Retour d'expérience

EBIOS Risk Manager

CLUBEBIOS

CLUBEBIOS

RETEX EBIOS Risk Manager – ALL4TEC

Gouvernance & SMSI / SAFRAN

Pierre-Marie ALLEMAND

Responsable du SMSI et de la gouvernance de sécurité

Safran – Contexte et historique

Organisation

- Groupe constitué de 13 sociétés, + filiales et JV.
- 1 RSSI par société + adjoint + équipe SSI. 30 personnes directement concernées par les AdR.
- Une direction centrale pour la sécurité du SI Groupe.

Démarche

- Mise en place d'une démarche d'homologation en 2013
- Basée sur Iso 27005 avec par défaut la méthode EBIOS 2010
- Utilisation des documents de l'ANSSI (niveau mezzo forte)
- Démarche initiée avec des moyens réduits, ressources RSSI dispersées

Safran – Contexte et historique

Centralisation

- La politique de sécurité, l'organisation et l'outillage ont été centralisés.
- Utilisation d'un fichier Excel et d'une procédure d'homologation.
- Contributif aux processus projets.

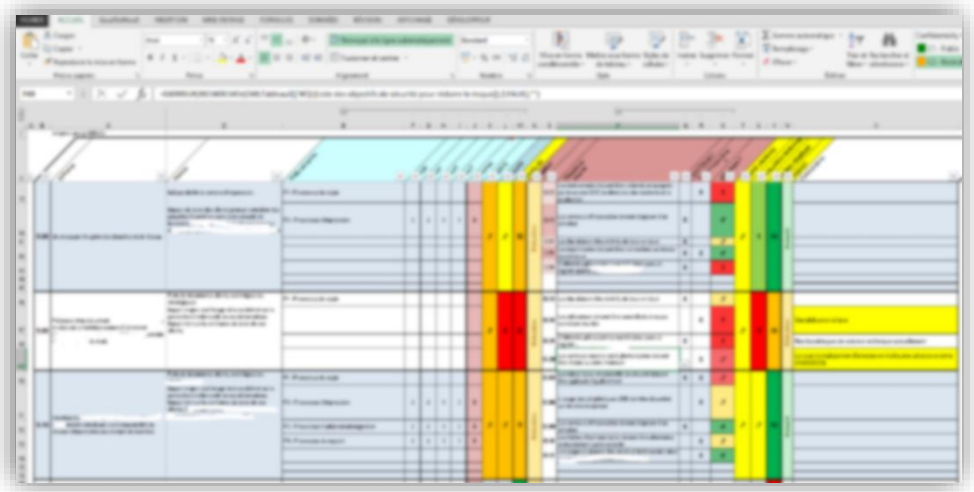
Progressivité

- Mise en place progressivement dans les sociétés.
- 5% à 10% des projets aboutissait à une analyse de risques avec homologation.
- 20% en central.

Pilotage

- Pilotage des sociétés pour suivre le déploiement et le respect du processus.
- Accompagnement et aide aux RSSI pour la mise en place de leur processus projet.
- Indicateur et retex.

Safran – Avant Agile Risk Manager



- Utilisation de fichier excel
  - ~8 ans d'amélioration continue
  - 11 onglets à remplir
  - 16 versions
- Arrive à ses limites
  - Copier/coller manuels
  - Pas de graphique
  - Des problèmes de cohérences

Lancement de la démarche d'outillage et choix d'Agile Risk Manager (ARM)

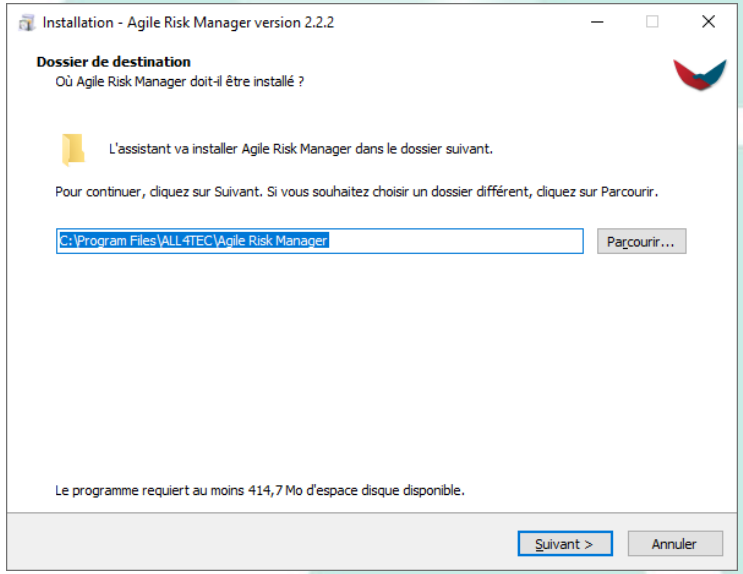
Safran – Agile Risk Manager

Facile à déployer	**Facile à exploiter**	**EBIOS RM**
Ouverture	**Adaptabilité**	**Production graphique**

Safran – Agile Risk Manager

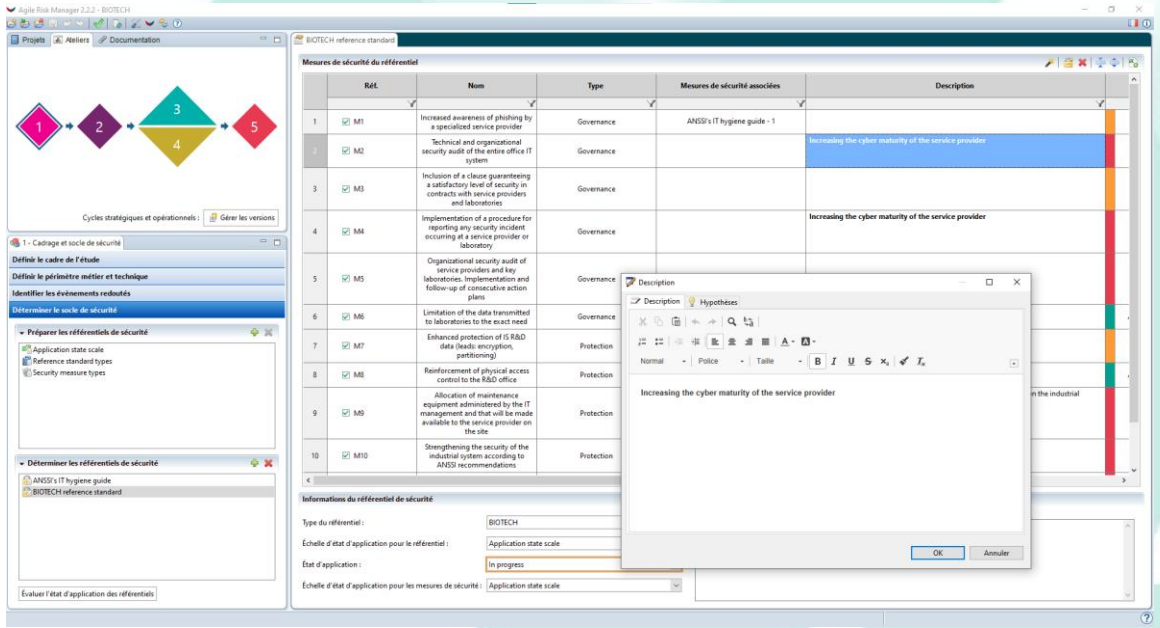
Facile à déployer

- Application onPremise, déploiement en quelques minutes malgré les différences d'environnement et d'organisation
- Pas de difficulté de gestion (ouverture de flux, etc.)



Safran – Agile Risk Manager

Facile à exploiter



- Ergonomie générale, facilité d'édition proche d'Excel, simplicité de la solution
- Respect des procédures existantes
- Les RSSI sont confrontés à de nombreux outils, un temps d'apprentissage trop long aurait bloqué le déploiement

Safran – Agile Risk Manager

EBIOS RM

- Respect de la méthode, consolidée par le label associé
- Souplesse suffisante
- Permet d'éviter de faire de mauvais raccourcis


AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Attestation de conformité à la méthodologie EBIOS Risk Manager
visant à labelliser les éditeurs de solutions logicielle standalone attribuée à :

ALL4TEC

Pour sa solution logicielle « Agile Risk Manager V1 »

Référence de l'attestation : ANSSI-01-001, valide jusqu'en juin 2022

Fait à PARIS, le 4 juin 2019

Guillaume Poupard
Directeur général de l'Agence nationale de la sécurité des systèmes d'information


AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Attestation de conformité à la méthodologie EBIOS Risk Manager
visant à labelliser les éditeurs de solutions logicielle client-serveur attribuée à :

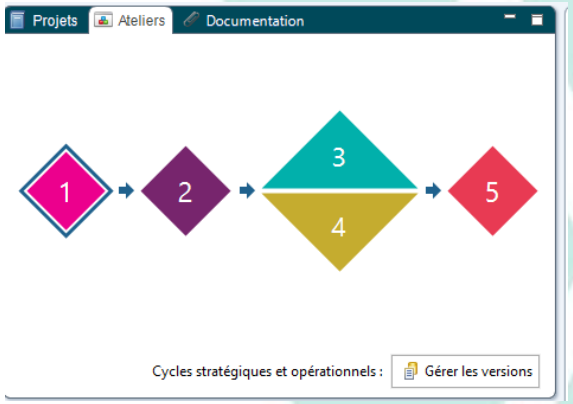
ALL4TEC

Pour sa solution logicielle « Agile Risk Manager V2.0 »

Référence de l'attestation : ANSSI-02-001, valide jusqu'en février 2023

Fait à Paris, le 29 janvier 2020

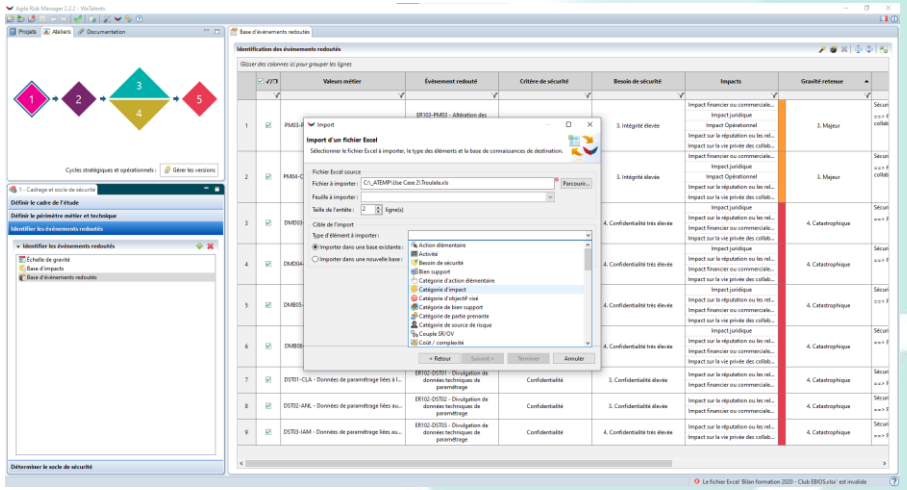
Guillaume Poupard
Directeur général de l'Agence nationale de la sécurité des systèmes d'information

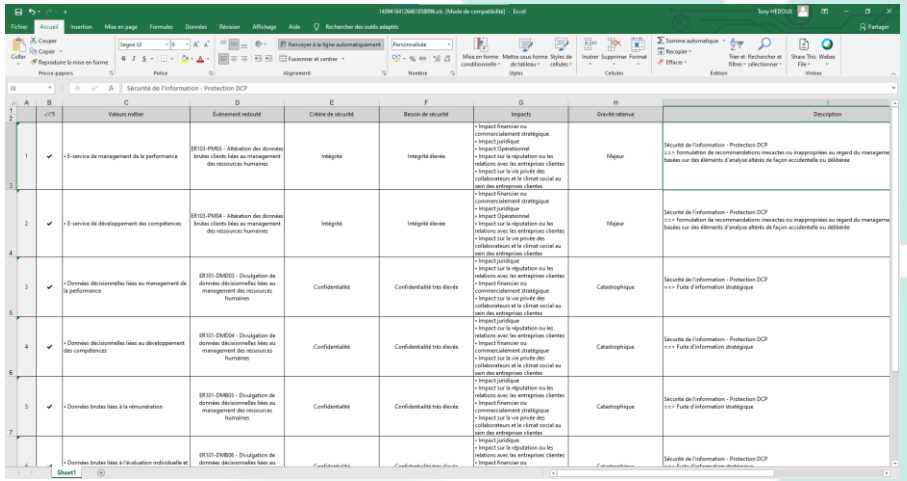


Safran – Agile Risk Manager

Ouverture

- L'application permet d'importer toutes les bases de connaissance à partir d'Excel : récupération simplifiée de l'existant
- L'application permet d'exporter toutes les bases au format Excel : interaction possible avec le reste de l'écosystème
- La combinaison des deux permet d'interagir avec tout le monde, y compris les personnes n'ayant pas l'outil

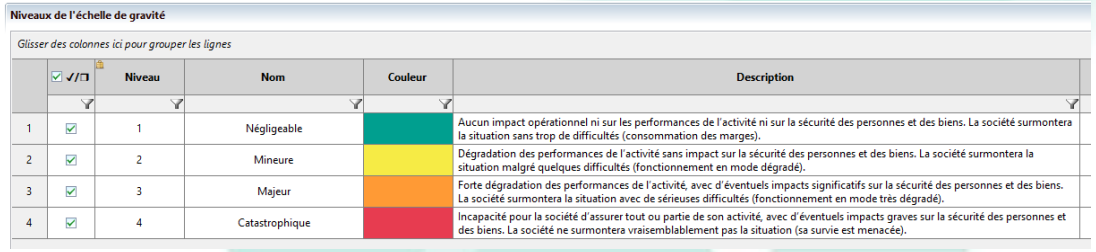




Safran – Agile Risk Manager

Adaptabilité

- L'application permet de redéfinir :
  - Toutes les échelles (DICT, gravité, impacts, niveaux de menaces, vraisemblances, etc.)
  - Toutes les matrices associées (acceptation du risque, etc.)



Niveaux de l'échelle de gravité

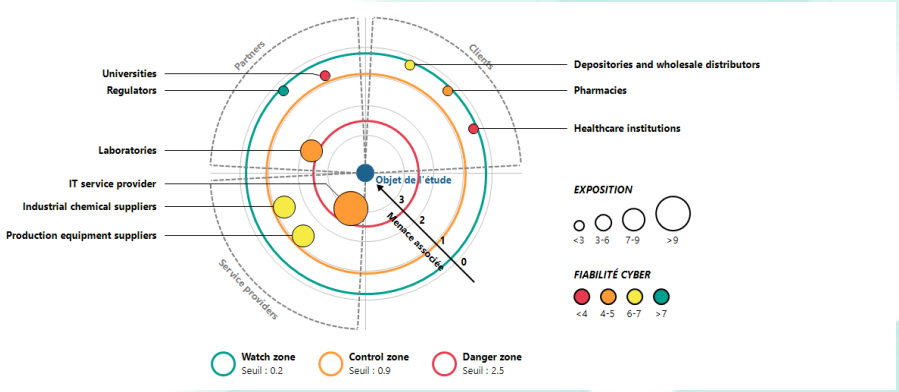
Glisser des colonnes ici pour grouper les lignes

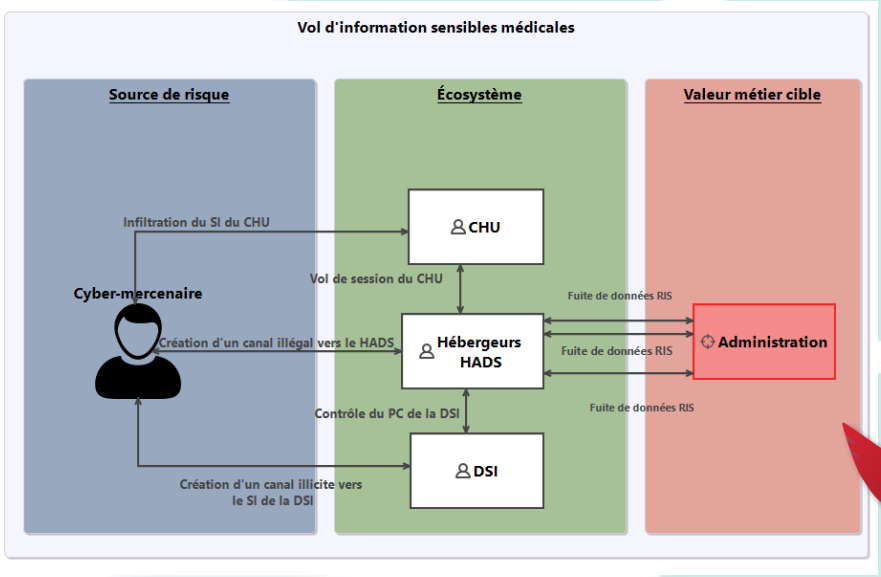
	✓/☐	Niveau	Nom	Couleur	Description
1	☑	1	Négligeable		Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges).
2	☑	2	Mineure		Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
3	☑	3	Majeur		Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé).
4	☑	4	Catastrophique		Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée).

Safran – Agile Risk Manager

Production graphique

- Sortie graphique pour les ateliers 2/3/4/5
  - Radars, Matrices
  - Scénarios stratégiques et opérationnels
- Renforce la valeur ajoutée de la méthode, en permettant de concrétiser l'aspect communication





Safran - Formation et accompagnement des RSSI

01

Certification EBIOS RM (3j)

02

Formation à l'outil (2h)

03

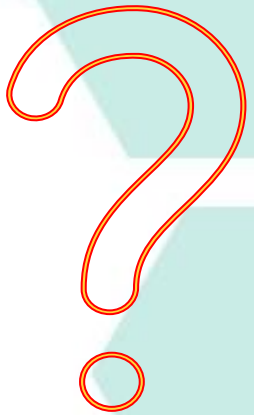
Support interne Safran (95% des questions)

04

Support complémentaire (5% des questions)

Difficultés et réflexions autour de la méthode – 1/2

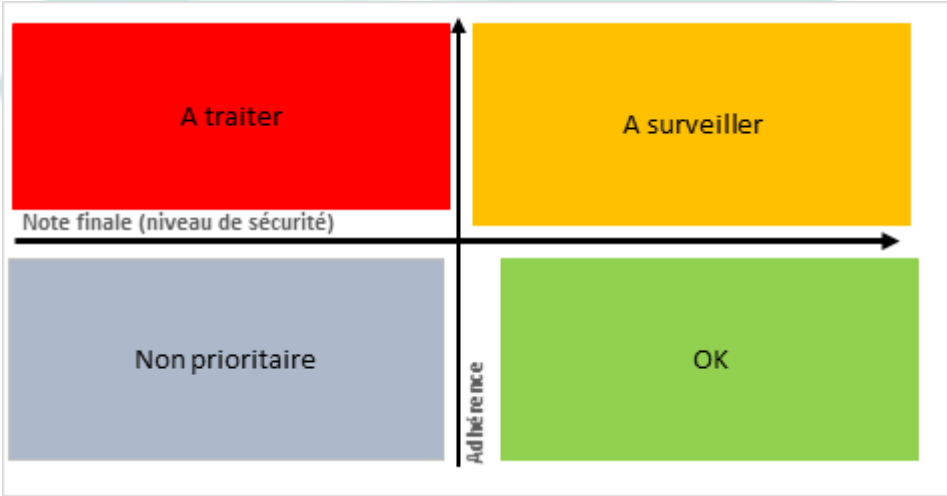
- A ce stade, très faible exploitation des ateliers 4, car le niveau de maturité nécessaire est élevé.
- Les visuels proposés par défaut à l'atelier 3 (autour de la menace), à trois niveaux de lecture, sont trop compliqués pour un ComEx.
- Les résultats obtenus sont plus subjectifs qu'avec EBIOS 2010.



EBIOS RISK MANAGER
ANSSI

Difficultés et réflexions autour de la méthode – 2/2

- Comment prendre en compte la problématique de l'adhérence du système analysé?



Améliorations possibles pour Agile Risk Manager

- Pouvoir porter sur les mesures de sécurité l'identification des types d'impact (occurrence, gravité).

- L'outil est actuellement centré sur des analyses individuelles. Le pilotage de la mise en œuvre de la PSSI est assurée via un fichier Excel externe.

Merci pour votre attention

CLUBEBIOS

CLUBEBIOS

Site : https://club-ebios.org
Twitter : @club_ebios
LinkedIn : https://fr.linkedin.com/company/club-ebios