Présentation fonctionnelle ARTEMIS

Analyse de risques des systèmes d'information

1. Pourquoi baser un outil d'analyse de risques sur un modèle de maturité ?

Une des définitions les plus communément admises d'un risque est celle-ci :

Un risque est la combinaison de la probabilité de la survenue d'un évènement et de sa gravité.

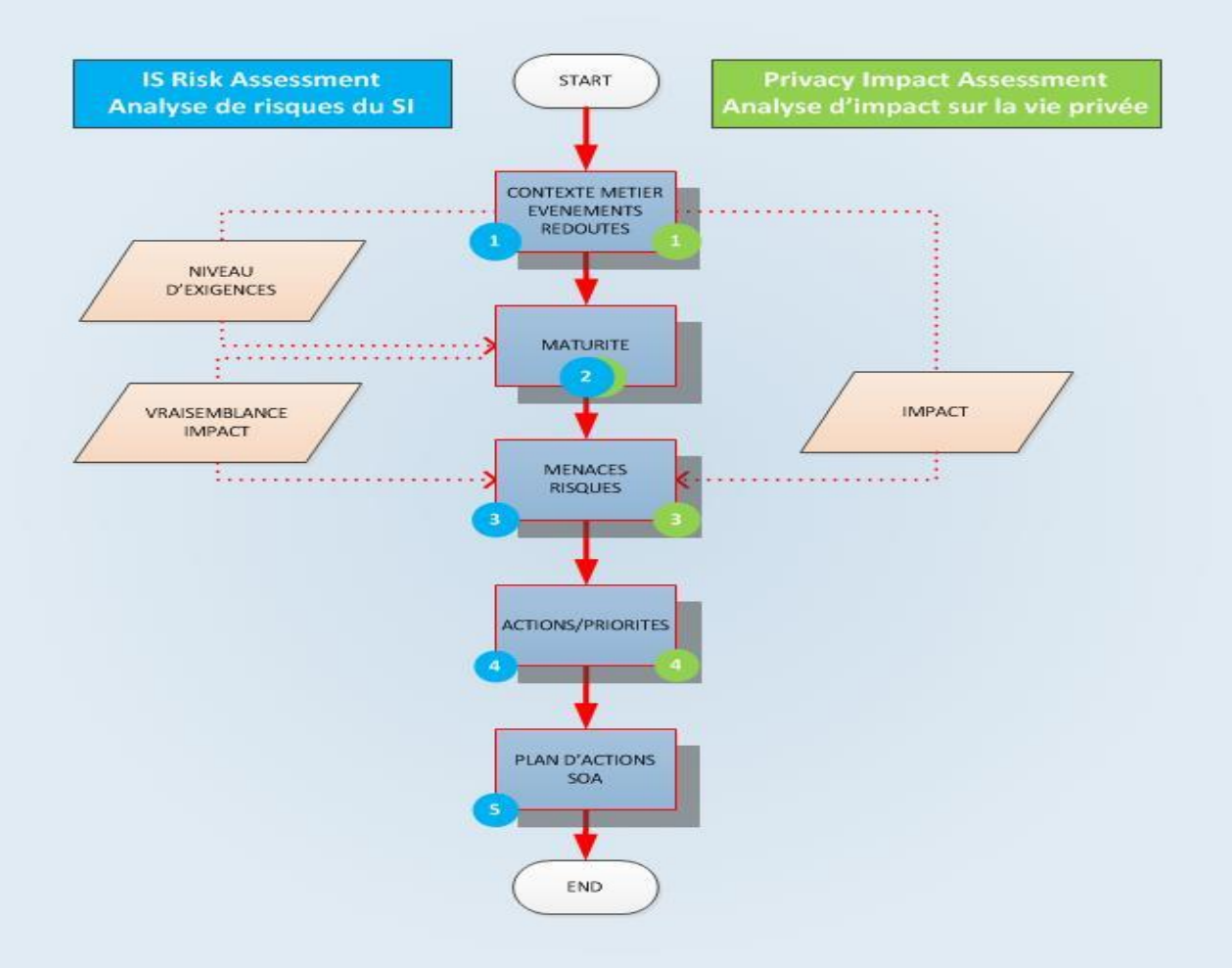
Si dans cette équation, l'évaluation de la gravité (ou l'impact, la nuisance) dans les projets informatiques est en général du ressort du "demandeur" (métier maîtrise d'ouvrage,...), l'évaluation de la probabilité demande une investigation dans un domaine qui reste principalement technique.
La démarche "classique", préconisée par l'ISO 27005, EBIOS, MEHARI, OCTAVE, etc., consiste à inventorier les actifs de l'information (ou biens essentiels), et de lister leurs biens supports. Une fois cet inventaire réalisé, une analyse des vulnérabilités des biens supports, en tenant compte l'inventaire des mesures existantes et par rapport aux 3 grands objectifs de sécurité (Confidentialité, Intégrité et Accessibilité), permet d'évaluer la probabilité d'événements liés à certaines menaces ou scénarios de risques.

Si cette démarche est correcte d'un point de vue logique et permet une analyse ciblée des risques, elle présente cependant le défaut de la lourdeur et nécessite beaucoup d'expérience, notamment dans l'évaluation du niveau de probabilité à partir des vulnérabilités identifiées.
Car il faut tout d'abord être conscient que les analyses de risques n'évaluent pas vraiment une probabilité (calcul mathématique objectivable d'une situation fictive), mais bien une vraisemblance, qui est un jugement subjectif sur la possibilité qu'un scénario de menace ou un risque, se produise.
La croyance en la valeur « scientifique », objective, des analyses de risques repose notamment sur cette confusion entre « estimation d'une vraisemblance » et « calcul probabiliste ». Si le calcul de risque dans les assurances voiture est réellement probabiliste, le « calcul » de risque en sécurité de l'information reste une estimation

humaine totalement subjective. La question se pose alors de savoir si le jeu (inventaire des actifs, des biens support, etc.) en vaut la chandelle (estimation subjective des risques).
Par rapport à d'autres approches d'analyse de sécurité, ARTEMIS préfère se baser, pour la partie "vraisemblance d'un événement", sur une évaluation de la maturité du système d'informations, plus systémique. ARTEMIS considère que l'évaluation de la maturité, quel que soit le périmètre envisagé, va forcément toucher au fonctionnement même de l'entièreté de l'organisation et donc apporter des solutions plus systémiques que l'approche classique décrite plus haut. Il faut signaler qu'ARTEMIS n'évalue pas UN niveau de maturité, mais plus de 40 ! Et ARTEMIS va confronter son modèle de maturité à plus de 100 mesures potentielles issues de l'ISO 27002.

Ce n'est donc pas une démarche simplifiée, mais bien systémique.

2. Rappel du processus global (flowchart)



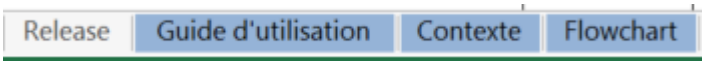
ARTEMIS s'articule autour de 5 étapes successives, chaque étape se nourrissant des résultats des étapes précédentes pour aboutir à un plan d'action adressant les menaces présentant les risques les plus élevés. Les différentes étapes sont :

- Questionnaire métier : établir avec les référents métiers le niveau d'exigences général de l'organisme et faire l'inventaire des événements redoutés pour permettre l'analyse d'impact.
- Analyse de maturité : sur base du cadre de l'ISO27002 (bonnes pratiques de la sécurité de l'information), analyser la maturité de l'organisation sous 48 facettes, sur base du principe qu'un niveau de maturité faible augmente la vraisemblance de certaines menaces standards.
- Analyse de risques : sur base de l'analyse d'impact (étape 1) et l'analyse de vraisemblance (étape 2), ARTEMIS va calculer, parmi 16 menaces standards, celles qui présentent le plus de risques pour l'organisation.
- Priorité des mesures : ARTEMIS va proposer les mesures ISO27002 les plus efficaces par rapport aux risques les plus élevés. En y ajoutant les pondérations sur le coût et la complexité d'une part, l'alignement stratégique d'autre part, ARTEMIS prioritise les mesures et permet de prendre une décision de traitement sur les risques identifiés.
- Plan de traitement : sur base des décisions de l'étape précédente, ARTEMIS propose un plan de traitement des mesures les plus efficaces, pour lesquelles une décision de traitement adéquate a été prise.

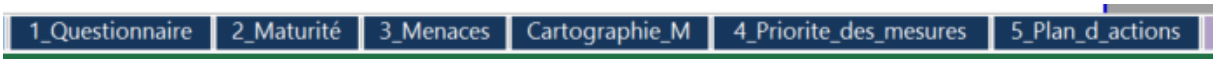
3. Présentation générale de l'interface

Pour des raisons de portabilité et d'interopérabilité, ARTEMIS a été bâti sur un tableur Excel qui comporte diverses catégories d'onglets :

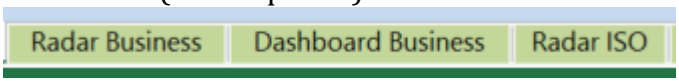
- Onglets d'information, comprenant une aide générale, des informations de contexte et des informations sur les différents releases d'ARTEMIS



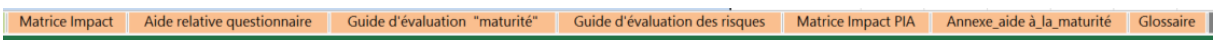
- Onglets interactifs représentant les 5 étapes du processus



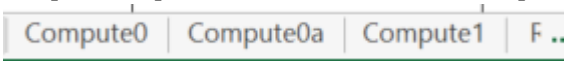
- Onglets infographiques produisant à différentes étapes du processus des résultats visuels (radars par ex)



- Onglets d'aide permettant d'aider l'utilisateur dans différents aspects (matrice d'impact, aide sur la maturité, etc.)



- Onglets de calculs, au départ cachés, contenant toute la logique de calcul d'ARTEMIS pour exploiter les données de chaque étape.



4. Etape 1 : Questionnaire métier – Niveau d'exigences – Worst Cases

a. Objectif général : établir un niveau d'exigence de sécurité général et identifier les évenements redoutés.
b. Public : référent(s) métier.
c. Durée estimée : 3h-4h
d. Description : Le questionnaire métier permet de connaître les attentes et les besoins du métier en termes de sécurité. Ce questionnaire se décompose en deux parties:

- La première partie identifie les types de données traitées et leur niveau de sensibilité, les contraintes et obligations métiers, etc. Cette partie permet de déterminer le niveau d'exigence à respecter en termes de confidentialité, d'intégrité et de disponibilité : répondez aux dix premières questions par ""Oui/Non "" en complétant éventuellement la réponse dans la zone de commentaire. En cas de réponses multiples (plusieurs ""Oui""), l'outil choisira le risque le plus élevé pour générer les exigences.

1	Veillez spécifier ci-dessous les types de données traitées	
	- Données disponibles publiquement	Non
	- Données non DACP - à faible valeur marchande - à faible valeur stratégique pour le business - à attractivité peu élevée	Non
	- Données non DACP - à forte valeur marchande - à forte valeur stratégique pour le business - à attractivité élevée	Oui
	- Données à caractère personnel permettant d'identifier (directement ou indirectement) des personnes	Oui
	- Données à caractère personnel sensibles telles que - l'origine ethnique ; - les opinions politiques ; - les convictions religieuses ou philosophiques ; - l'appartenance syndicale ; - la santé, l'orientation sexuelle ; - les suspicions, poursuites, condamnations pénales ou administratives	Oui
	- Données confidentielles sensibles telles que : - Sureté de l'Etat, Stratégie politique,... - Secret Défense. - Licences d'armes, licences et brevets sensibles en général.	Non

Les réponses aux exigences de cette partie doivent toujours correspondre aux situations de périodes critiques, s'il y en a !

- La seconde partie évalue l'impact sur le processus évalué suivant l'établissement d'évènements redoutés :
  - Classez le type d'impact par ordre d'importance;
  - Etablissez les pires scénarios d'incident pour chaque critère de sécurité dans la zone pourvu à cet effet;
  - Evaluez le niveau d'impact sur les scénarios d'incident choisis à l'aide du menu déroulant

- Remarques Importantes :
  - Ce questionnaire doit être parcouru à chaque cycle d'évaluation. En effet, les besoins en sécurité peuvent évoluer quand l'application métier subit des modifications
  - Le niveau d'impact doit être soigneusement choisi avec l'aide de la matrice d'impact disponible dans l'onglet ""Matrice d'impact""."

11	Quel serait l'impact métier en cas d'une indisponibilité prolongée du système critique?		Niveau d'impact estimé (voir matrice) :
	Perte fonctionnelle interne (démotivation, dysfonctionnement du service, surcharge...)		4 - Critique
	Perte financière (perte de budget, amendes, pénalités, condamnation au civil....)		4 - Critique
	Perte de réputation (image altérée dans le public, interpellation parlementaire, large échos dans la presse,...)		2 - Significatif
	'Perte de conformité (par rapport à un décret, une loi, une directive européenne,etc...)		2 - Significatif

5. **Et a**

Il est important de réunir un workshop pour réaliser cette étape. Il faut « challenger » les participants sur les niveaux d'impact ressentis et utiliser la matrice d'impact comme élément modérateur. Les participants sont peu habitués à cet exercice et ont souvent tendance à exagérer les impacts !

pe 2 : Analyse de maturité

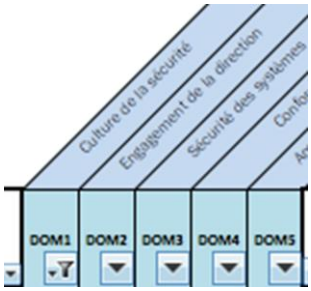
a. Objectif général : établir la maturité globale de l'organisation, sur base des bonnes pratiques de l'ISO27002, confrontées à un modèle de maturité.
b. Public : toute personne qui a une connaissance suffisante de la sécurité de son organisation, au sens ISO27002 du terme : CSI/RSSI, DSI, responsable RH, responsable MP,…
c. Durée estimée : 6 heures (très variable suivant public présent).
d. Description : En fonction du questionnaire métier, une liste d'exigences de sécurité préétablie a été filtrée par ARTEMIS. Il existe trois niveaux d'exigences de sécurité: Général (ESG) - Standard (ESS) - Forte (ESF). Dans le cas d'un niveau d'exigence maximum, 48 groupes d'exigences de sécurité devront être évalués en terme de maturité. Les niveaux de maturité représentent la manière dont une organisation exécute, contrôle, maintient et assure le suivi de ces exigences. Dans l'onglet « maturité », pour chaque exigence de sécurité appliquée déterminez le niveau de maturité à l'aide du menu déroulant.

 L'analyse de maturité est l'exercice le plus difficile et qui demande la plus grande expérience. N'hésitez pas à vous servir de l'aide à la maturité (dans les onglets d'aide). C'est un exercice qui reste subjectif parfois : cherchez le consensus avec vos interlocuteurs !

Il peut apparaître que, suivant le contexte particulier du périmètre, certaines exigences initialement demandées soient peu ou non pertinentes ; elles devraient dès lors être exclues de l'analyse . Dans ce cas, mettez un "X" dans la colonne prévue ("Pas applicable") au même niveau de la mesure non pertinente afin de la supprimer partiellement de l'analyse de maturité.

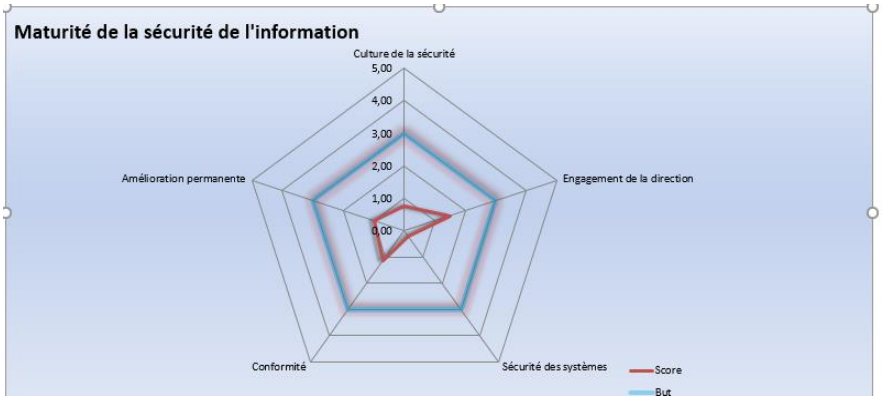
 Comment la maturité influence la sécurité : utilisez les filtres Excel. Pour commencer, n'affichez que les critères de maturité qui vont vraiment influencer l'analyse (Il y en a 48 au maximum). Filtrez à "OUI" cette colonne.

Ensuite, filtrez par exemple les critères de maturité qui concourent à l'axe "Culture de la sécurité".
Filtrez à "OUI" cette colonne.

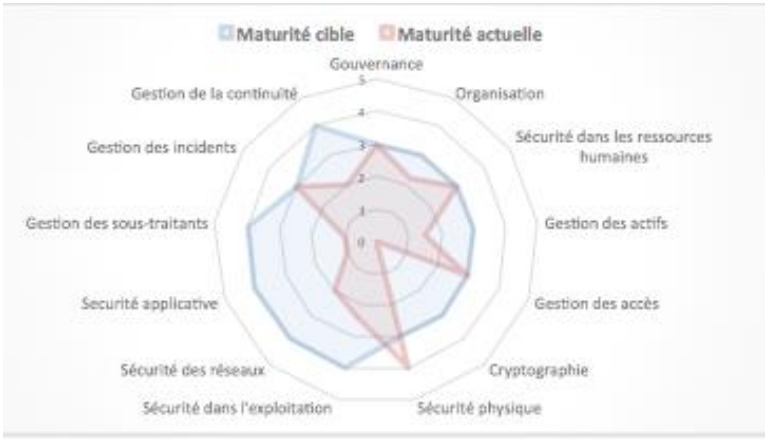


Nous avons à ce moment les quelques critères qui interviendront dans l'évaluation de maturité de l'axe Business "Culture de la sécurité" !

e. A ce stade, ARTEMIS, propose déjà des résultats visuels sur la maturité de l'organisation, qui sont 2 facettes d'une même réalité :
   - Une vue « Business » de la maturité sur 5 axes (Culture de la sécurité, engagement de la direction, conformité, sécurité des systèmes, amélioration continue)



   - Une vue « ISO27002 » de la maturité sur les différents axes de la norme.



6. Etape 3 : Evaluation de la menace – cartographie des risques

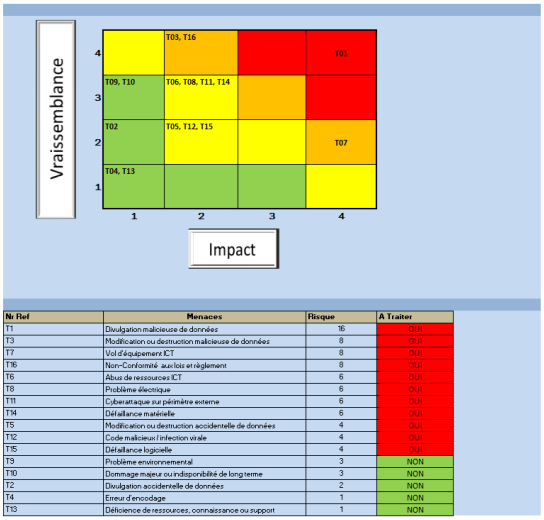
a. Objectif général : sur base des indicateurs de vraisemblance et d'impact calculés par ARTEMIS aux 2 étapes précédentes, établir la cartographie des risques par rapport à 16 menaces standards.
b. Public : les 2 publics précédents + le management.
c. Durée estimée : 2 h + 1h de présentation au management.
d. Description :
   - L'onglet "menaces" permet de faire l'appréciation des risques sur 16 menaces prédéfinies. Afin d'aider l'appréciateur, l'application calcule automatiquement la vraisemblance et l'impact pour chaque menace, à titre indicatif. Ces indicateurs proviennent des résultats des deux onglets précédents "Questionnaire" et "Maturité". L'utilisateur doit avoir présent à l'esprit que d'autres sources d'informations, non évoquées lors de l'analyse, peuvent influencer l'appréciation de ces deux paramètres. Il est donc nécessaire de confirmer les indicateurs

proposés par l'outil. Pour chaque menace, il vous est demandé d'évaluer la vraisemblance (colonne F) et l'impact potentiel (Colonne O).

	Evaluation du risque			Tolérence au risque:	4	? Back	Cartographie des risques	
	Id	Menace	Description	Indicateur de vraisemblance	Vraisemblance	Indicateur d'impact	Impact	Indicateur du Risque
1	T01	Divulgation malicieuse de données	Divulgation non autorisée et malicieuse de données confidentielles par le fait d'une personne/organisation interne ou externe, dans le but de tirer un bénéfice personnel ou de causer du tort à la société cible	↗	Haute	↗	Critique	
2	T02	Divulgation accidentelle de données	Divulgation accidentelle / erronnée de données confidentielles vers des personnes (internes ou externes) qui pourraient en tirer avantage	↗	Basse	↗	Mineur	
3	T03	Modification ou destruction malicieuse de données	Modification ou destruction non autorisée et malicieuse de données critiques par le fait d'une personne/organisation interne ou externe dans le but de commettre une fraude ou de causer du tort à la société cible	↗	Haute	↑	Significatif	
4	T04	Erreur d'encodage	Erreur accidentelle lors de l'encodage de données dans des applications ou systèmes résultant en des données erronées (non exactes ou non complètes) ou résultant en un dysfonctionnement des systèmes	↗	Très basse	↑	Mineur	
5	T05	Modification ou destruction accidentelle de données	Erreur accidentelle lors de la manipulation de données dans des applications ou systèmes résultant en des données détruites ou erronées (non exactes ou non complètes) ou résultant en un dysfonctionnement des systèmes	↗	Basse	↑	Significatif	
6	T06	Abus de ressources ICT	Abus de ressources ICT à des fins non autorisées mais sans mauvaise intention, résultant en perte de productivité et/ou dégradation du service	↗	Moyenne	↑	Significatif	
7	T07	Vol d'équipement ICT	Vol d'équipement ICT résultant en pertes matérielles et potentiellement en brèche de confidentialité et/ou disponibilité	↗	Basse	↑	Critique	
8	T08	Problème électrique	Problème électrique (coupure, fluctuation, interférence) résultant en une indisponibilité de services et / ou en données perdues ou corrompues	↓	Moyenne	↘	Significatif	
9	T09	Problème environnemental	Problème environnemental tel que début de feu, infiltration d'eau, surchauffe ou autre résultant en une indisponibilité de services et / ou en données perdues ou corrompues	↘	Moyenne	↑	Mineur	
10	T10	Dommage majeur ou indisponibilité de long terme	Désastre naturel, acte terroriste, grève à grande échelle ou autre résultant en dommages et / ou indisponibilité long terme de services	↘	Moyenne	↗	Mineur	
11	T11	Cyberattaque sur périmètre externe	Attaque malicieuse (déni de service ou autre) résultant en une perte de confidentialité, d'intégrité ou une indisponibilité / dégradation de services ou systèmes ICT	↗	Moyenne	↘	Significatif	
12	T12	Code malicieux / infection virale	Infection par virus, ver, cheval de troie ou autre code malicieux résultant en une indisponibilité de services ou systèmes ICT et / ou en brèche de confidentialité, intégrité ou disponibilité	↗	Basse	↗	Significatif	
			Déficience de ressources, connaissance ou support (en interne ou par le fait d'un					

- De plus, la "tolérance au risque" appelée communément "Appétit pour le risque " est introduite à ce niveau. En effet, la tolérance au risque peut être définie comme un niveau de risque que l'organisation est prête à accepter et à prendre pour atteindre ses objectifs stratégiques. C'est-à-dire que les risques dont la valeur est identique ou supérieure à ce niveau devront être traités. En fonction des objectifs stratégiques de l'organisation, cette valeur peut être modifiée au niveau de la cellule "F2".

- Après cela, vous pouvez visualiser la cartographie des risques en cliquant sur le bouton "Cartographie des risques" (cellule "P2") L'aperçu de la cartographie des risques est alors présentée automatiquement via l'onglet "Cartographie_M"



Nr Ref	Menaces	Risque	A Traiter
T1	Divulgation malicieuse de données	16	OUI
T3	Modification ou destruction malicieuse de données	8	OUI
T7	Vol d'équipement ICT	8	OUI
T16	Non-Conformité aux lois et règlement	8	OUI
T6	Abus de ressources ICT	6	OUI
T8	Problème électrique	6	OUI
T11	Cyberattaque sur périmètre externe	6	OUI
T14	Défaillance matérielle	6	OUI
T5	Modification ou destruction accidentelle de données	4	OUI
T12	Code malicieux / infection virale	4	OUI
T15	Défaillance logicielle	4	OUI
T9	Problème environnemental	3	NON
T10	Dommage majeur ou indisponibilité de long terme	3	NON
T2	Divulgation accidentelle de données	2	NON
T4	Erreur d'encodage	1	NON
T13	Déficience de ressources, connaissance ou support	1	NON

7. Etape 4 : Prioritisation des mesures

a. Objectif général : décider des mesures les plus efficaces pour les risques identifiés à l'étape 3, en les pondérant par rapport à 2 critères : coût/complexité et alignemanet stratégique. Décider ensuite du traitement à appliquer par rapport à chaque mesure :
   - Réduire le risque
   - Transférer le risque
   - Accepter le risque
   - Supprimer le risque

b. Public : le CSI/RSSI (ou le comité de sécurité) pour la partie « pondération », le management pour la partie « Décision de traitement ».

c. Durée estimée : 2 h pour la pondération + 1h de discussion avec le management.

d. Description :
   - Le bouton "Traitement" présent au niveau de l'onglet "Cartographie_M" permet l'exécution d'une macro visant à d'établir la liste des traitements/mesures prioritaires. Cette liste est présentée automatiquement lors de l'exécution de la macro via l'onglet "Priorité des mesures". Pour chaque mesure de sécurité associé au risque, il est nécessaire de déterminer sa priorité d'implémentation. La priorité d'implémentation est établie par l'évaluation de mise en œuvre et par la priorité stratégique de l'organisme :
     1. L'évaluation de mise en oeuvre correspond à la complexité et au coût d'implémentation de la mesure de sécurité.
     2. La priorité stratégique correspond aux lignes prioritaires correspondant aux valeurs et aux missions de l'organisation (définies par exemple dans un plan stratégique).
   - Le type de traitement du risque doit également être spécifié. Il existe 4 types de traitement du risque proposés: la réduction, le transfert, le maintien ou le refus du risque. Il est recommandé de toujours privilégier la réduction du risque avant d'envisager les trois autres options de traitement. Il s'agit toujours d'une décision managériale, vu les conséquences budgétaires, organisationnelles ou humaines qu'entraîne ce type de choix.

Mesures de sécurité	Ref Menace	Menaces	Niveau du Risque	Evaluation de mise en œuvre	Priorité Stratégique	Traitement	Priorité d'implémentation
Sous-traitant	T2	Divulgation accidentelle de données	12	2: Non élémentaire - coûts significatifs	2: Modérée	Transfert du risque	
	T11	Cyberattaque sur périmètre externe	12				
	T16	Non-Conformité aux lois et règlement	12				
	T3	Modification ou destruction malicieuse de données	9				
	T5	Modification ou destruction accidentelle de données	9				
	T1	Divulgation malicieuse de données	8				
Journalisation et surveillance	T2	Divulgation accidentelle de données	12	3: Facile - coûts limités	2: Modérée	Transfert du risque	
	T11	Cyberattaque sur périmètre externe	12				
	T12	Code malicieux / infection virale	12				
	T16	Non-Conformité aux lois et règlement	12				
	T3	Modification ou destruction malicieuse de données	9				
	T5	Modification ou destruction accidentelle de données	9				
	T1	Divulgation malicieuse de données	8				
	T4	Erreur d'encodage	8				
Exigences de sécurité	T2	Divulgation accidentelle de données	12				

Vous remarquerez qu'à ce stade, ARTEMIS a modifié la vue précédente, qui classait les menaces par rapport aux risques. A présent, ce sont les mesures de sécurité les plus efficaces sur les risques importants qui sont présentés. Et une mesure peut bien sûr influencer plusieurs menaces !

- Afin d'établir la priorité d'implémentation, il vous est demandé de complèter, pour chaque mesure de sécurité retenue, "l'évaluation de mise en œuvre" (colonne F), " la priorité stratégique" (colonne G) et le "traitement" (colonne H) au travers de menus déroulants.

 Décisions de traitement : il est indispensable d'impliquer le management dans les décisions sur le traitement des risques, vu les implications budgétaires et/ou organisationnelles que peuvent entraîner ces choix !

8. Etape 5 : plan de traitement

a. Objectif général : établir un plan d'actions de type ISO27002 pour l'analyse de risques en cours.
b. Public : CSI et/ou RSSI + Management
c. Durée estimée : 6h + 1h de présentation au management.
d. Description : La priorité d'implémentation établie, vous pouvez créer votre plan de traitement en cliquant sur le bouton "Plan de traitement"(cellule "I2"). Le plan de traitement est alors présenté automatiquement via l'onglet "Plan_de_traitement", qui reprend les mesures de sécurité analysées à l'étape précédente. Pour chacune d'entre elles, le type de traitement, la priorité ainsi que la référence et la description succinte de la mesure de sécurité ISO27002 associée sont indiquées dans le tableau. Les colonnes "H"et "I", respectivement nommées "Statut" et "Date d'échéance", vous permettent de pouvoir faire le suivi du plan.

Ref	Mesures de sécurité	Type de traitement	Priorité	réf_ISO	Description
6	Protection de l'environnement	Réduction du risque	8	11.1.4	Concevoir et d'appliquer des mesures de protection physique contre les dommages causés par les incendies, les inondations, les tremblements de terre, les explosions, les troubles civils et autres formes de catastrophes naturelles ou de sinistres provoqués par l'homme.
4	Protection contre des logiciels malv	Réduction du risque	6	12.2.1	Mettre en oeuvre des mesures de détection, de prévention et de récupération pour se protéger des codes malveillants ainsi que des procédures appropriées de sensibilisation des utilisateurs. Lorsque l'utilisation de code mobile est autorisée, que la configuration garantisse que le code mobile fonctionne selon une politique de sécurité clairement définie et d'empêcher tout code mobile non autorisé de s'exécuter
9	Documentation de développement	Réduction du risque	6	14.2.5	Des principes d'ingénierie de la sécurité des SI sont établis, documentés, tenus à jour et appliqués à tous les travaux de mise en oeuvre des SI

Utilisation d'ARTEMIS pour une DPIA (Data Privacy Impact Assessment)

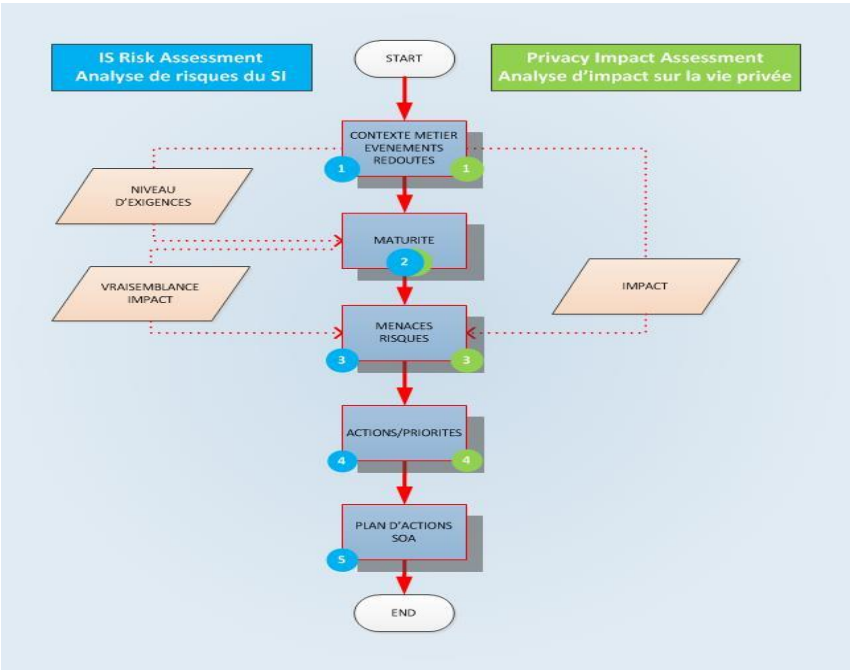
1. Portée d'ARTEMIS dans une DPIA

ARTEMIS réalise la partie « Analyse de risque » du contexte global d'une DPIA.

Figure 3 – La démarche de conformité à l'aide d'un PIA

2. Démarche globale d'une DPIA

La démarche est identique mais de fait en 4 étapes. La dernière étape d'ARTEMIS, le plan de traitement, n'est pas prévue. Ci-dessous les étapes de la DPIA (pastilles vertes).



3. Déroulement d'une DPIA et différence avec l'analyse de risques classique.

a. Etape 1 : Questionnaire métier – Niveau d'exigences – Worst Cases

La première partie de l'étape 1 (niveaux d'exigences) est identique, par contre l'analyse d'impact, est propre à la DPIA, et propose 8 questions d'impact sur les évènements redoutés de type :

- Accès illégitimes aux données à caractère personnel
- Modification non désirées des données à caractère personnel
- Disparition des données à caractère personnel

PIA: Evaluation des événements redoutés sur la vie privée si aucune mesure de sécurité n'existait autour des données

1	Quel serait l'impact "Privé" en cas d'un accès illégitime volontaire ou non aux données à caractère personnel de la personne?	Aucune	Niveau d'impact estimé (voir matrice) :	Décrire ci-dessous le scénario d'incident :
	Impacts coporels		4 - Maximale	*Les données sont vues par des personnes qui n'ont pas à les connaître, sans que celles-ci ne les exploitent.*
	Impacts moraux		3 - Important	
	Impacts matériels		1 - Négligeable	
	Impacts génériques (directs et indirects)		1 - Négligeable	
2	Quel serait l'impact "Privé" en cas de modification divulgation involontaire ou non d'informations sensibles?	Stockage	Niveau d'impact estimé (voir matrice) :	Décrire ci-dessous le scénario d'incident :
	Impacts coporels		2 - Limité	*Les données sont copiées et sauvegardées à un autre endroit sans être davantage exploitées*
	Impacts moraux		4 - Critique	
	Impact matériels		1 - Négligeable	
	Impact génériques (directs et indirects)		2 - Limité	
3	Quel serait l'impact "Privé" en cas de modification divulgation involontaire ou non d'informations sensibles?	Rediffusion	Niveau d'impact estimé (voir matrice) :	Décrire ci-dessous le scénario d'incident :
	Impacts coporels		2 - Limité	Les données sont diffusées plus que nécessaire et échappent à la maîtrise des personnes concernées (ex.: diffusion non désirée d'une photo sur internet, perte de controle d'informations publiées dans un réseau social...)
	Impacts moraux		1 - Négligeable	
	Impacts matériels		1 - Négligeable	
	Impacts génériques (directs et indirects)		1 - Négligeable	

b. Etape 2 : Analyse de maturité

L'étape 2 est identique à une analyse de risque classique et peut donc être utilisés telle quelle si elle a déjà été réalisée.

c. Etape 3 : Evaluation de la menace – cartographie des risques

L'étape 3 évalue les risques par rapport à 45 menaces dont :

- 14 sur la confidentialité
- 8 sur l'intégrité
- 23 sur la disponibilité

Critères bloche	Type de supp	Actions	Exemples de menaces	Exemples de vulnérabilités des supports	Vraisemblance	Impact	Risque	Evaluation	Justification
MD36	Personnes	Surchargées	Charge de travail important, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée ou mauvaise utilisation des compétences	Ressources insuffisantes pour les tâches assignées, capacités inappropriées aux conditions de travail , compétences inappropriées à la fonction. Incapacité à s'adapter au changement					
MD37	Personnes	Détériorés	Accident du travail, maladie professionnelle, autre blessure ou maladie, décès, affection neurologique, psychologique ou psychiatrique	Limites physiques, psychologiques ou mentales					
MD38	Personnes	Perdues	Décès, retraite, changement d'affectation, fin de contrat ou licenciement, rachat de tout ou partie de l'organisation	Faible loyauté vis-à-vis de l'organisme , faible satisfaction des besoins personnels, facilité de rupture du lien contractuel					
MD39	Documents Pa	Utilisés de manière inadaptée	Effacement progressif avec le temps, effacement volontaire de parties d'un texte, réutilisation des papiers pour prendre des notes sans relation avec le traitement, utilisation des cahiers pour faire autre chose	Modifiable (Support papier au contenu effaçable, papiers thermiques non résistants aux modification de températures					
MD40	Documents Pa	Détériorés	Vieillissement de documents archivés, embrasement des dossiers lors d'un incendie	Composant de mauvaise facture (fragile, sujet au vieillissement), n'est pas approprié aux conditions d'utilisation					
MD41	Documents Pa	Perdus	Vol de documents, perte de dossiers lors d'un déménagement, mise au rebut	Portable					
MD42	Canaux papier	Surchargés	Surcharge de courriers , surcharge d'un processus de validation	Existence de limites quantitatives ou qualitatives					
MD43	Canaux papier	Détériorés	Coupure du flux suite à une réorganisation, blocage du courrier du fait d'une grève	Instable, unique					
MD44	Canaux papier	Modifiés	Modification dans l'expédition des courriers, réaffectation des bureaux ou des locaux, réorganisation de circuit papier, changement de langue professionnelle	Modifiable (remplaçable)					
MD45	Canaux papier	Perdus	Réorganisation supprimant un processus, disparition d'un transporteur de document, vacance de postes	Utilité non reconnue					

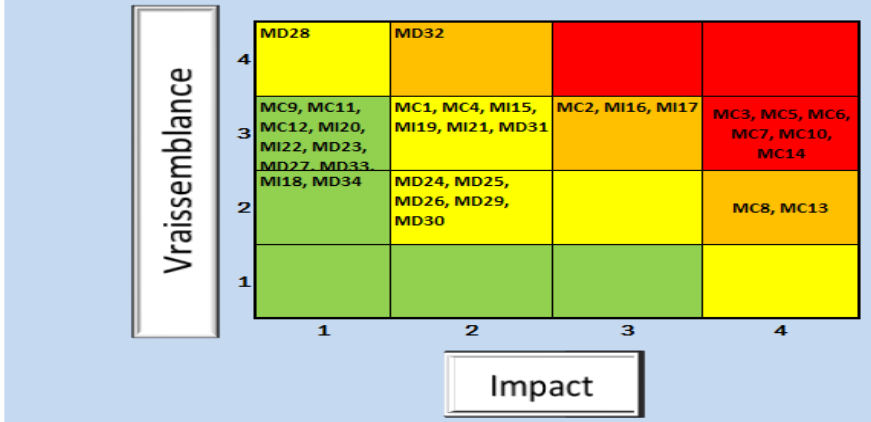
La cartographie des risques qui en résulte se présente comme ceci :

Aperçu de la cartographie PIA (*)

Organisation: XYZ

Date: 15-10-2016

(*) Basé sur l'analyse des menaces



Menaces	Risque	Mesure 1	Mesure 2	Mesure 3
Piégeage par un keylogger, retrait d'un composant matériel, branchement d'un appareil pour lancer un système d'exploitation ou récupérer des données	12	Protection des ressources	Responsabilité des utilisateurs	Protection des données sur des médias mobiles
Fouille de contenu, croisement illégitime de données, élévation de privilèges, effacement de traces, envoi de spams depuis la messagerie, détournement de fonction réseaux	12	Responsabilité des utilisateurs	Journalisation et surveillance	Politique de sauvegarde
Balayage d'adresses et ports réseau, collecte de données de configuration, étude d'un code source pour déterminer les défauts exploitables , test des réponses d'une base de données à des requêtes malveillantes	12	Responsabilité des utilisateurs	Télétravail	Journalisation et surveillance

Notons que contrairement à la démarche classique d'analyse de risques, ARTEMIS ne traite d'office que les risques supérieurs ou égaux à 12 et ne propose que les 3 mesures les plus pertinentes pour les réduire.

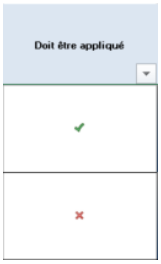
Annexe : exemples de méthodes de calcul d'ARTEMIS

1. Calcul d'impact

- Principe général : sur base des « worst cases » et de l'influence de chaque menace sur les objectifs de sécurité (C-I-A), un indicateur d'impact moyen est calculé par menace (Voir onglets « Compute0 » et « Compute2 »)
  - Compute0 : récupération des valeurs « Worst cases » et calcul des valeurs moyennes sur les critères C-I-A
  - Compute2 : répartition des valeurs précédentes par menace
- Apparition des indicateurs d'impact dans « Menaces »
- Dans certains cas, l'impact peut être diminué par un niveau de maturité suffisant dans certains domaines. Exemple : une bonne maturité dans la gestion des réseaux réduit l'impact par l'existence de possibilité de confinement lors d'une attaque (Voir onglet « Compute2 » et « Compute4b »). Seuls les niveaux de maturité >= à 3 diminuent l'impact.

2. Influence du niveau d'exigence sur l'analyse de maturité

- Principe général : les réponses au questionnaire métier donnent des indications sur le niveau d'exigences en termes C-I-A :
  - types de données traitées,
  - existence de sous-traitants,
  - besoins de disponibilité,
  - Etc.
- Chaque exigence de l'analyse de maturité est exprimée sur un des 3 niveaux :
  - ESG (générale)
  - ESS (standard)
  - ESF (Forte)
- De plus, chaque exigence de l'analyse de maturité est catégorisée :
  - GOUV (Gouvernance)
  - SPHY (Sécurité Physique)
  - GACC (Gestion des accès)
  - Etc.
- Dans l'onglet « Compute0a », on trouve la table de décision « Niveau<-> catégorie ».
- Par conséquent, certaines questions de maturité ne seront éventuellement pas posées en fonction du niveau d'exigences. Cela se traduira dans la colonne « Doit être appliqué » avec un « V » ou un « X » selon le cas.



3. Influence de la maturité sur la vraisemblance d'un risque

- Principe : une maturité basse augmente la vraisemblance d'une des 16 menaces standards d'ARTEMIS.
- Corollaire : les différents niveaux de maturité analysés (max. 48) n'influencent pas toutes les menaces de la même manière.
- Corollaire : les niveaux de maturité qui influencent les menaces n'ont pas le même « poids » sur chaque menace.
- L'Onglet « Compute4a » est le centre de calcul de la relation maturité-ISO27002 :
  - « Matching » entre les critères ISO et les 16 menaces
  - 48 critères d'évaluation X 16 menaces
  - 5 poids possibles de chaque critère pour une menace : 0, 1, 2, 4, 8
  - 3840 possibilités d'influence des mesures de sécurité sur les menaces
- Exemple :

Critère	Libellé	Menaces			
12.8	Gestion des vulnérabilités	T06. Abus de ressources ICT	T11. Cyberattaque sur périmètre externe	T12. Code malicieux – infection virale	T15. Défaillance logicielle
Poids relatif		4	8	8	2
Poids * inverse maturité Exemple : 2. Reproductible → 4		4*4 = 16	8*4 = 32	8*4 = 32	2*4 = 8
Poids global du critère « 12.8 Gestion des vulnérabilités » : 16+32+32+8 = 88					

4. Prioritisation des mesures de sécurité

Le principal général d'ARTEMIS pour donner une priorité aux mesures est celui-ci :
Quelle mesure influence le plus la menace présentant le risque le plus élevé ?
Pour calculer cette priorité, ARTEMIS combine 2 pondérations :

- Le poids global d'une mesure (PGM)
  - Somme des poids sur les menaces pour **une** mesure donnée (Diminution éventuelle si maturité mesure>maturité cible)
  - Transversal pour toutes les menaces
  - Ne tient pas compte du RISQUE
  - Exemple :

12.8	Gestion des vulnérabilités	T06.Abus de ressources ICT	T11. Cyberattaque sur périmètre externe	T12. Code malicieux – infection virale	T15. Défaillance logicielle
Poids par menace (Total : 88)		16	32	32	8
Poids potentiel GLOBAL par menace (Maturité minimum)		215	345	260	135
Participation de la mesure dans le poids global		16/215 = 0,074	32/345 = 0,092	32/260 = 0,123	8/135 = 0,059
				Participation TOTALE de la mesure = 0,074 + 0,092 + 0,123 + 0,059	0,3495

- Le poids d'une mesure sur le risque (PRM)
  - Est calculé comme suit pour chaque menace :

$$\frac{\text{Risque d'une menace}}{\text{Maturité de la mesure}}$$

  - Exprime le poids d'une mesure sur une menace
  - Tient compte du RISQUE
  - Exemple :

12.8	Gestion des vulnérabilités	T06.Abus de ressources ICT	T11. Cyberattaque sur périmètre externe	T12. Code malicieux – infection virale	T15. Défaillance logicielle
Poids de maturité par menace		3	3	3	3
Risque (onglet « Menaces »)		3	12	12	3
Risque / Poids		3/3 = 1	12/3 = 4	12/3 = 4	3/3 = 1

- Priorité d'une mesure :

12.8 Gestion des vulnérabilités	T06.Abus de ressources ICT	T11. Cyberattaque sur périmètre externe	T12. Code malicieux – infection virale	T15. Défaillance logicielle
PGM	0,35	0,35	0,35	0,35
PMR	1	4	4	1
Priorité de la mesure par menace	1*0,35 = 0,35	4*0,35=1,40	4*0,35=1,40	1*0,35 = 0,35

- La macro « Traitement » établit ensuite une priorité sur base des mesures ayant le plus de poids sur les risques les plus élevés.