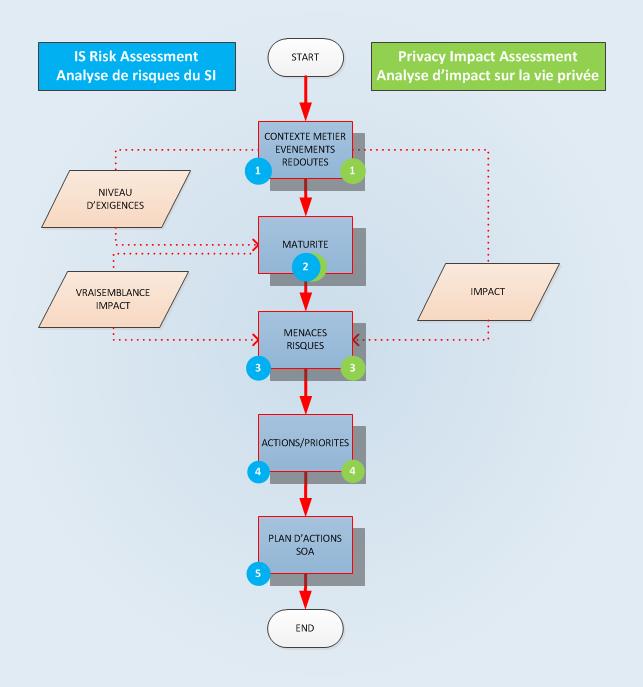
Présentation fonctionnelle ARTEMIS

1. 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 d’action : sur base des décisions de l’étape précédente, ARTEMIS propose un plan d’action des mesures les plus efficaces, pour lesquelles une décision de traitement adéquate a été prise.

1. Etape 1 : Questionnaire métier – Niveau d’exigences – Worst Cases
   1. Objectif général : établir un niveau d’exigence de sécurité général et identifier les évenements redoutés.
   2. Public : référent(s) métier.
   3. Durée estimée : 3h-4h
   4. 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.
      * La seconde 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 en fonction de la matrice d'impact disponible dans l'onglet ""Matrice d’impact""."

1. Etape 2 : Analyse de maturité
   1. Objectif général : établir la maturité globale de l’organisation, sur base des bonnes pratiques de l’ISO27002, confrontées à un modèle de maturité.
   2. 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,…
   3. Durée estimée : 6 heures (très variable suivant public présent).
   4. Description : En fonction du questionnaire métier, une liste d'exigences de sécurité a été établie par ARTEMIS. Il existe trois niveaux d'exigences de sécurité: Général (ESG) - Standard (ESS) - Forte (ESF). Dans le cas d'un niveau 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. 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.
2. Etape 3 : Evaluation de la menace – cartographie des risques
   1. 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.
   2. Public : les 2 publics précédents + le management.
   3. Durée estimée : 2 h + 1h de présentation au management.
   4. Description :
      * L'onglet "menaces" permet de faire l'appréciation des risques sur 16 menaces définies. 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'information, 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).
      * 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. Ici, la tolérance au risque est mise au niveau 4 par défaut. C’est-à-dire que les risques dont la valeur est identique ou supérieure à ce niveau devront être traités. Le niveau 4 correspond à la frontière entre la zone verte et jaune du tableau des risques. 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"
3. Etape 4 : Prioritisation des mesures
   1. 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
   2. Public : le CSI/RSSI (ou le comité de sécurité) pour la partie « pondération », le management pour la partie « Décision de traitement ».
   3. Durée estimée : 2 h pour la pondération + 1h de discussion avec le management.
   4. 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.
      * 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. La priorité d'implémentation établie, vous pouvez créer votre plan d'actions en cliquant sur le bouton "Plan d'actions"(cellule "I2"). Le plan d'actions est alors présenté automatiquement via l'onglet "Plan\_d'\_actions"
4. Etape 5 : plan d’actions
   1. Objectif général : établir un plan d’actions de type ISO27002 pour l’analyse de risques en cours.
   2. Public : CSI et/ou RSSI + Management
   3. Durée estimée : 6h + 1h de présentation au management.
   4. Description : L'onglet "Plan d'actions" reprend le plan d'actions initial reprenant les mesures de sécurité. 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 nommés "Statut" et "Date d'échéance", vous permet de pouvoir faire le suivi du plan d'actions.