Présentation de Méhari- Standard (2017)

Le présent document a pour but de présenter Méhari –Standard (2017), tant aux utilisateurs de Méhari Expert (quelles différences essentielles ?) qu'aux responsables peu connaisseurs de Méhari mais souhaitant appréhender l'analyse et la gestion des risques liés aux systèmes d'information.

1. Rappel des fondamentaux de Méhari

Méhari est une méthode d'analyse de risques fondée sur une identification préalable et générale de situations de risque et sur une méthode d'évaluation de la gravité de chaque situation, en fonction du contexte et de la situation de chaque entreprise ou organisme.

La méthode d'évaluation de la gravité des risques est basée sur un modèle de risque qui a été publié pour la première fois en 1992 et dont la pertinence, confirmée par l'expérience, n'est plus à démontrer.

Les situations de risques, décrites par des scénarios de risque, ainsi que les services de sécurité à même de réduire les risques, sont décrits dans des bases de connaissance propres à chaque version de Méhari. Ces bases contiennent également des questionnaires d'évaluation des services de sécurité ainsi que l'ensemble des éléments et algorithmes permettant d'évaluer les risques.

Les particularités de Méhari Standard sont développées ci-dessous.

2. Services de sécurité de Méhari Standard et norme ISO 27002

Les services de sécurité de la base de connaissance de Méhari Standard ont été redéfinis avec les objectifs suivants :

- s'aligner au maximum sur la norme ISO 27002:2013
- rester fidèle à l'esprit de rigueur de l'analyse de risque Méhari
- conserver le domaine couvert par l'analyse
- limiter le nombre de questions dans le diagnostic des services de sécurité et éviter les redondances inutiles

Alignement des services de sécurité sur les contrôles de l'ISO 27002 :2013

Afin de respecter les objectifs ci-dessus, les dispositions suivantes ont été prises :

- Là où des services de sécurité différents (dans les bases précédentes) correspondaient à un seul contrôle ISO, ils ont été regroupés afin d'obtenir une correspondance « un contrôle ISO => un service Méhari »
- Là où des contrôles ISO ne correspondaient à aucun service Méhari, un nouveau service a été créé
- Les services de sécurité ne correspondant à aucun contrôle ISO mais nécessaires à la réduction de certains risques ou relatifs à des domaines non couverts par l'ISO ont été maintenus (par exemple, protection de l'information écrite, des archives, etc.)

Alignement des questionnaires d'audit sur les considérations de l'ISO

Afin de respecter les objectifs ci-dessus mentionnés, les dispositions suivantes ont été prises :

- Les considérations, parfois nombreuses, de l'ISO (« should » dans la norme) ont été prises en compte en tant que questions (avec des regroupements quand cela était possible)
- Les questions liées à la rigueur de l'analyse de risque, en particulier celles relatives à la robustesse[1] et à la mise sous contrôle[2] des services de sécurité, ont été maintenues pour les services utilisés pour la réduction des risques
- Compte tenu des deux points ci-dessus, les questionnaires ont été réduits, autant que faire se peut

Conséquences sur les types d'actifs retenus dans la base 2016

Le regroupement de services de sécurité a conduit à revoir également les types d'actifs qui ont été réduits, par rapport à la base 2010 (Méhari-Expert).

Néanmoins, des actifs nouveaux ont été créés pour tenir compte des services externalisés (« cloud »).

Actifs et services de sécurité de Méhari Standard

Les types d'actifs ont été ramenés à 13 (26 dans la base Expert)

Le nombre de service de sécurité a été ramené à 142 (300 dans la base Expert), répartis dans 8 domaines de diagnostic (14 dans la base Expert)

Le nombre total de questions a été ramené à 908, malgré les nouvelles questions due à l'alignement sur l'ISO (environ 2150 dans la base Expert)

3. Situations de risque décrites par les scénarios de Méhari Standard

Dans les bases de connaissance existantes de Méhari, tant Expert que Pro, les scénarios de risque sont présentés par domaine, chaque domaine représentant un actif primaire et un type de dommage (par exemple « Perte de disponibilité de données applicatives »).

On constate alors qu'un même type de scénario, tel que « l'effacement accidentel d'un support de données, dû à un incident d'exploitation », est reproduit plusieurs fois, souvent à l'identique, pour des données applicatives, pour des données bureautiques partagées ou non, pour des données publiées sur des sites web, pour des programmes applicatifs, etc.

Il a été retenu de regrouper tous ces scénarios, à chaque fois que les services appelés étaient bien les mêmes (ce n'est pas toujours le cas car certains services sont spécifiques d'un type d'actif), c'est-à-dire à chaque fois que les actions de réduction des risques étaient bien les mêmes (étant entendu qu'au moment de la mise en œuvre de ces mesures, il reste possible de ne les appliquer qu'à un ou plusieurs types d'actifs, en fonction de leur sensibilité).

Cela conduit, bien entendu, pour évaluer la gravité d'un scénario regroupé, à faire référence au maximum des impacts intrinsèques de tous les actifs concernés par le regroupement.

---

1 La robustesse s'un service de sécurité mesure sa capacité à résister à une action visant à le court-circuiter ou à l'inhiber.

2 La mise sous contrôle d'un service vise à s'assurer (par des mesures adéquates) que les paramètres ou conditions initiales supportant l'efficacité du service, sont bien maintenus dans le temps.

Ce regroupement et la réduction du nombre d'actifs a permis de réduire notablement le nombre de scénarios à analyser, tout en gardant une analyse exhaustive.

La base Standard comprend ainsi 210 scénarios répartis dans 20 familles (près de 800 dans la base Expert).

4. Plans d'action et projets

Méhari Standard comprend, comme Méhari Expert, des possibilités de décision relatives à des plans d'action à mener pour réduire les risques à un niveau acceptable.

Ces plans sont maintenant décrits dans des « projets », chaque projet ayant une finalité particulière et pouvant faire l'objet d'une planification propre.

Il y a ainsi, dans la base Expert, 47 projets, chacun d'entre eux étant décrit par les services de sécurité à mettre en place ou à améliorer et, pour chaque service de sécurité, par un objectif de qualité de service à atteindre.

La base permet de préciser la date de début et la date d'achèvement de chaque projet, permettant ainsi de faire une projection de l'état des risques à une date donnée.

5. Outils de pilotage et de suivi

Méhari Standard comprend de nouveaux outils de pilotage des risques :

- Des aides à la sélection de projets, par un automatisme permettant de mettre en évidence les projets susceptibles de réduire le maximum de risques de niveaux élevés (insupportables ou inadmissibles).
- Une présentation synthétique du nombre de risques de niveaux 3 et 4 (insupportables et inadmissibles) par année en fonction des dates d'achèvements des projets décidés et planifiés
- Un tableau de bord général des risques divers panoramas de risques

Annexe : Tableau comparatif des versions

	Méhari-Pro	Méhari-Standard	Méhari-Expert
Nombre de types d'actifs	10	13	26
Nombre de services de sécurité	43	142	300
Nombre de domaines de services	6	8	14
Nombre de questions de diagnostic	380	900	2150
Nombre de scénarios de risque	74	210	800