Overview of selected KPN Security Policies

Creation date: Wednesday, November 7, 2018 3:41:47 PM

Selected by: Ruud Leurs

Requirement	Capacity
Description	When the (B)IA classification is 'high' or 'critical', the average need of processing capacity must be guaranteed. Regardless faults or peak loads, the multi-year average processing capacity is always available in the busiest hour in a day.
Supplement	Processing capacity relates to transport and service processing capacity as well as to storage, cpu power, cooling, etcetera.
ID	KSP-RE-550
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (BCM)

Requirement	**Capacity (specific overload)**
Description	A platform has sufficient capacity to maintain its functionality, even if there is overload (both in normal situations and in case of calamities).
Supplement	Consider applying assets such as load balancers and load limiters.
ID	KSP-RE-551
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (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	Business Continuity Management (BCM)
Rationale	Logging
Rationale	The examination of security, safety and integrity incidents
Rationale	Reporting security incidents

Requirement	**Capacity (specific provisioning)**
Description	The provisioning process must always have sufficient capacity to comply to the demands of processing and delivery.
Supplement	It involves stockpiling before delivery and after delivery. The delivery process may not be disrupted due to a disruption in delivery and / or processing. Where processing capacity is dependent on delivery, then sufficient capacity must be provided.
ID	KSP-RE-552
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (BCM)

Requirement	Impact on continuity
Description	In the creation, adaptation or elimination of a case (such as a process, product, service, application, semi-finished product, infrastructure, building, etcetera) it must be determined whether continuity plans must be written or adjusted. Before the creation, adaptation or elimination is taken into production or transferred to management, it must be demonstrated by a test of the continuity plan that the related continuity standards are being met.
Supplement	All KPN business activities are directly or indirectly connected to each other. That is why it is important that every change is prepared and tested in such a way that it demonstrably has no adverse effect on the continuity of related matters.
ID	KSP-RE-531
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (BCM)
Rationale	Determine BCM planning & process
Rationale	Implementing changes
Rationale	Law and regulation

Requirement	**Capacity (specific limitation)**
Description	The capacity limit of all elements is known, as well as the influence that the capacity of an element has on the capacity of another element.
Supplement	These are capacity limits such as licenses, working memory, processor capacity, etcetera.
ID	KSP-RE-553
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (BCM)

Requirement	**Proactively detecting disruptions**
Description	A failure or performance degradation in systems, networks and services must be detected as soon as possible to the actual time of disruption.
ID	KSP-RE-532
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (BCM)

Requirement	**Capacity (specific utility)**
Description	Utility processes have sufficient capacity. The technical infrastructure (TI) may not exceed the capacity of the utility processes.
Supplement	Utility processes are power supplies, air conditioning, floor capacity and building space.
ID	KSP-RE-554
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (BCM)

Requirement	**Data: complete and correct**
Description	Data required for the continuous provision of services and the management of calamities are up-to-date, correct and accurate.
ID	KSP-RE-533
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (BCM)

Requirement	**Capacity (specific continuous delivery)**
Description	The capacity of continuous delivery is not disturbed by providing provisioning and assurance data.
Supplement	Continuous delivery is a critical business process.
ID	KSP-RE-555
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (BCM)

Requirement	**Data is available**
Description	Data is available and accessible at the right time, in the right location and for the right people when necessary for answering continuity questions (including incident management).
ID	KSP-RE-534
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (BCM)

Requirement	**Adequate IT capacity**
Description	IT infrastructure with a (B)IA classification 'high', 'critical', or 'medium', of which the RTO is shorter than a week, must always be performed at two different physical locations, each providing 100% of the required capacity (total of 200%). The infrastructure design for both locations is similar.
Related info	In practice, a week (7 days of 24 hours = 168 hours) is required for replacing hardware. Because this recovery time is too long for IT infrastructure with the above-mentioned classifications, a second physical location with the required capacity has to be in place.
ID	KSP-RE-556
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (BCM)

Requirement	**IT infrastructure and IT data are available**
Description	The availability of the IT infrastructure is always in accordance with the stated RTO and RPO. The availability of IT data (production data) is in accordance with RTO and RPO. IT infrastructure and IT data can be restored within the RTO.
ID	KSP-RE-535
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (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	Business Continuity Management (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	Business Continuity Management (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	Business Continuity Management (BCM)

Requirement	**Back-up and restore**
Description	All data necessary to get the service and / or the continuous delivery operational again in the event of an incident, are in accordance with the agreed RTO and RPO.
Supplement	There are sufficient recent copies (back-ups) of data and configurations for timely restoration of the service or the process as a whole within its recovery norm (RTO).
ID	KSP-RE-537
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (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	Business Continuity Management (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	Business Continuity Management (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	Business Continuity Management (BCM)

Requirement	**Cables and trenches seperation in the Core and Backhaul infrastructure (specific)**
Description	The cable network is constructed in such a way that Core and Backhaul connections can be routed via redundant cable routes.
Supplement	Core sites are routed through two physically separate distributors. Infrastructure for core infrastructural connections is build redundantly. The number of manipulation points (distributors) should be restricted to a minimum. Core cables are not used for welding backhaul and access connections.
ID	KSP-RE-560
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (BCM)

Requirement	**Testing system and application**
Description	The continuity requirements of systems and applications (for both IT and TI) must be demonstrably tested at least annually.
Supplement	Systems and applications are demonstrably tested to ensure that they have the required capacity and performance to meet the defined continuity requirements.
ID	KSP-RE-540
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (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	Business Continuity Management (BCM)

Requirement	**Geographic redundancy**
Description	Technical buildings with the highest security rating and data centers with platforms of which the RTO is less than 168 hours (one calendar week), account must be taken of geographical redundancy and redundancy in utilities (power supply, air conditioning and internal cabling).
Supplement	The distance between two georedundant locations is about 50 km in relation to regional infrastructures such as electricity, water and regional effects of, for example, an earthquake and storm.
ID	KSP-RE-542
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (BCM)

Requirement	**Redundancy related to a building**
Description	Critical services, critical service components and critical applications need to be resilient for the failure of a building and should be able to operate within the defined BCM norms (e.g. RTO, RPO).
Supplement	A service, service component or application can be defined as critical based on the BIA / IA outcome. Hardware elements of such service, service component and / or application are located in a building. Failure of that building may not lead to exceeding the defined BCM norms of the critical service, service component or application.
ID	KSP-RE-543
Version	2.0
Date	November 2, 2018
Rationale	Business Continuity Management (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	Business Continuity Management (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 warm/cold standby is used, the technique and the business processes should be tested annually.
ID	KSP-RE-545
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (BCM)

Requirement	**Redundancy of cables and trenches**
Description	Applied redundancy must also be guaranteed in underlying layers of the infrastructure.
Supplement	Cable infrastructure that has been laid out redundant must be laid in separate cable channels and separate cable ducts within a building.
ID	KSP-RE-546
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (BCM)

Requirement	**Redundancy management**
Description	Redundancy management must be set up in such a way that, in case of a site failure, management is still possible and able to carry out mitigation actions.
ID	KSP-RE-547
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (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	Business Continuity Management (BCM)

Requirement	**Robustness tests**
Description	In case of TI equipment implementations, immediately demonstrable robustness tests are performed with regard to all continuity measures.
ID	KSP-RE-549
Version	1.1
Date	November 2, 2018
Rationale	Business Continuity Management (BCM)