Wednesday, June 27, 2018 1:52:36 PM
Ruud Leurs

Requirement	**Defining and documenting authorizations**
Description	Authorizations within a system must be defined and documented.
Supplement	To allow consistent assignment of authorizations in the system and to enable periodic review the correctness. Authorizations can be documented in Function Authorization Matrix (FAM), which can vary from a 1 to 1 matrix (there is only 1 function for all users) to matrix with many functions in different segments to many system resources.
ID	KSP-RE-372
Version	1.0
Date	December 11, 2017
Rationale	Central identity and access management

Requirement	**Registration of Reliable Financial Reporting (RFR) applications**
Description	All new applications which are defined as RFR application by Group Risk & Compliance must on-board in IAM Portal. Furthermore, if as a result from an audit or a compliance test (e.g. a walkthrough) an existing application is defined as a RFR application, it is considered to be a new RFR application and must on-board in IAM Portal. All RFR applications must follow the process steps for attestation, validation (by the owner on functional application matrix and Business Process Rules) and monthly reconciliation.
Supplement	Registration of RFR applications in IAM Portal is essential: • to stay in control of logical access; • to prevent unwanted impact on the KPN Financial Annual Account. Examples are granting more than needed access levels (need to have principle), insufficient Segregation of Duties in the application or not taking into account regulatory compliance (i.e. Chinese Walls). It is preferable to onboard a RFR application in IAM via direct provisioning (link to an Active Directory or LDAP which automatically make authorization mutations). Registration of financial applications like ZEUS, critical applications like BOSS or WASP. Exceptions need to be documented and founded. Approval is needed by Group Risk & Compliance.
ID	KSP-RE-374
Version	1.1
Date	April 4, 2018
Rationale	Central identity and access management

Requirement	**Identity Management Systems**
Description	Identity Management systems (and chains of systems), such as (but not limited to) Active Directory Servers, Kerberos Servers, Identity & Access Management systems must be located within KPN premises and maintained by KPN (EP) employees.
Supplement	KPN must be in ultimate control of who can access information of KPN's customers and KPN. An application owner must be able to grant or deny access to the information systems under his control, without possible intervention by third parties.
ID	KSP-RE-375
Version	1.0
Date	December 11, 2017
Rationale	Central identity and access management

Requirement	**Identities are linked to a natural person**
Description	The personal identities of direct contracted employees must be registered in the applicable central HR system together with a KPN digital identity (Ruisnaam / Europe account). In case of external companies, these must assure the link between the KPN digital identity and personal identity of persons working for KPN.
Supplement	It must be able to link every action performed by a KPN digital identity to a natural person, both for reasons of accountability as well as for verification of potential digital identity theft. As the privacy act prohibits registration of some personal identities responsibility for making the link must be formally delegated to the third party that registered the personal identity. Account in logging reveals the person who created an order. When group accounts are necessary, the reasons must be documented together with the additional measures to ensure traceability of actions to the natural person and approved by an appropriate business representative.
ID	KSP-RE-377
Version	1.1
Date	April 4, 2018
Rationale	Personal and digital identity

Requirement	**Functional accounts**
Description	For functional accounts a responsible natural person must be assigned who is responsible for the use of the account, will act as authoriser and must be aware of this assignment and the implications of it.
Supplement	We must be able to link every action performed by a KPN digital identity to a natural person, both for reasons of accountability as well as for verification of potential digital identity theft. Examples of functional accounts are: - Service accounts (A digital identity used for transferring data between specific IT systems. Persons can not login with these accounts); - Shared functional accounts (e.g. for the use of a monitoring station on a NOC); - System accounts (Accounts that come with a system).
ID	KSP-RE-378
Version	1.1
Date	June 18, 2018
Rationale	Personal and digital identity

Requirement	**Default accounts**
Description	Default accounts must be disabled. If their use is necessary, additional measures should be taken to prevent misuse of these accounts and the accounts must be assigned to a manager responsible for use and authorization.
Supplement	Default accounts are known to hackers and the first attempt is to get in by guessing the password. A default ‘root’ or ‘guest’ user must be disabled or removed if possible. When technically not possible to disable or remove, a password must be used of at least twenty characters and which contains multiple upper case, lower case, base digits and non-alphanumeric characters.
ID	KSP-RE-379
Version	1.0
Date	December 11, 2017
Rationale	Personal and digital identity

Requirement	**Identity registration**
Description	Both the personal and KPN digital identities of direct contracted employees must be registered in the applicable systems, whereas for external companies the KPN digital identities must be registered by KPN and the personal identities must be registered by the external party.
Supplement	To enable the linking of actions to responsible parties identities must be registered. For KPN employees we can perform both personal and digital identity registration whereas for outsourced activities we are prohibited from registering their personal identity information by the privacy act (“Wet bescherming persoonsgegevens’). For KPN employees we register personal identities in the central HR system and the digital identity in the identity and access management portal. For employees working in offshoring contracts we only register the KPN digital identity, personal identity is the responsibility of the external party. Information on registration and management of ‘overig personeel’ can be found in the group Human Resources KPN on TEAMKPN.
ID	KSP-RE-371
Version	1.0
Date	December 11, 2017
Rationale	Central identity and access management

Requirement	**Inventory of authorization decisions**
Description	Each application, system and network element must have an up to date administration registering the current granted accounts and authorizations and who authorised these (manager and additional authorisers) and at what time.
Supplement	For all existing accounts and authorizations must be traceable who authorised whom and at what time. Therefore an account/authorization request must be registered including who authorised whom and when. Excel list with agree of managers and second authorizers.
ID	KSP-RE-373
Version	1.0
Date	December 11, 2017
Rationale	Central identity and access management