MEHARI

Guide de l'analyse des enjeux et de la classification

Avril 2022

CLUSIF

Sommaire

1 Introduction

L'analyse des enjeux est une étape essentielle de tout processus de gestion des risques.

L'objectif de ce document est de compléter le guide de mise en œuvre et le guide de la gestion des risques en procurant des aides au déroulement du processus et en justifiant, si nécessaire, les tâches à mener à bien.

L'analyse des enjeux se concrétise par deux résultats principaux :

L'échelle de valeurs des dysfonctionnements.

La classification des actifs du système d'information, et, en particulier, le tableau d'impact intrinsèque utilisé par les bases de connaissances de MEHARI pour l'évaluation des scénarios de risque.

Les processus d'obtention de ces résultats sont décrits ci-après.

La démarche MEHARI consiste à procéder à une analyse des activités et donc des processus de l'entreprise ou de l'organisme, d'en déduire les dysfonctionnements qui peuvent être redoutés, puis d'évaluer en quoi ces dysfonctionnements peuvent être plus ou moins graves, avant d'effectuer, éventuellement, la classification proprement dite des actifs du système d'information, selon le schéma ci-dessous.

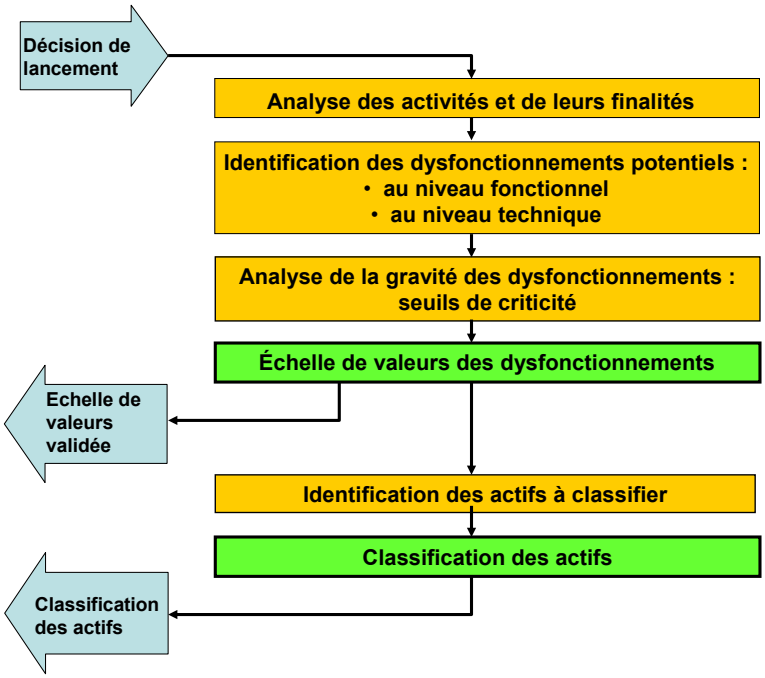

Figure 1 : Échelle de valeurs et classification

2 L'échelle de valeurs des dysfonctionnements

L'objectif de ce processus est de déterminer une échelle de valeurs des dysfonctionnements significatifs des activités de l'entité[1].

Cette analyse se déroulera en quatre étapes :

- L'identification des activités majeures et de leurs finalités,
- L'identification des dysfonctionnements redoutés de chaque activité, ceci pouvant se faire :
  - ✓ Au niveau de l'activité,
  - ✓ Au niveau fonctionnel.
- L'évaluation du niveau de gravité de ces dysfonctionnements, activité par activité,
- La détermination et la validation d'une échelle de valeurs globale, au niveau de l'entité.

2.1. Identification des activités majeures et de leurs finalités

Un bon point de départ est d'identifier les activités majeures du domaine analysé, de les décrire en quelques mots et de noter en regard les résultats attendus ou les objectifs.

2.2. Résultats attendus

Les activités seront décrites en termes de fonctionnalités.

En complément de la description fonctionnelle, il est utile de décrire les objectifs ou finalités, c'est-à-dire les résultats attendus au niveau de l'activité. Ces résultats attendus sont à décrire du point de vue de l'entité et du point de vue des entités « clientes ».

Un exemple est donné ci-dessous :

Fonctionnalité	***Résultats attendus ou objectifs***
Établir et tenir à jour une synthèse des besoins de trésorerie	Permettre aux gestionnaires de la trésorerie d'approvisionner les comptes à temps (et d'éviter les ruptures de paiements)

2.3. Démarche

Cette identification des activités peut se faire de manière rigoureuse et exhaustive par une analyse de processus, en recherchant tous les processus du domaine étudié, voire en les décomposant en autant de sous-processus que nécessaire pour mettre en évidence les diverses dépendances et tous les résultats intermédiaires.

L'expérience prouve qu'une démarche globale et plus intuitive, si elle est menée au bon niveau de responsabilité, c'est-à-dire avec les responsables des grandes fonctions de l'entreprise ou

1 L'entité peut être une entreprise ou représenter une unité organisationnelle, pour laquelle on cherche à établir des objectifs de sécurité, ou un projet particulier, pour lequel on cherche à identifier les risques spécifiques.

de l'organisme, permet de dégager très rapidement les fonctions majeures et leurs finalités, ce qui est amplement suffisant pour le but recherché.

La démarche repose donc sur des entretiens individuels avec les responsables des diverses activités de l'entreprise ou de l'organisme. De tels entretiens durent généralement entre une heure et une heure trente.

2.4. Identification des dysfonctionnements redoutés

Il faut rechercher ensuite les dysfonctionnements redoutés pour ces activités.

2.5. Résultats attendus

La description des dysfonctionnements doit être telle qu'il soit possible ensuite d'en évaluer la gravité. Il est à noter, cependant, qu'un dysfonctionnement peut être décrit à plusieurs niveaux :

- Au niveau de l'élément perturbateur ou perturbé dans le processus concerné (par exemple l'indisponibilité de l'application de gestion de trésorerie ou de la base de données associée), donc à un niveau technique.
- Au niveau du processus, c'est-à-dire à un niveau fonctionnel, par exemple l'incapacité à établir une synthèse des besoins de trésorerie.

Ainsi le même dysfonctionnement peut être décrit soit comme l'indisponibilité des données nécessaires à l'obtention d'un certain résultat, soit comme l'incapacité à fournir ce résultat. Le premier aspect correspond à ce que nous appelons ***l'analyse des enjeux au niveau technique,*** le deuxième à ***l'analyse des enjeux au niveau fonctionnel***.

2.5.1.1 Dysfonctionnements redoutés au niveau fonctionnel

Au niveau fonctionnel, l'objectif est d'identifier les dysfonctionnements potentiels significatifs dans les activités de l'entreprise. Il s'agit donc de dysfonctionnements de processus et l'on peut s'appuyer sur la typologie générique suivante des dysfonctionnements de processus :

- **Défaut de ponctualité** : les tâches prévues ou les activités ne sont pas effectuées dans les délais prévus
- **Défaut de conformité** : les tâches prévues ou les activités ne sont pas effectuées conformément à ce qui est spécifié
- **Défaut d'exhaustivité** : les tâches prévues ou les activités ne sont effectuées que partiellement (mais ce qui est effectué est conforme à ce qui est spécifié)
- **Défaut de justesse** : des tâches ou des activités non prévues ni spécifiées sont effectuées en supplément
- **Défaut de discrétion** : des informations sont divulguées à l'occasion de l'accomplissement des tâches ou activités
- **Défaut de contrôle** : les tâches prévues ou les activités se déroulent conformément à ce qui est spécifié mais sans contrôle ou sans visibilité

Il est donc possible de décrire un dysfonctionnement par l'activité ou la tâche concernée et par un type de dysfonctionnement.

Il est souvent utile de décrire en outre les conséquences redoutées, afin de mieux pouvoir juger de leur gravité.

Ainsi, par exemple, dans l'hypothèse de la divulgation des salaires du personnel, il peut être utile de préciser les conséquences redoutées : déclenchement d'une grève, obligation de procéder à des augmentations nombreuses pour des catégories de personnel, perte de motivation du personnel, etc.

De même, si le dysfonctionnement envisagé est l'altération de la paye, il est nécessaire de

préciser si les conséquences redoutées sont une fraude et la perte d'argent ou la grève du personnel ou sa démotivation ou l'obligation de gérer des rappels nombreux et compliqués.

Chaque dysfonctionnement sera décrit, au niveau fonctionnel, comme une altération de processus, donc par le processus ou l'activité concerné et par le type de dysfonctionnement et par le type de conséquences redouté.

Par exemple, pour la gestion de trésorerie, déjà évoquée :

Dysfonctionnement	***Conséquences***
Retard dans l'approvisionnement des comptes de trésorerie	Incapacité à payer les fournisseurs se traduisant par un arrêt des livraisons et un arrêt de la production

2.5.1.2 Dysfonctionnements redoutés au niveau technique

Au niveau technique, l'objectif est d'identifier les dysfonctionnements significatifs dans la mise en œuvre des moyens requis pour les activités de l'entreprise ou de l'organisme.

Les moyens mis en œuvre peuvent être :

- Les moyens matériels :
  - ✓ Les moyens courants (locaux, équipements de bureaux, téléphones et télécopieurs, équipements spécifiques, etc.),
  - ✓ Les moyens informatiques (serveurs, stations de travail, réseaux de données, etc.),
  - ✓ Les moyens documentaires généraux ou spécifiques de l'activité,
  - ✓ Les moyens de liaison et de communication (courrier, réseau téléphonique, etc.).
- Les moyens immatériels :
  - ✓ Les données (fichiers, bases de données, éléments de référence nécessaires à l'activité),
  - ✓ Les programmes (logiciels de base, applicatifs, etc.),
- Les moyens en personnel :
  - ✓ Le personnel indispensable (compétence, pouvoir de décision, etc.).

Les types de dysfonctionnements sont, classiquement **la perte de disponibilité, d'intégrité ou de confidentialité**.

De la même manière que pour les dysfonctionnements identifiés au niveau fonctionnel et pour les mêmes raisons, il est souvent utile de décrire en outre les conséquences que l'on redoute, afin de mieux pouvoir juger de leur gravité.

Les dysfonctionnements techniques identifiés seront décrits par les dégradations subies au niveau des moyens employés par les processus et par les conséquences de ces dégradations.

Par exemple, pour la gestion de trésorerie, déjà évoquée :

Dysfonctionnement	***Conséquences***
Indisponibilité de la base de données de la trésorerie Indisponibilité de l'application de gestion de trésorerie	Retard dans l'approvisionnement des comptes se traduisant par une incapacité à payer les fournisseurs se traduisant elle-même par un arrêt des livraisons et un arrêt de la production

Remarque :

L'exemple choisi met en évidence une redondance des résultats et effectivement un même dysfonctionnement peut être exprimé aussi bien au niveau technique ou au niveau fonctionnel. Cependant, les descriptions faites au niveau technique peuvent avoir plusieurs conséquences

et elles seront moins pérennes car dépendantes des technologies employées. Il est donc préférable de privilégier les descriptions au niveau fonctionnel.

2.6. Démarche

Ici encore, il est possible d'envisager une démarche très systématique, en se basant sur une analyse de processus et en envisageant toutes les « déviations » possibles des processus et sous-processus : non-conformité des résultats, retard ou absence de résultat, indiscrétions, etc.

L'expérience prouve également qu'au bon niveau de responsabilité, les dysfonctionnements majeurs sont très rapidement mis en évidence par une approche plus globale revenant à demander aux principaux responsables ce qu'ils redoutent le plus ou ce qui représente pour eux un souci majeur.

Au niveau fonctionnel, ils connaissent très bien leurs processus critiques et au niveau technique, s'ils ne savent pas forcément faire une liste détaillée et exhaustive des applications ou bases de données mises en œuvre, ils savent très bien les désigner globalement sous une dénomination générique amplement suffisante (« la paye » pour l'ensemble des programmes concernés, par exemple).

La description des dysfonctionnements, tant au niveau fonctionnel qu'au niveau technique, sera donc obtenue au cours des entretiens individuels, précédemment évoqués, avec les responsables des diverses activités de l'entreprise ou de l'organisme.

2.7. Analyse des enjeux : évaluation de la gravité des dysfonctionnements identifiés

La troisième étape, dans la détermination de l'échelle de valeurs, vise à **déterminer la gravité des dysfonctionnements précédemment identifiés**. Il faut faire référence, pour cela, à une échelle de gravité standard.

2.8. Échelle de gravité

MEHARI distingue 4 niveaux de gravité ou de criticité, notés de 1 à 4, dont les définitions générales sont développées ci-après :

Niveau 4 : Vital

A ce niveau le dysfonctionnement redouté est extrêmement grave et met en danger l'existence même ou la survie de l'entité ou de l'une de ses activités majeures.

Si un tel dysfonctionnement survient, l'ensemble du personnel est concerné et peut se sentir menacé dans son emploi.

Pour des organismes dont la fonction ne saurait être remise en cause, en particulier les services publics, ce niveau de gravité peut remettre en question l'existence du service et le redéploiement de la fonction dans d'autres services ou ministères. Un tel niveau peut également être défini en liaison avec la gêne occasionnée dans le public : nombre de personnes touchées et durée de la perturbation.

Pour les sociétés commerciales et en termes financiers, il est souvent judicieux de considérer, à ce niveau, une perte conduisant à un déficit tel que les actionnaires pourraient se désengager (avec chute du titre pour les sociétés cotées).

C'est l'équivalent, dans le domaine de la santé des personnes, d'un accident ou d'une maladie « extrêmement grave », assorti d'un « diagnostic réservé » de la part des médecins.

En cas de survie, les séquelles sont importantes et durables.

Niveau 3 : Très Grave

Il s'agit là des dysfonctionnements très graves au niveau de l'entité, sans que son avenir

soit compromis.

A ce niveau de gravité, l'ensemble ou une grande partie du personnel est concerné, dans ses relations sociales et dans ses conditions de travail, mais sans risque direct pour son emploi.

En termes financiers, cela peut amputer significativement le résultat de l'exercice, sans que les actionnaires se dégagent massivement.

En termes d'image, on considérera souvent à ce niveau une perte d'image dommageable qu'il faudra plusieurs mois à remonter, même si l'impact financier ne peut être évalué avec précision.

Des sinistres conduisant à une désorganisation notable de l'entreprise pendant une durée de plusieurs mois seront aussi souvent évalués à ce niveau.

Niveau 2 : Important

Il s'agit là de dysfonctionnements ayant un impact notable au niveau des opérations de l'entité, de ses résultats ou de son image, mais restant globalement supportables.

Seule une partie limitée du personnel serait très impliquée dans le traitement des conséquences du dysfonctionnement avec un impact significatif sur les conditions de travail.

Niveau 1 : Non significatif

A ce niveau les dommages encourus n'ont pratiquement pas d'impact sur les résultats de l'entité ni sur son image, même si certaines personnes sont fortement impliquées dans le rétablissement de la situation d'origine.

2.9. Critères de dysfonctionnement et seuils de criticité : résultats élémentaires

Les dysfonctionnements identifiés n'ont pas forcément une gravité unique. Au contraire, dans de nombreux cas, les dysfonctionnements doivent être caractérisés par un ou plusieurs paramètres déterminants pour leur gravité.

Par exemple, le retard dans l'aboutissement d'un processus est un dysfonctionnement dont la gravité dépend, très généralement, de la durée de ce retard, d'une part, et du nombre de personnes concernées par le retard, d'autre part.

Il faut donc déterminer, pour chaque dysfonctionnement, quels sont les paramètres significatifs et quels sont les seuils de ces paramètres qui font passer le dysfonctionnement d'un niveau de gravité à un autre.

Les critères de criticité et les seuils correspondants permettront d'évaluer la gravité de chaque dysfonctionnement, depuis le dysfonctionnement ayant un impact insignifiant jusqu'au dysfonctionnement pouvant être vital pour l'entité concernée.

A titre d'exemple, en reprenant le cas de la gestion de trésorerie, le tableau suivant pourrait être obtenu, pour le dysfonctionnement déjà cité :

Dysfonctionnement	***Niveau 1 Non significatif***	***Niveau 2 Important***	***Niveau 3 Grave***	***Niveau 4 Vital***
Incapacité à approvisionner les comptes bancaires par indisponibilité des bases de données de la trésorerie	Incapacité durant moins de 4 heures	Incapacité comprise entre 4 heures et 2 jours	Incapacité durant plus de 2 jours	

2.10. Démarche

La recherche de ces critères de dysfonctionnement et des seuils de criticité sera faite lors des

entretiens avec les responsables des activités de l'entreprise, toujours au cours du même entretien, dont la durée globale estimée, entre une heure et une heure et demie, comprend la description de l'activité, la recherche des dysfonctionnements redoutés et l'expression de leur criticité en fonction des paramètres significatifs.

Les résultats élémentaires de chaque entretien consisteront ainsi en une description des activités, en une description des dysfonctionnements redoutés et en une évaluation de la gravité de ces dysfonctionnements.

2.11. Échelle de valeurs des dysfonctionnements

Une synthèse des divers résultats sera alors établie au niveau de chaque activité.

Un exemple partiel en est donné ci-dessous, pour une responsable de l'activité de gestion des Ressources Humaines.

Dysfonctionnement	***Niveau 1 Non significatif***	***Niveau 2 Important***	***Niveau 3 Très Grave***	***Niveau 4 Vital***
Falsification des données de paye conduisant à une fraude	Perte < 0.1 M€	Perte comprise entre 0.1 M€ et 1 M€	Perte comprise entre 1 et 10 M€	Perte > 10 M€
Divulgation d'informations sur des données personnelles	Divulgation du salaire d'un employé	Divulgation des salaires de l'ensemble du personnel	Divulgation répétée des salaires du personnel	
Retard dans le paiement des salaires	Retard < 2 jours	Retard compris entre 2 et 15 jours	Retard > 15 jours	
Destruction des données de base concernant le règlement de la paye (calcul et paramétrage)	Effacement des données récentes (moins d'un mois)	Effacement des données de l'année	Destruction des données et de tout l'historique	

Ayant traité ainsi chaque activité, les synthèses établies ensuite constitueront des échelles de valeurs des dysfonctionnements, au niveau de chaque activité, puis au niveau global de l'entreprise ou de l'organisme.

L'échelle de valeurs recherchée n'est ainsi rien d'autre que le rassemblement dans un document unique de l'ensemble des types de dysfonctionnement et des seuils de criticité. Il pourrait donc s'agir d'une étape purement formelle. L'expérience prouve, cependant, que la mise en commun de tous les types de dysfonctionnement et des seuils de criticité de chacun d'eux peut faire apparaître des discordances qui n'ont pas été mises en évidence dans une analyse activité par activité.

Une étape de consolidation est donc nécessaire.

Par ailleurs, toutes les conclusions et décisions d'action qui pourront être déduites de cette échelle de valeurs ou qui s'appuieront sur elle ne seront véritablement suivies d'effet que si cette échelle de valeurs reflète un consensus des dirigeants de l'entité.

Il est donc fortement recommandé, si ce n'est impératif, qu'il y ait un véritable débat et qu'un consensus soit obtenu sur l'échelle de valeurs des dysfonctionnements de l'entité, en présence de l'ensemble du comité de Direction.

Le résultat final sera une échelle de valeurs des dysfonctionnements validée.

Un exemple complet est donné en annexe 1.

3 La classification des actifs du système d'information

L'échelle de valeurs des dysfonctionnements est le résultat principal de l'analyse des enjeux de la sécurité, car directement liée aux activités et processus fondamentaux de l'entreprise ou de l'organisme.

Ceci étant, les mécanismes employés dans l'appréciation et la gestion des risques, de même que certaines démarches plus systématiques dans le choix des solutions ou d'élaboration de plans d'action, nécessitent que ces dysfonctionnements, exprimés initialement en termes liés à l'activité, soient traduits en termes techniques relatifs à des ressources de toute nature du Système d'Information, généralement regroupées sous l'appellation d'« actifs ».
Il s'agit, par exemple, de la perte de confidentialité de telle base de données applicative, ou de l'indisponibilité de tel serveur, etc.

Cette traduction consiste à formaliser l'échelle de valeurs sous forme de « classification ».

Cette formalisation complémentaire consiste à :

- Définir une typologie d'actifs devant être classifiées.
- Qualifier chacun de ces actifs en fonction à la fois :
  - ✓ de la manière dont il peut conduire ou être sujet à un dysfonctionnement préalablement identifié,
  - ✓ de la gravité qui en résulte.

Le but de la classification des actifs ainsi est de définir des "étiquettes" que l'on peut attacher à chaque type d'actif, afin de faire savoir à tous ceux qui sont amenés à travailler avec ces actifs, en quoi et dans quelle mesure ils ont de l'importance pour la sécurité.

3.1. Typologie des actifs à classifier

Il serait envisageable de classifier individuellement tous les actifs, c'est-à-dire toutes les informations et tous les moyens supports de traitement, de stockage ou de transport de l'information.

En pratique, il est plus efficace d'effectuer des « regroupements » d'objets, d'informations ou de ressources ayant des finalités voisines et qui demandent le même type et le même niveau de protection. Ainsi, un logiciel et des utilitaires qui lui sont associés, l'ensemble des tables d'une base de données, etc., seront fréquemment réunis dans un même groupe d'objets.

Tous les objets identifiables d'une entité ne peuvent être classifiés individuellement, il faut les regrouper. Les actifs à classifier seront ces groupes d'objets regroupés en typologie.

Ainsi que cela a été présenté dans le document « *MEHARI – Principes fondamentaux et spécifications fonctionnelles* », les actifs doivent se référer aux **besoins** des organisations que l'on peut classer dans trois catégories :

- Les services (informatiques, de télécommunication et généraux),
- Les données nécessaires au fonctionnement des services,
- Les processus transverses de gestion de la sécurité ou de la conformité à des référentiels.

Ces catégories constituent ce que nous appelons des actifs primaires.

La typologie d'actifs primaires retenue par MEHARI dépend des bases de connaissances. En effet, plus cette typologie est détaillée, plus il y aura de scénarios de risque à analyser et plus il

sera nécessaire de détailler les services de sécurité. Les variantes de bases de connaissances correspondent à différents niveaux de détail de l'ensemble des composantes de la base.

Les actifs primaires correspondent aux besoins des organisations et c'est donc à ce niveau qu'il conviendra d'évaluer l'importance de ce besoin, importance dont il sera tenu compte pour juger du niveau de risque. Ce sont donc eux qu'il convient de classifier.

3.2. Critères de classification

Les données informatiques peuvent être à l'origine d'un dysfonctionnement pour trois raisons principales : la perte de disponibilité, d'intégrité ou de confidentialité.

Pour les services, il s'agit essentiellement de la perte de disponibilité ou d'intégrité, mais il peut aussi s'agir de confidentialité pour certaines applications représentant un avantage concurrentiel pour l'entité.

Pour les processus de gestion de la conformité à des lois, réglementations ou exigences contractuelles ou pour les processus de gestion de la sécurité, le critère de classification est l' « Efficience » (notée E dans le tableau d'impact intrinsèque).

3.3. Processus de classification

Parce qu'un même type de dysfonctionnement n'a pas forcément la même gravité pour différents métiers ou différentes activités, il est nécessaire d'effectuer un premier travail de classification par domaine d'activité.

3.4. Classification des actifs liés à des domaines d'activité

Pour chaque type d'actif et chaque processus métier ou domaine d'activité, une analyse sera faite pour déterminer si une perte de confidentialité de ce type d'actif est susceptible de conduire à un ou plusieurs des dysfonctionnements redoutés et si oui, à quel niveau. Si plusieurs dysfonctionnements peuvent être occasionnés par une perte de confidentialité de la ressource, le plus grave niveau atteint (noté de 1 à 4) est le niveau de classification recherché pour le critère de confidentialité.

Il sera fait de même pour les autres critères, de disponibilité et d'intégrité, pour aboutir, in fine et pour chaque type d'actif, à 1, 2 ou 3 valeurs de classification, une par critère pertinent (Disponibilité, Intégrité, Confidentialité).

Pour les processus de management, il s'agit d'évaluer le niveau de conséquence de dysfonctionnement dont l'aboutissement est une non-conformité aux lois, réglementations ou exigences contractuelles ou aux règles de gouvernance dans tel ou tel domaine. Le critère correspondant est appelé l' « efficience » des processus de gestion.

L'objectif de la classification est ainsi de définir, pour les types d'actifs identifiés, les "étiquettes" permettant de connaître les niveaux de conséquences qu'aurait une perte de disponibilité, d'intégrité ou de confidentialité de chaque type et pour chaque domaine d'activité.

Les bases de connaissances proposent, en support de cette classification, des tableaux à remplir.

3.5. Classification des actifs en fonction d'une vue globale

Par ailleurs, à un niveau plus global, il importe de se questionner sur l'impact d'une altération de ces actifs, indépendamment des impacts spécifiques à un domaine d'activité.

Cela sera le cas quand, par exemple, ils peuvent avoir une influence sur une stratégie de développement ou d'urbanisme informatique ou quand ils peuvent avoir un impact sur l'image de professionnalisme de l'entreprise et de ses services supports, en interne ou vis-à-vis de l'extérieur.

3.6. Elaboration du tableau d'impact intrinsèque

Le tableau d'impact intrinsèque représente la classification d'ensemble, tous domaines d'activité confondus, des actifs de l'entité.

Lors d'une appréciation des risques MEHARI, il est fait appel à la notion d'impact intrinsèque d'un scénario qui est l'évaluation des conséquences de l'occurrence du risque, indépendamment de toute mesure de sécurité.

Plus précisément, les bases de connaissances de MEHARI font référence à un tableau d'impact intrinsèque qui peut être rempli soit directement à partir de l'échelle de valeur des dysfonctionnements (MEHARI -ManagerBC) soit à partir des tableaux de classification évoqués précédemment (MEHARI -Expert et MEHARI -Standard).

4 Conseils pratiques

4.1. Points importants dans l'élaboration de l'échelle de valeurs

4.2. Focalisation sur les aspects les plus critiques

Le plus important est de bien se focaliser sur les dysfonctionnements essentiels et de ne pas essayer de recenser tous les dysfonctionnements possibles.

L'objectif premier de la sécurité, quelle que soit la démarche, est d'éviter l'occurrence de situations très graves, voire vitales. Ce sont donc celles-là qu'il faut absolument repérer.

C'est la raison pour laquelle il est souhaité que les responsables de l'activité s'impliquent directement dans la démarche et qu'ils ne délèguent pas leurs adjoints lors de l'analyse des enjeux.

En pratique, pour une activité, il faudrait se limiter à quelques dysfonctionnements critiques, généralement entre 3 et 8.

4.3. Non prise en compte des mesures de sécurité

Le deuxième point, tout aussi fondamental, est de ne pas occulter des dysfonctionnements qui paraîtraient "impossibles". Il est extrêmement courant de voir des dirigeants occulter l'éventualité d'une disparition de données vitales, au prétexte que ces données sont informatisées et "donc" sauvegardées par l'informatique. ***Les dysfonctionnements et leur gravité doivent être identifiés et évalués sans tenir compte de mesures de sécurité, même si ces mesures sont déjà en place***. Sinon, cela amènerait à conclure qu'il n'y a pas d'enjeu important et donc que les mesures de sécurité ne sont pas indispensables et qu'elles peuvent être supprimées.

De même, le caractère plus ou moins probable de l'événement conduisant au dysfonctionnement ne doit pas être pris en considération à cette étape de la démarche.

4.4. Cohérence des dysfonctionnements de natures différentes

Un autre point important dans la détermination des critères et des seuils de criticité est de maintenir la cohérence entre différents types de dysfonctionnements de niveau de gravité équivalent.

A cette fin, il est recommandé de rechercher des axes majeurs stratégiques auxquels il sera possible de se référer pour rendre cohérents les niveaux de gravité des divers dysfonctionnements, ainsi qu'il apparaît dans l'annexe 1.

Il peut s'agir de l'axe financier, auquel cas des équivalences financières seront recherchées pour tous les types de dysfonctionnement, ou d'un axe "service rendu au public", auquel cas ce sont des équivalences en ampleur individuelle d'impact et nombre de personnes touchées qui seront recherchées, etc.

4.5. Aspect décisionnel ou stratégique de l'échelle de valeurs

Il arrive que la gravité de certains dysfonctionnements ne puisse pas être évaluée, soit parce que les conséquences indirectes du dysfonctionnement sont difficiles à appréhender, soit parce qu'il n'est pas possible de juger sérieusement de l'efficacité des actions qui pourraient être menées dans de telles situations.

Dans certaines situations, la gravité d'un dysfonctionnement peut être le résultat d'une simple décision. Il ne s'agit plus alors d'une évaluation, mais d'une option stratégique qui consiste à décider que, dans l'entreprise ou l'organisme, tel dysfonctionnement doit être considéré comme Très grave, voire Vital.

4.6. Points importants lors de la classification

Le premier point important est de bien faire les regroupements d'actifs de finalités voisines pour ne pas avoir à analyser une quantité astronomique d'objets.

Un regroupement par grands domaines applicatifs est généralement la bonne maille d'analyse.

Le deuxième point important est de prévoir, comme pour l'échelle de valeurs, une étape de consolidation et de validation au niveau de l'entité.

4.7. Périmètre de validité de la classification

Il est clair que tout le processus décrit, que ce soit l'élaboration de l'échelle de valeurs ou la classification proprement dite, se situe au niveau d'une entité ayant son autonomie de décision et ses objectifs propres. Il peut s'agir d'une filiale d'un Groupe, d'une « unité d'affaire » (ou business unit), d'une Direction opérationnelle ayant un domaine de responsabilité bien défini ou d'une Direction fonctionnelle.

L'échelle de valeurs des dysfonctionnements et la classification des actifs établies au sein d'une entité sont, bien entendu, valides au sein de cette entité. Mais qu'en est-il à l'extérieur de cette entité ?

Par définition, la classification établie au sein d'une entité étant un moyen de communiquer le niveau de sensibilité d'un actif appartenant à cette entité, cette classification est valide pour l'ensemble de l'entreprise.

Il s'agit, en fait, d'une règle du jeu de la communication d'éléments, en particulier d'informations, entre entités. Si une entité A, une petite filiale par exemple, estime vitale, pour elle, la confidentialité d'une information et la classifie en conséquence, il ne saurait être question que l'entité B, le siège par exemple, reconsidère cette classification et décide de traiter cette information comme non sensible. Si cela était admis, la seule solution pour l'entité A serait de ne pas transmettre cette information.

Cette notion de périmètre de validité de la classification est particulièrement importante dans le cas de gestion de la sécurité basée sur un ensemble de règles appelé Référentiel de sécurité. Dans ce cas, en effet, les précautions qui seront prises ou les mesures de sécurité qui seront appliquées, en fonction de cette classification, sont connues. Il serait absurde de classifier localement une information et d'appliquer, dans l'entité émettrice, des règles de sécurité en conséquence et que la même information se voie appliquer des règles différentes par une autre entité qui considèrerait de son propre chef qu'elle ne mérite pas une telle classification.

4.8. Plans d'actions

Il n'est pas question ici de traiter de démarches consistant à bâtir des plans de sécurité directement à partir d'une analyse des enjeux.

Il faut néanmoins tenir compte du fait que les entretiens individuels ayant conduit à l'élaboration

de l'échelle de valeurs des dysfonctionnements, complétés par un comité de Direction au cours duquel les dysfonctionnements les plus graves auront été évoqués, auront fait naître une attente forte de solutions et qu'il est donc très souhaitable que cette démarche soit suivie, rapidement, d'actions de sécurisation. Il serait, en effet, extrêmement frustrant, pour un responsable, d'avoir consacré du temps à une analyse constatant l'existence de vulnérabilités et que rien ne se passe ensuite.

Un plan des actions les plus urgentes devrait donc être élaboré, et éventuellement discuté en Comité de Direction, dans des délais très courts après une analyse des enjeux.

5 Annexe 1 :

Exemple d'échelle de valeurs (Entreprise industrielle)

1. Gestion financière et budgétaire

Dysfonctionnement	***Niveau 1 Non significatif***	***Niveau 2 Important***	***Niveau 3 Très Grave***	***Niveau 4 Vital***
Perte financière	Perte < 1 M€	Perte comprise entre 1 M€ et 10 M€	Perte comprise entre 10 et 100 M€	Perte > 100 M€
Fraude ou détournement de fonds	Fraude ou détournement dans la gestion des achats et des paiements correspondants ou dans la gestion des livraisons.			
Incapacité à facturer les livraisons	Incapacité globale à facturer durant moins de 1 semaine	Incapacité globale à facturer comprise entre 1 semaine et 1 mois Perte des informations sur les livraisons effectuées sur une journée	Incapacité globale à facturer durant plus de 1 mois Perte définitive des preuves des livraisons d'une semaine	
Dysfonctionnement du processus de relance des clients	Indisponibilité temporaire de l'outil de relance	Indisponibilité durable de l'outil de relance		

2. Stratégie – Orientations générales – Pilotage et tableau de bord

Dysfonctionnement	***Niveau 1 Non significatif***	***Niveau 2 Important***	***Niveau 3 Très Grave***	***Niveau 4 Vital***
Divulgation de données ou d'informations relatives au budget, au plan à long terme ou la stratégie		Divulgation du plan à long terme d'une filiale Divulgation du budget Divulgation du tableau de bord mensuel	Divulgation d'informations sur des évolutions stratégiques majeures Divulgation du plan à long terme consolidé de l'entreprise	
Indisponibilité du système d'analyse des résultats et de reporting interne	Indisponibilité des outils nécessaires à	Incapacité à effectuer le reporting et		

	l'élaboration du tableau de bord mensuel	l'analyse des résultats durant plus de 2 mois		
Manipulation des données conduisant au reporting et au tableau de bord mensuel	Manipulation des données élémentaires ou des données élaborées à partie d'elles			

3. Développement commercial – Gestion de la clientèle

Dysfonctionnement	***Niveau 1 Non significatif***	***Niveau 2 Important***	***Niveau 3 Très Grave***	***Niveau 4 Vital***
Divulgation d'informations sur les opérations de développement commercial	Divulgation de notes et de synthèses sur la stratégie commerciale			
Divulgation de conditions économiques	Divulgation à un client des conditions économiques faites à un autre client	Divulgation de documents sur la stratégie de fixation des prix	Divulgation des conditions économiques faites à l'ensemble des clients	
Divulgation d'informations sur les clients	Divulgation de quelques éléments de la base clientèle	Divulgation de l'ensemble de la base clientèle		

4. Conduite de la recherche – Développements techniques

Dysfonctionnement	*Niveau 1 Non significatif*	*Niveau 2 Important*	*Niveau 3 Très Grave*	*Niveau 4 Vital*
Divulgation d'informations techniques	Divulgation de modèles de simulation	Divulgation de notes techniques courantes Divulgation d'information sur des spécifications ou procédés internes et sur des évolutions courantes	Divulgation de notes techniques dans des cas exceptionnels Divulgation d'informations sur l'impact d'évolutions techniques se traduisant par des fermetures de sites	
Rupture d'accords de confidentialité		Rupture d'accords de confidentialité avec des partenaires	Rupture d'accords de confidentialité passés avec des fournisseurs de technologie clé	
Perte de savoir-faire			Perte de l'ensemble des archives de mémos et de notes relatives aux développements techniques	

5. Gestion de l'outil industriel – Projets d'évolution - Maintenance

Dysfonctionnement	*Niveau 1 Non significatif*	*Niveau 2 Important*	*Niveau 3 Très Grave*	*Niveau 4 Vital*
Perte d'archives de documents sur les projets d'évolution Perte de la documentation technique des équipements existants	Perte des archives d'un projet pendant le cours du projet Perte d'originaux de plans d'équipements officiellement approuvés par les autorités locales ou régionales	Perte totale des archives de longue durée relatives à la vie des équipements et aux modifications		

Dysfonctionnement	*Niveau 1 Non significatif*	*Niveau 2 Important*	*Niveau 3 Très Grave*	*Niveau 4 Vital*
Dysfonctionnement conduisant à utiliser des plans d'installation faux lors d'évolutions			Erreur ou altération des plans des installations existantes ou dysfonctionnement de la gestion des modifications	
Divulgation d'informations techniques		Divulgation des thèmes de travail et du programme d'études d'avant projet	Divulgation de dossiers complets sur des avant projets (comprenant le positionnement stratégique du projet)	
Indisponibilité des outils support de la gestion de projets (planning, gestion des commandes, dossiers administratifs, etc.)	Indisponibilité de l'outil interne de suivi des plannings Indisponibilité de l'outil de gestion des commandes durant moins de 1 semaine	Indisponibilité de l'outil de gestion des commandes relatives aux projets durant plus de 1 semaine		
Dysfonctionnement dans la gestion de la maintenance	Perte de la base de données des actions de maintenance planifiées	Indisponibilité des outils de gestion de la maintenance durant moins de 1 mois Perte des données techniques et historiques requises pour planifier la maintenance	Indisponibilité des outils de gestion de la maintenance durant plus de 1 mois Altération du paramétrage des outils de gestion de la maintenance	

6. Production et expéditions – Logistique

Dysfonctionnement	*Niveau 1 Non significatif*	*Niveau 2 Important*	*Niveau 3 Très Grave*	*Niveau 4 Vital*
Arrêt de la production (absence d'énergie, indisponibilité du système de contrôle, perte d'une installation critique)	Arrêt de la production durant moins de 1 semaine	Arrêt de la production durant entre 1 semaine et 1 mois	Arrêt de la production durant entre 1 et 3 mois	Arrêt de la production durant plus de 3 mois Perte d'une

		Perte d'une installation critique conduisant à un arrêt de production de moins de 1 mois	Perte d'une installation critique conduisant à un arrêt de la production de 1 à 3 mois	installation critique conduisant à un arrêt de la production de plus de 3 mois
Indisponibilité des outils de pilotage de la production	Indisponibilité des outils de pilotage de la production durant moins de 1 semaine	Indisponibilité des outils de pilotage de la production durant entre 1 semaine et 1 mois	Indisponibilité des outils de pilotage de la production durant plus de 1 mois	
Altération des outils de pilotage de la production ou falsification des paramètres de pilotage			Altération du pilotage de la production conduisant à des produits hors spécification	Altération du pilotage de la production conduisant un accident ou à une détérioration de l'outil de production
Incapacité à assurer la logistique et les livraisons de produits	Incapacité à assurer les livraisons critiques pendant moins de 1 semaine	Incapacité à assurer les livraisons critiques pendant plus de 1 semaine		

7. Rapports avec les tiers (hors relations commerciales)

Dysfonctionnement	***Niveau 1 Non significatif***	***Niveau 2 Important***	***Niveau 3 Très Grave***	***Niveau 4 Vital***
Divulgation d'informations sur les résultats de l'entreprise		Divulgation prématurée d'informations sur les résultats d'une filiale	Divulgation prématurée d'information sur les résultats consolidés	
Dysfonctionnement du processus d'établissement des comptes annuels	Retard dans la sortie des comptes inférieur à 2 semaines	Retard dans la sortie des comptes supérieur à 2 semaines	Perte totale de tous les éléments comptables nécessaires à la sortie des comptes annuels	
Divulgation de notes ou mémos sur un risque fiscal ou une optimisation fiscale	Divulgation d'une note circonstanciée sur un risque fiscal ou une optimisation fiscale, selon l'objet de la note			
Perte des éléments historiques justifiant une	Perte des notes, mémos et synthèse ayant permis de justifier une opération fiscale			

opération fiscale				
Retards dans les paiements fiscaux		Indisponibilité des outils supportant le calcul ou le paiement de la TVA ou de la Taxe professionnelle		
Perte de documents officiels ou d'archives		Perte d'autorisations officielles d'exploiter	Perte des informations ou archives légalement exigibles de la part de l'administration (fisc, etc.)	

8. Gestion des contentieux, des affaires pénales et aspects juridiques

Dysfonctionnement	*Niveau 1 Non significatif*	*Niveau 2 Important*	*Niveau 3 Très Grave*	*Niveau 4 Vital*
Divulgation des pièces ou d'arguments relatifs à un contentieux	Divulgation relative à un contentieux courant	Divulgation relative à un contentieux exceptionnel		
Divulgation des pièces d'un dossier pénal impliquant le personnel		Divulgation des pièces d'un dossier pénal courant	Divulgation des pièces d'un dossier pénal dans un cas exceptionnel	
Perte ou disparition de documents originaux	Perte des originaux de contrats	Perte d'originaux de protocoles ou d'accords spécifiques		

9. Gestion des ressources humaines

Dysfonctionnement	*Niveau 1 Non significatif*	*Niveau 2 Important*	*Niveau 3 Très Grave*	*Niveau 4 Vital*
Divulgation d'informations sur des données personnelles	Divulgation du salaire d'un employé	Divulgation des salaires de l'ensemble du personnel	Divulgation répétée des salaires du personnel	
Retard dans le paiement des salaires	Retard < 2 jours	Retard compris entre 2 et 15 jours	Retard > 15 jours	
Destruction des données de base concernant le règlement de la paye (calcul et paramétrage)	Effacement des données récentes (moins d'un mois)	Effacement des données de l'année	Destruction des données et de tout l'historique	

10. Système d'information

Dysfonctionnement	*Niveau 1 Non significatif*	*Niveau 2 Important*	*Niveau 3 Très Grave*	*Niveau 4 Vital*
Indisponibilité du réseau et des serveurs (données partagées et personnelles)	Indisponibilité durant moins d'un mois	Indisponibilité durant plus d'un mois		
Indisponibilité de la messagerie	Indisponibilité de la messagerie			
Indisponibilité du réseau téléphonique	Indisponibilité du réseau téléphonique			
Perte complète d'archives		Parte des données des serveurs de données ou des archives		

		de la messagerie		
Ouverture injustifiée de droits d'administrateurs sur des systèmes			Altération de la table des droits et ouverture de droits d'administrateurs	
Divulgation de données systèmes ou d'architecture			Divulgation de rapports de synthèse ou d'informations détaillées sur la sécurité des systèmes et sur les failles non corrigées	

Tour Eria
5 rue Bellini
92821 Puteaux cedex
✆ + 33 1 53 25 08 80
clusif@clusif.fr

Téléchargez les bases de connaissances et la documentation de Méhari sur

https://clusif.fr/