
Description	All relevant data is available and accessible at the right time, in the correct location for the right people. Relevant data is all the data necessary for continuity and for the management of disasters.
ID	KSP-RE-534
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Adequate IT capacity**
Description	With a impact classification (BIA) of high or critical, the IT infrastructure should have 200% capacity (100% per location). In all situations the set capacity in each location should be 100%. The design of the infrastructur is equal for both locations. Avoid single points of failure in the infrastructure.
ID	KSP-RE-556
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**IT and IT data are available**
Description	The availability of the IT infrastructure and IT Data (production data) is conform the set RTO and RPO. IT infrastructure and IT Data can be recovered within the set RTO. In cases where the set RTO is under 168 hours, the IT Infrastructure needs to be in at least two different locations.
ID	KSP-RE-535
Version	1.0
Date	December 11, 2017
Rationale	BCM

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

Requirement	**Maximum accepted data loss (back up and restore)**
Description	All systems that contain data, have established the Maximum Accepted Data Loss (MAD).
ID	KSP-RE-536
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Mass disruption (specific)**
Description	If an element of the service has a Single Point of Failure, then no more than 100.000 customers are allowed on this element.
ID	KSP-RE-558
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Back-up and restore**
Description	The back-up and restore of all data are conform set RTO and RPO. This concerns all data necessary to recover the operation of the service and/or the business process in order to recover continuous delivery in case of an incident. There need to be sufficient recent back ups of data (according to the set RPO), in order to restore the data within the set RTO and this process of back up and restore needs to be tested annually.
ID	KSP-RE-537
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Cables and trenches seperation in the Core and Backhaul infrastructure**
Description	There are always at least two trench separated cable routes between two network locations. The service should not malfunction by one calamity in the Core and/or Backhaul network in which one or more cables are involved.
ID	KSP-RE-559
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Back-up and restore: saving data off site**
Description	Back-ups are (also) saved off-site. In case of an incident in one location the data can be restored with the back up that is saved in another location.
ID	KSP-RE-538
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Back-up and restore: back-up location**
Description	The condition of the back-up location is equal to the production location to prevent degradation in quality of the data.
ID	KSP-RE-539
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Cables and trenches seperation in the Core and Backhaul infrastructure (specific)**
Description	The core and backhaul connections should be routed through redundant cable routes. The core locations are routed via two physically seperated distributers. The infrastructure for core infrastructure should be build redundant. The number of distributions points should be restricted to a minimum.
ID	KSP-RE-560
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Testing system and application**
Description	The continuity requirements for systems and applications (both for IT as TI) are tested annually. All systems and applications have a set of continuity requirements that is tested before go-life and consequently annually, in order to check whether they have the required capacity and performance level to deliver these continuity requirements.
ID	KSP-RE-540
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Redundant within the set RTO**
Description	Service platforms, network platforms and transportation networks and administration infrastructure should be redundant to the level dat they comply within the shortest set RTO.
ID	KSP-RE-541
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Geographic redundancy**
Description	Technical buildings with the highest security classification and datacenters with platforms of which the RTO is under 168 hours, should take geo-redundancy into account and also the redundancy in utilities (powersupply, airco, internal wiring). The distance betweed two geo-redundant locations is approximate 50 km, because of regional infra (electricity, water) and regional natural effects, such as earthquakes, floodings, storm.
ID	KSP-RE-542
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Redundancy of a building**
Description	Critical services need to be resilient for the failure of a building and should be able to operate within the set BCM norms (e.g. RTO, RPO).
ID	KSP-RE-543
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Redundancy of a building related to the climate**
Description	Mitigating measures must be taken against failure of a building to floodings. When new buildings are used, it must be checked what the water level above ground level is (can be checked at the local communal office) and measure must be according to this water level. This is also because of effects of climate change (e.g. heavy rain).
ID	KSP-RE-544
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Redundancy testing of building amenities**
Description	The redundancy of building amenities should be tested before use and when in use, tested annually. - When a hot standby is used, the technique should be tested annually. - When a cold standby is used, the technique and the business processes should be tested annually.
ID	KSP-RE-545
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Redundancy of cables and trenches**
Description	When redundancy is applied, this should also be in effect for the underlaying layers of the infrastructure (e.g. cabels should be separated in trenches and separated in buildings).
ID	KSP-RE-546
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Management of redundancy**
Description	Management of redundancy: a disturbance in a location (building) may not affect the management of the redundancy.
ID	KSP-RE-547
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Diverting to another location**
Description	The processes for diverting to another loation and the return to normal after a diversion, should be determined in procedures. The diversion to another location must be restored as soon as possible to recover redundancy.
ID	KSP-RE-548
Version	1.0
Date	December 11, 2017
Rationale	BCM

Requirement	**Robustness testing**
Description	Projects should have robustness testing for all operationale techniques (TI) at the implementation phase. A robustness test is focused on testing all continuity measures taken.
ID	KSP-RE-549
Version	1.0
Date	December 11, 2017
Rationale	BCM