Overview of selected KPN Security Policies

Creation date: Thursday, May 9, 2019 9:33:13 AM

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 measures

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 measures

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 measures
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 measures

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 measures

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 measures

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 measures

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 measures

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 measures

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	1.2
Date	May 3, 2019
Rationale	Business Continuity measures

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 measures

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 measures

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 measures

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 measures

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 measures

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 measures

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 measures

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 measures

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

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 measures

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 measures

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 measures

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 measures

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 measures

Requirement	**Network availability**
Description	The design of a network must ensure the required level of availability.
Supplement	Due to the function of a network component (handling traffic), different data streams for different services are transported. The highest availability requirement of the data streams prescribes the measures that must be taken for a network infrastructure. If a service must be “always on”, robust components must be used and device- or location redundancy must be implemented. The service description of the network enables the end user to be aware of possible continuity interruptions and the duration and extent of this. It is up to the end user to take suitable measures.
ID	KSP-RE-562
Version	1.1
Date	August 16, 2018
Rationale	Designing to availability level
Rationale	Business Continuity measures

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	Top Level Policy
Rationale	Business Continuity measures

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	Business Continuity measures

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	Business Continuity measures