Analyses de risques sécurité de l'information

Table des matières

L'analyse de risques : généralités

Le seul moyen d'identifier efficacement les mesures à mettre en place.

L'analyse de risque, une démarche normalisée :

- ISO 31000(management du risque)
- ISO 27005(management du risque de sécurité de l'information)

L'application de ces normes fait l'objet de diverses méthodes.

L'analyse de risques : définitions

Dans l'ISO 27000

Sécurité de l'information

Protection de la confidentialité, de l'intégrité, et de la disponibilité de l'information.

Disponibilité

Propriété d'être accessible et utilisable à la demande par une entité autorisée.

Intégrité

Propriété de protection de l'**exactitude** et de la **complétude** des actifs.

Confidentialité

Propriété selon laquelle l'information **n'est pas rendue disponible ou divulguée** à des personnes, des entités, des processus.

Actif

Tout élément représentant une valeur pour l'organisation (information, logiciels, actifs physiques, services, personnel, savoir-faire, réputation, image, …).

L'un des trois éléments constituant un risque.

Menace

Cause potentielle d'un incident indésirable, **qui peut nuire** à un système ou une organisation.

L'un des trois éléments constituant un risque.

Vulnérabilité

Faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces.

L'un des trois éléments constituant un risque.

Risque

ISO 27000 - Effet* de l'incertitude sur la réalisation des objectifs.

ISO 27005 - Possibilité qu'une **menace** donnée exploite les **vulnérabilités** d'un **actif** ou d'un groupe d'actifs et nuise donc à l'organisation

* *Ecart par rapport à des attentes*

Le risque est défini par : un actif, une vulnérabilité et une menace. Ces trois éléments sont nécessaires et suffisants.

Le niveau d'un risque peut être évalué à partir du niveau de vraisemblance de la menace, et de l'impact de l'atteinte à l'un des critères de sécurité sur l'actif considéré (lié au risque).

Vraisemblance

Possibilité que quelque chose se produise.

L'un des éléments d'évaluation du niveau d'un risque.

Impact

Changement radical au niveau des objectifs métiers atteints :

- Impacts financiers
- Impacts juridiques
- Impacts d'image…

L'un des éléments d'évaluation du niveau d'un risque.

Dans l'ISO 27005

Identification du risque

Processus utilisé pour trouver, lister et caractériser les éléments à risque.

Estimation du risque

Processus utilisé pour affecter des valeurs à la probabilité et aux conséquences d'un risque.

Analyse du risque

L'analyse du risque est constituée de l'**identification des risques** et de l'**estimation de ces risques**.

Evaluation du risque

Prise de décision vis-à-vis de chaque risque, par comparaison du niveau du risque aux critères d'évaluation du risque et aux critères d'acceptation du risque.

Appréciation du risque

L'appréciation du risque est constituée de son **analyse** et de son **évaluation**.

Communication du risque

Echange ou partage de l'information concernant un risque entre le décideur et les autres parties prenantes.

Maintien du risque

Acceptation du poids de la perte ou du bénéfice de gain découlant d'un **risque** particulier.

Réduction du risque

Mesures prises pour diminuer la probabilité, les conséquences négatives, ou les deux à la fois, associées à un risque.

Transfert du risque

Partage avec un tiers du poids de la perte ou du bénéfice de gain découlant d'un risque.

Evitement du risque

Décision de se retirer d'une situation à risque, ou de ne pas s'y engager.

Option de traitement du risque

Les options de traitement d'un risque sont :

- Son maintien,
- Sa réduction,
- Son transfert,
- Son évitement.

Analyse des risques : norme ISO 27005

1. Etablissement du contexte

Fixer les **critères** d'évaluation, d'impact et d'acceptation du risque ;
Fixer les **limites** du processus d'analyse des risques (en justifiant les exclusions) ;
Détailler **l'organisation** de la gestion du risque (qui, comment, qui tranche/décide, que garder/tracer).

2. Appréciation du risque

Général

Niveau de risque = f (conséquences découlant de l'occurrence d'un évènement indésirable ; probabilité d'occurrence de cet évènement)

Appréciation :

- déterminer la **valeur des actifs**,
- identifier les **menaces**,
- identifier les **vulnérabilités** (existantes ou possibles),
- identifier les **mesures** (existantes ou possibles),
- identifier les **conséquences** potentielles,
- **classer ces risques** par ordre de priorité.

L'identification du risque

Objectif : déterminer les évènements possibles, causant une perte potentielle, en donnant un aperçu de comment, où et quand cela pourrait se produire.

Moyens :

- Identification des **actifs**
- Identification des **menaces**
- Identification des **mesures de sécurité**
- Identification des **vulnérabilités**
- Identification des **conséquences**

L'estimation du risque

- **Plusieurs méthodes possibles :**

  - Simple: qualitative (« faible/moyen »)
  - Quantitative (« 97% de chances »)
- **Appréciation des conséquences** d'une atteinte à l'un des critères (DIC)
- **Appréciation de la vraisemblance** (dépend de l'expérience, statistiques, motivations, capacités, perception de l'attrait, vulnérabilités, mesures existantes)
- **Estimation du niveau de risque**

Évaluation du risque

Objectif : obtenir la liste des risques classés par ordre de priorité selon les critères d'évaluation, en relation avec les scenarios d'incident qui conduisent à ces risques.

3. Traitement du risque

Objectif : déterminer l'option de traitement (maintien, réduction, transfert, évitement) de chaque risque.

4. Acceptation du risque (explicitement par la direction)

Objectif : faire accepter les risques résiduels (i.e. après application des mesures) en justifiant l'acceptation des risques ne remplissant pas les critères d'acceptation.

5. Communication, surveillance et réexamen du risque

Objectifs :

1. **Communiquer :** faire connaître les informations relatives au risque aux parties prenantes.
2. **Surveiller :** veiller à ce que l'évolution du contexte n'influence pas l'évaluation et le plan de traitement des risques
3. **Réexaminer et améliorer :** surveiller le bon fonctionnement du processus de gestion des risques pour l'améliorer.

Annexes

- Définition du domaine d'application et des limites du processus de gestion
- Identification et évaluation des actifs et appréciation des impacts
- Exemple de menaces type
- Vulnérabilités et méthodes d'appréciation des vulnérabilités
- Approches d'appréciation du risque en sécurité
- Contraintes liées à la réduction du risque

Analyse des risques : méthode EBIOS

Contexte

EBIOS = **E**xpression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité

ISO 27005 est **un cadre** pour **toutes les méthodes** de gestion des risques SSI : elle énonce des lignes directrices.

« *La présente Norme internationale ne fournit aucune méthodologie spécifique à la gestion de risque en sécurité de l'information. [...] Plusieurs méthodologies existantes peuvent être utilisées en cohérence avec le cadre décrit dans la présente Norme internationale pour appliquer les exigences du SMSI* » [ISO 27005]

Une méthode telle qu'EBIOS est donc nécessaire pour les mettre en application de manière opérationnelle.

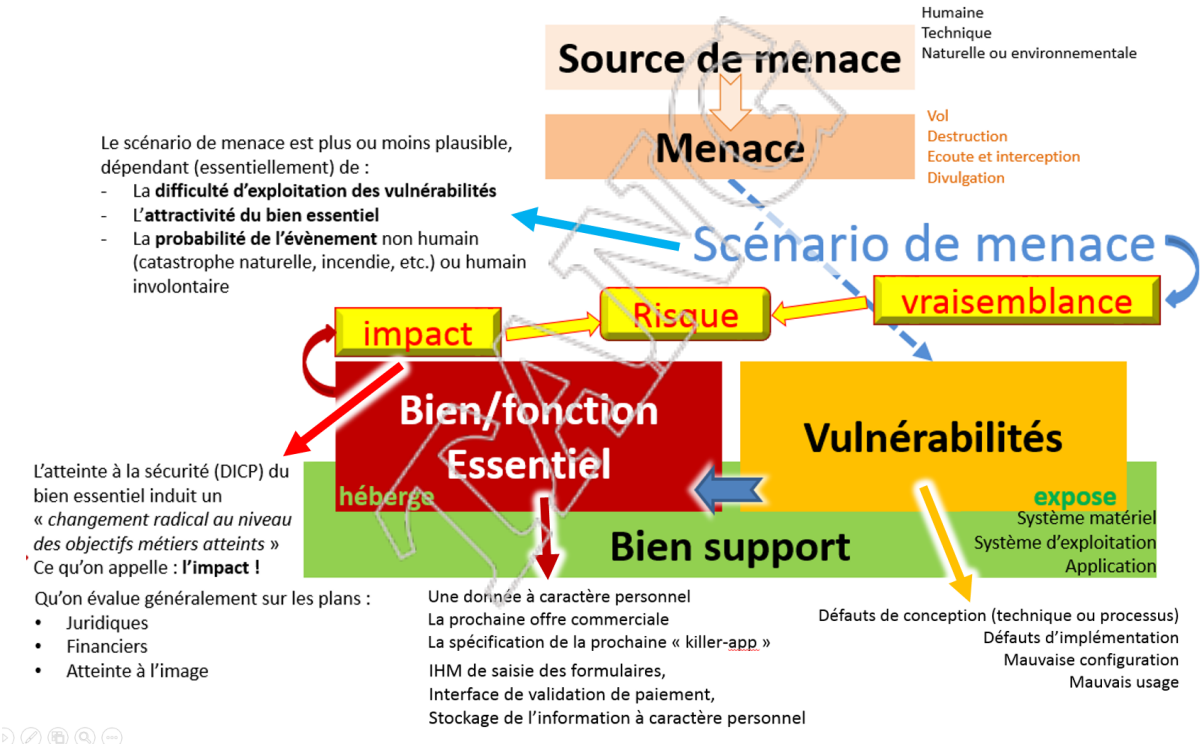
La méthode EBIOS est un outil complet de gestion des risques SSI conforme au RGS et aux dernières normes ISO 27001, 27005 et 31000.

Créée en 1995 par l'ANSSI et régulièrement mise à jour, la méthode bénéficie de ses 20 ans d'expérience dans le domaine de la gestion du risque.

ANSSI | Agence nationale de la sécurité des systèmes d'information

Elle permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information (SSI). Elle permet aussi de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires, constituant ainsi un outil complet de gestion des risques SSI.

Schéma de synthèse



Démarche : principe général

Une démarche en cinq modules :

1. **Étude du contexte**
2. **Étude des évènements redoutés** portant sur les **biens et fonctions essentiels**
3. **Étude des scenarios de menaces** portant sur les **biens support**
4. **Étude des risques** associant les évènements redoutés et leur impact avec les scenarios de menace et leur vraisemblance
5. **Étude des mesures de sécurité**

Reposant sur des **référentiels publics** facilitant la mise en œuvre :

- Référentiel des **sources de menaces** :

  Activité animale
  Catastrophe naturelle ou sanitaire
  Code malveillant d'origine inconnu
  Evènement interne
  Phénomène naturel
  Source humaine externe, malveillante, avec de faibles capacités
  Source humaine externe, malveillante, avec des capacités illimitées
  Source humaine externe, malveillante, avec des capacités importantes
  Source humaine externe, sans intention de nuire, avec des capacités illimitées
  Source humaine externe, sans intention de nuire, avec de faibles capacités
  Source humaine externe, sans intention de nuire, avec des capacités importantes
  Source humaine interne, malveillante, avec de faibles capacités
  Source humaine interne, malveillante, avec des capacités illimitées
  Source humaine interne, malveillante, avec des capacités importantes
  Source humaine interne, sans intention de nuire, avec des capacités illimitées
  Source humaine interne, sans intention de nuire, avec de faibles capacités
  Source humaine interne, sans intention de nuire, avec des capacités importantes

- Référentiel de **menaces génériques**,

  Exemple pour la catégorie « Réseau » :

  Attaque du milieu
  Dégradation du canal
  Déni d'actions
  Disparition du canal
  Ecoute passive
  Espionnage à distance
  Modification du canal
  Panne du matériel de télécommunications
  Saturation du système d'information
  Usurpation de droits
  Utilisation non autorisée du réseau

  Exemple pour la catégorie « Logiciel » :

  Abus de droits
  Analyse du logiciel, divulgation de failles ou de données
  Dépassement des limites du logiciel
  Détournement de l'usage prévu du logiciel
  Disparition du logiciel
  Dysfonctionnement du logiciel
  Erreur d'utilisation du logiciel
  Modification du logiciel
  Piegeage du logiciel
  Suppression de tout ou partie du logiciel
  Traitement illégal de données
  Usurpation de droits
  Vol du logiciel

  Exemple pour la catégorie « matériel » :

  Atteinte à la maintenabilité du matériel
  Dépassement des limites de fonctionnement du matériel
  Destruction du matériel
  Détérioration du matériel
  Détournement de l'usage prévu d'un matériel
  Espionnage d'un matériel
  Modification du matériel
  Perte d'alimentation énergétique
  Vol du matériel

  Exemple pour la catégorie « organisation » :

Abus de droits
Corruption de données
Déni d'actions
Données provenant de sources douteuses
Erreur d'utilisation
Panne de matériel
Traitement illégal de données
Utilisation de logiciels copiés ou de contrefaçon
Utilisation non autorisée du matériel
Violation de la maintenabilité du système d'information
Vol de matériel
Vol de supports ou de documents

- Référentiel de **vulnérabilités génériques**

  Exemple pour la catégorie « Logiciel » / menace « Détournement de l'usage prévu du logiciel » :

  Absence de politiques relatives à la bonne utilisation du logiciel
  Le logiciel permet de manipuler des données (supprimer, modifier, déplacer…)
  Le logiciel permet d'utiliser des fonctionnalités avancées
  Le logiciel peut être détourné de son usage nominal (offre la possibilité d'envois massifs…)

  Exemple pour la catégorie « Logiciel » / menace « Piégeage du logiciel » :

  Absence de copies de sauvegarde
  Chargement et utilisation non contrôlés du logiciel

1. Etude du contexte

Objectif

Circonscrire et décrire le champ d'investigation de l'étude et l'ensemble des paramètres à prendre en compte dans les autres modules.

Tâches

1.1 Définir le cadre de la gestion des risques, en identifiant

- Le **contexte** (interne, externe, processus de l'analyse, validation),
- Périmètre et interfaces de la ressource, exclusions de l'analyse
- Les **enjeux**,
- Les **contraintes spécifiques** (normatives, d'organisation, légales et réglementaires),
- Les **acteurs internes** et **externes** (parties prenantes, …)

Cette partie permet de savoir exactement de quoi on parle, et d'expliquer pourquoi on exclue certaines choses

1.2 Définir les sources de menaces et les métriques de l'étude

- **Sources de menaces** : internes, externes, malveillantes ou pas, virus, etc.
- **Echelles** : de besoins de sécurité, d'impact, de vraisemblance
- **Grille de gestion des risques** (croisement impact / vraisemblance)

Les échelles doivent être communes à toute l'organisation.

Exemple d'échelles (chaque organisation doit se fixer sa propre échelle en fonction de son contexte, mais normalement il ne devrait y avoir qu'une échelle pour toute l'organisation) :

Echelle d'impact :

IMPACT EN CAS DE REALISATION DE LA MENACE			
	Financier	Juridique	Réputation
4	> 10 M€	Pénal	Image durablement dégradée
3	1M€ à 10M€	Amende forte et publication	Forte médiatisation dans tous les médias, mais situation rattrapable
2	1k€ à 1M€	Amende forte	Forte médiatisation dans les médias spécialisés
1	< 1k€	Amende faible	Faible médiatisation

Echelle de vraisemblance :

PROBABILITE DE LA MENACE	
1	Nécessite une **très grande expertise et un très bon niveau technique** ; ainsi que des **moyens financiers inaccessibles à un particulier**, (même riche). Jamais arrivé depuis le début du service.
2	Nécessite un **bon niveau technique et un bon niveau technique**. Peut-être **financé par un particulier** à revenu moyen, si l'enjeu en vaut le coût. Arrive une fois tous les 5 ans environ.
3	Ne nécessite **pas d'expertise** et un **faible niveau technique**. Arrive deux trois fois par an.
4	Ne nécessite aucune compétence.

Matrice de risques :

Impact					
1	2	3	4		
1	1	2	2	1	Vraisemblance
1	2	2	3	2	
2	2	3	3	3	
2	3	3	4	4	

1.3 Identifier les biens

Pour le module 2 : les biens et processus essentiels, leurs responsables (et informations gérées par le bien essentiel)

Pour le module 3 : les biens et processus supports aux biens essentiels, leurs propriétaires

Pour le module 4 : les **relations entre les biens essentiels et supports**

Chaque bien/processus essentiel doit faire l'objet d'une description précise : entrées, traitements, sorties, acteurs…

Bien lister tous les éléments qui constituent le système étudié (site, défense périmétrique, matériel, OS, applications, etc.)

La matrice reliant chaque bien essentiel à ses biens support permet de combiner plus tard chaque impact et les vraisemblances.

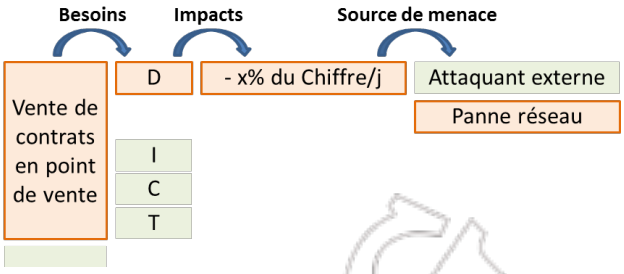
2. Etude des évènements redoutés (biens et fonctions essentiels)

Objectif

Identifier de manière systématique les scénarios génériques à éviter, d'un point de vue fonctionnel (plus que technique), sur les **biens essentiels**.

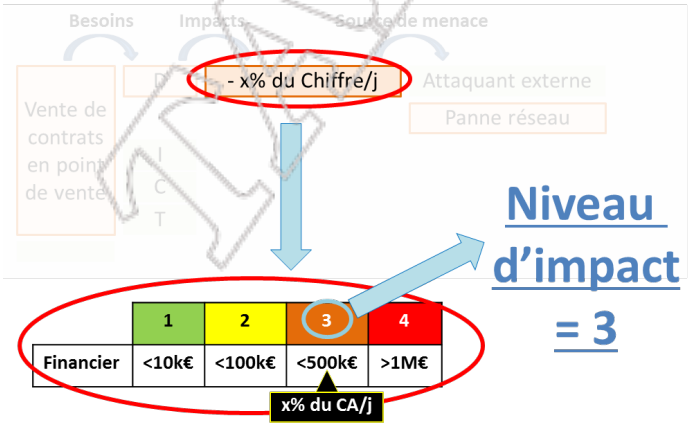
Tâches

2.1 Apprécier les évènements redoutés pour chaque bien essentiel, et sur tous les critères de sécurité retenus (DIC obligatoires selon l'ISO 27k).



Evènement redouté : « *Perte de disponibilité dans la vente de contrats en points de vente dû à une panne réseau* »

2.2 Evaluer le niveau d'impact des évènements redoutés, grâce à la matrice d'impacts définie au module 1.



2.3 Classer tous les évènements redoutés par impact décroissant.

L'objectif est de ne retenir que les évènements redoutés dont le niveau d'impact peut donner un risque inacceptable (pour au moins une valeur de la vraisemblance, d'après la matrice de risques, définie au module 1).

3. Etude des scenarios de menaces (biens support)

Objectif

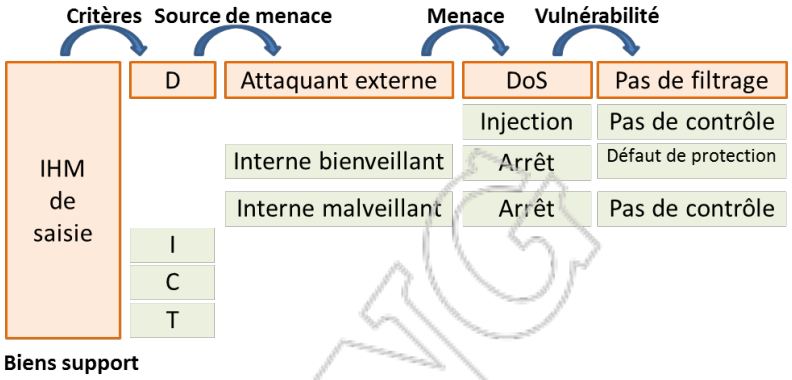
Identifier de manière systématique les modes opératoires génériques pouvant porter atteinte à la sécurité de l'information, sur le plan technique (plutôt que fonctionnel).

Tâches

Attention :

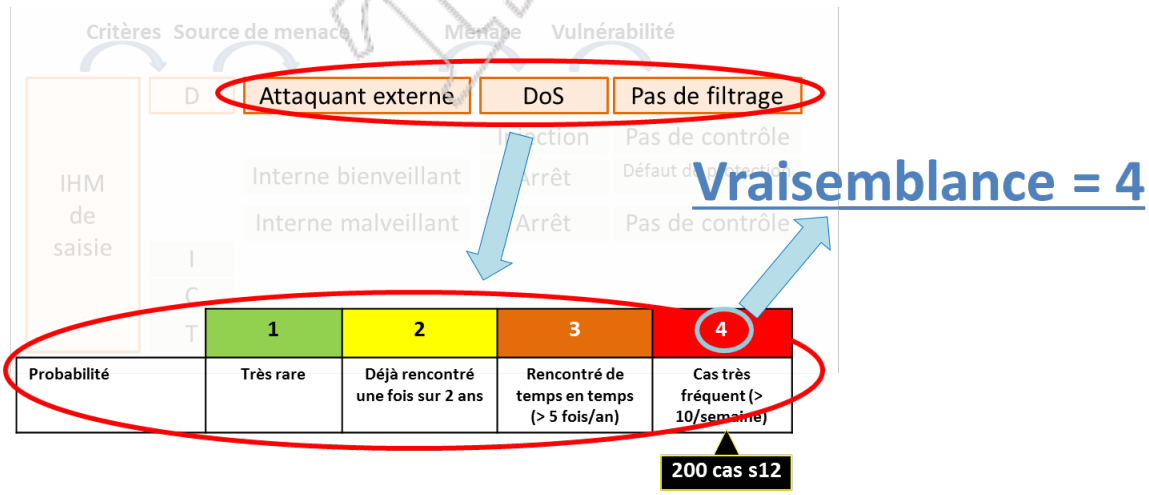
L'évaluation doit se faire sans considérer les mesures éventuellement en place. Puisque le but est d'abord d'identifier tous les risques « dans l'absolu », puis de voir quelles mesures (en place ou à mettre en place) peuvent les rendre acceptables.

3.1 Identifier et apprécier les scenarios de menace portant sur chacun des biens support



Scenario de menace : « *Un attaquant externe lance une attaque en déni de service contre l'IHM de saisie, qui n'a pas de filtrage* »

3.2 Evaluer le niveau de vraisemblance des scenarios de menace, grâce à la matrice de vraisemblance définie au module 1.



2.3 Classer tous les scenarios de menace par vraisemblance décroissante.

L'objectif est de ne retenir que les scenarios de menace dont le niveau de vraisemblance peut donner un risque inacceptable (pour au moins une valeur d'impact, d'après la matrice de risques, définie au module 1).

4. Etude des risques

Objectif

Mettre en évidence de manière systématique les risques, et choisir la manière de les traiter.

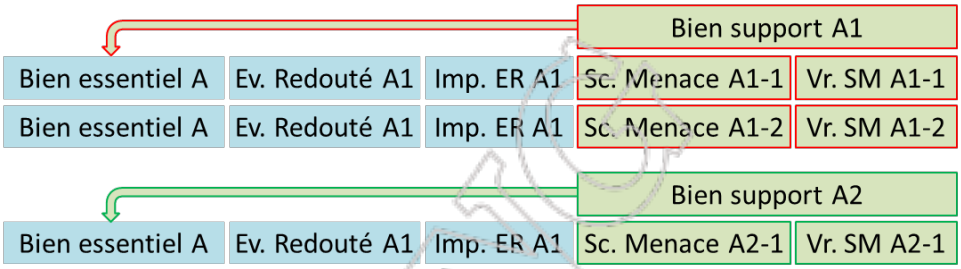
Tâches

4.1 Apprécier les risques : d'abord sans puis avec les mesures existantes

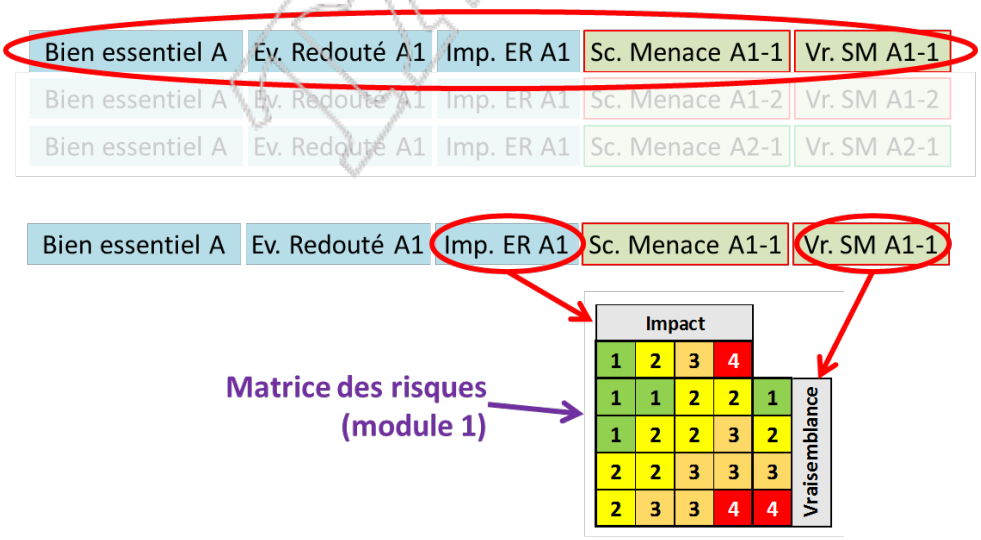
En utilisant le résultat des modules 1, 2 et 3 :

On associe à chaque évènement redouté tous les biens supports associés au bien essentiel (grâce au module 1), lié à l'évènement redouté (grâce au module 2).

Puis, pour chaque bien support, on reporte l'ensemble des scenarios de menace identifiés (au module 3).



Chaque ligne constitue alors un risque, quantifiable grâce aux valeurs de l'impact (de l'évènement redouté) et de la vraisemblance (du scénario de menace), à l'aide de la matrice de risques constituée au module 1.



4.2 Evaluer l'effet des mesures existantes, identifiées au module 1

Les mesures existantes identifiées au module 1 peuvent réduire le niveau des risques a priori inacceptables à un niveau acceptable. C'est pourquoi on intègre à ce stade ces mesures en place.

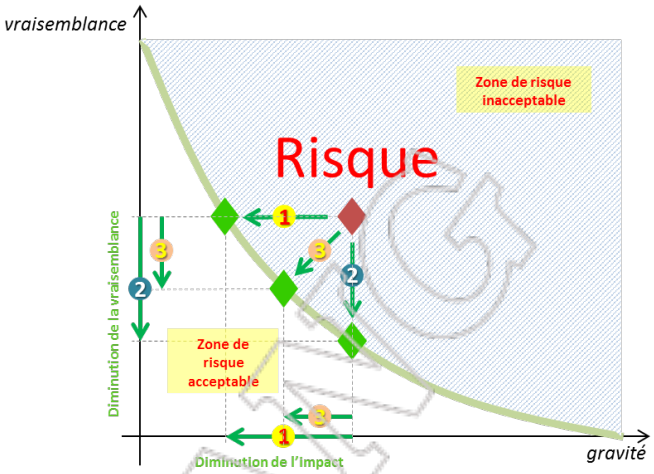
4.3 Classer les risques dans l'ordre décroissant et choisir les options de traitement

Pour chaque risque jugé inacceptable, il faut choisir l'une des options de traitement des risques :

- Maintien
- Réduction
- Transfert
- Evitement

5. Etude des mesures de sécurité

Dans ce dernier module, on considère les risques qui doivent être réduits, et pour chacun d'eux on recherche une mesure qui permet de rendre le risque acceptable.



Objectif

Chaque mesure doit ramener le risque au moins à un niveau acceptable.

Cela peut se faire en diminuant sa vraisemblance et/ou son impact.

Tâche

Les mesures peuvent être choisies d'abord d'une manière générique dans le référentiel proposé par la norme ISO (cf. ISO 27002).

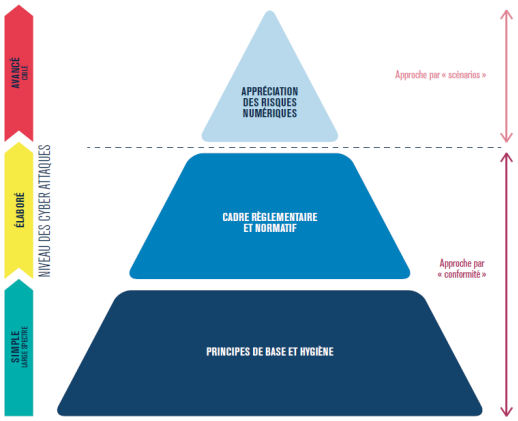
Mais ensuite il faut décrire le plan de mise en œuvre, ce dernier dépend de l'organisation et de l'existant.

A noter :

- Une mesure peut « traiter » plusieurs risques simultanément
- Une mesure peut ramener des risques à un niveau de risque plus bas que le plafond d'acceptabilité. Ce n'est pas un problème, mais l'objectif est de ne mettre en œuvre que les moyens minimums nécessaires, en prenant en compte l'existant et le contexte.

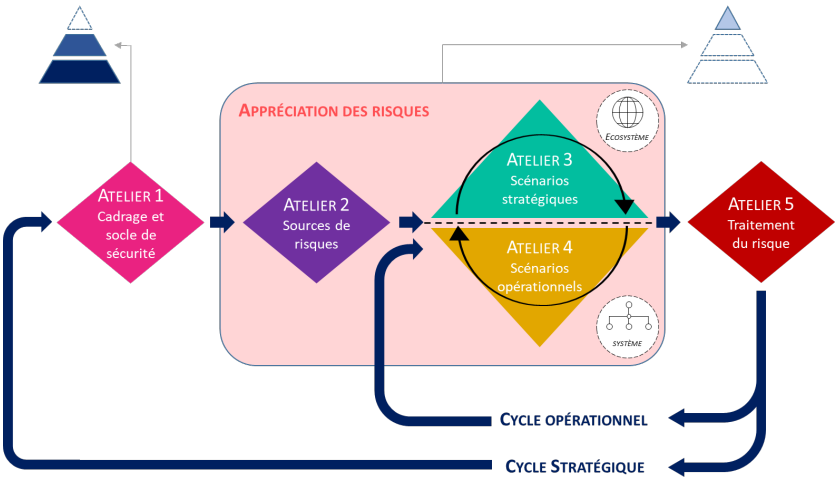
Analyse des risques : la méthode EBIOS RM

La méthode se décompose en deux parties : un **audit de conformité** pour tout ce qui est relatif aux principes de base et au cadre règlementaire et normatif (voir chapitre précédent), et une partie d'**appréciation des risques numériques** pour tout ce qui est « purement » métier.



La séparation se fait lors d'un premier atelier, dans lequel on identifie toutes les règles applicables au service analysé, dont on précise aussi les contours. Cet atelier permet aussi de bien cadrer les objectifs et parties prenantes de l'analyse, et les référentiels utilisés (impacts, vraisemblance, risques, etc.).

Contrairement à EBIOS, l'analyse **EBIOS RM se positionne beaucoup du point de vue de l'attaquant** : on essaye de voir qui pourrait avoir intérêt à compromettre le service ou ses données (la *source de risques*) et pour quelles raisons (l'*objectif visé*). En découlent l'attrait et la vraisemblance des *scénarios de risques*. On caractérise ensuite l'*écosystème numérique*, i.e. les *parties prenantes* du service (personnes physiques ou morales) et les *composants techniques* exposés. En fonction de leur niveau d'exposition, de l'intérêt qu'ils représentent pour l'attaquant et de leurs faiblesses, on retient les plus pertinents. Ainsi peut-on établir des *scénarios stratégiques*, alliant source de risque et écosystème numérique pour atteindre l'objectif visé, et leurs impacts. Puis, pour chaque scénario stratégique, reste à identifier les *scénarios opérationnels* pour connaître la cible, rentrer dans son environnement, trouver la cible puis l'exploiter. Les actions possibles à chacune de ces étapes (cf. Mitre Att&ck) ont une vraisemblance de succès, dépendant des mesures existantes. Finalement la vraisemblance du risque se détermine en fonction de l'enchaînement de ces actions unitaires. Enfin, les risques sont quantifiés et analysés, les options de traitement et les mesures à appliquer sur chaque action d'attaque identifiée déterminées (cf. Mitre D3fend). Un PACS (plan d'amélioration continue de la sécurité) est enfin convenu.



Le détail du fonctionnement de l'analyse de risques EBIOS RM est disponible sur le site de l'ANSSI.

Voici une synthèse des étapes :

Cadrage et socle de sécurité	Source de risques	Scénarios stratégiques	Scénarios opérationnels	Traitement du risque

• **Périmètres métier**
  • **Missions**
  • **Valeurs métier**
• **Périmètres techniques**
  • **Biens supports (BS)**
• **Evènements redoutés (ER)**
• **Gravité des ER**
• Quel est le **socle de sécurité** ?
• Pré requis :
  • Lister les missions de l'objet étudié (valeur ajoutée à l'entreprise)
  • Identifier et évaluer 5~10 valeurs métier (ce qu'une source de risques pourrait vouloir attaquer)
  • Identifier les biens support
	• **Sources de risques (SR)**
	• **Objectifs visés (OV)**
	• **Evaluation des SR/OV**
	• **Classement des SR/OV**
	• Chaque **couple SR/OV est-il vraiment pertinent** ? (selon la motivation, les ressources des attaquants considérés, l'activité objet de l'étude)
	• Pré requis :
	  • Identifier l'état de la menace : se référer aux bulletins de veille sur les cyber attaques et les actualités
		• **Parties prenantes critiques (PPC)**
		• **Niveau de menace de chaque PPC (1~4)**
		  • **Vulnérabilités structurelles**
		• **Scénarios stratégiques (SS)**
		  • **(SR/OV + ER)**
		• **Mesures de sécurité contre les vulnérabilités structurelles**
		• Pré requis :
		  • Missions et valeurs métier de l'objet étudié (At.1)
		  • Evènements redoutés (At.1)
		  • Sources de risques (At.2)
		  • Cartographie du SI et sa vue en écosystème (interaction avec les différentes parties prenantes)
			• **Biens supports critiques**
			• **Scénarios opérationnels (SO)**
			  • **Ex. : *Cyber kill chain***
			  • **(SR/OV + BS + cartographie du SI)**
			• **Vraisemblance des SO**
			• S'inspirer du modèle de *Cyber kill chain* (reconnaissance, armement, livraison, exploitation, installation d'une porte dérobée, C&C, actions sur la cible)
			• Pré requis :
			  • Missions et valeurs métier, biens supports (At.1)
			  • Socle de sécurité (At. 1)
			  • Sources de risques et objectifs visés retenus (At.2)
			  • Scénarios stratégiques retenus (At.3)
			  • Vues applications et infrastructure logiques de la cartographie du SI.
				• Quelle est la **stratégie de traitement** de chaque risque ?
				• Quels sont les **risques résiduels** ? Sont-ils **acceptables** ?
				• Quel est le **plan d'amélioration continue** ?
				• Quel est le **cadre de suivi des risques** ?
				• Pré requis :
				  • Socle de sécurité (At.1)
				  • Scénarios stratégiques (At. 3)
				  • Mesures de sécurité portant sur l'écosystème (At.3)
				  • Scénarios opérationnels (At.4)

Un peu plus détaillée :

Cadrage et socle de sécurité	Source de risques	Scénarios stratégiques	Scénarios opérationnels	Traitement du risque

• Quel sont les **périmètres métier et technique** de l'étude ?
• Quels sont les **évènements redoutés** associés et leur **niveau de gravité** ?
• Quel est le **socle de sécurité** ?
• Pré requis :
  • Lister les missions de l'objet étudié (valeur ajoutée à l'entreprise)
  • Identifier et évaluer 5~10 valeurs métier (ce qu'une source de risques pourrait vouloir attaquer)
  • Identifier les biens support
	• Quelles sont les **sources de risque** pour l'entreprise ?
	• Quels seraient les **objectifs visés** principaux ?
	• Chaque **couple SR/OV est-il vraiment pertinent** ? (selon la motivation, les ressources des attaquants considérés, l'activité objet de l'étude)
	• Pré requis :
	  • Identifier l'état de la menace : se référer aux bulletins de veille sur les cyber attaques et les actualités
		• Quelle est la **cartographie de la menace numérique** de l'écosystème et les **parties prenantes** critiques (PPC) ?
		• Quelles sont les **scénarios stratégiques** (réalistes de haut niveau) et les **évènements redoutés** ?
		• Quelles sont les **mesures de sécurité** retenues pour l'écosystème ?
		• Pré requis :
		  • Missions et valeurs métier de l'objet étudié (At.1)
		  • Evènements redoutés (At.1)
		  • Sources de risques (At.2)
		  • Cartographie du SI et sa vue en écosystème (interaction avec les différentes parties prenantes)
			• Quels sont les **biens support critiques** ?
			• Quels sont les **scénarios opérationnels** et leur **vraisemblance** ?
			• S'inspirer du modèle de *Cyber kill chain* (reconnaissance, armement, livraison, exploitation, installation d'une porte dérobée, C&C, actions sur la cible)
			• Pré requis :
			  • Missions et valeurs métier, biens supports (At.1)
			  • Socle de sécurité (At. 1)
			  • Sources de risques et objectifs visés retenus (At.2)
			  • Scénarios stratégiques retenus (At.3)
			  • Vues applications et infrastructure logiques de la cartographie du SI.
				• Quelle est la **stratégie de traitement** de chaque risque ?
				• Quels sont les **risques résiduels** ? Sont-ils **acceptables** ?
				• Quel est le **plan d'amélioration continue** ?
				• Quel est le **cadre de suivi des risques** ?
				• Pré requis :
				  • Socle de sécurité (At.1)
				  • Scénarios stratégiques (At. 3)
				  • Mesures de sécurité portant sur l'écosystème (At.3)
				  • Scénarios opérationnels (At.4)

Analyse des risques : d'autres méthodes

Marion

Méthode d'analyse informatique en organisation par niveaux, développée par le CLUSIF en 1983, puis régulièrement améliorée et adaptée. Elle a été abandonnée en 1998.

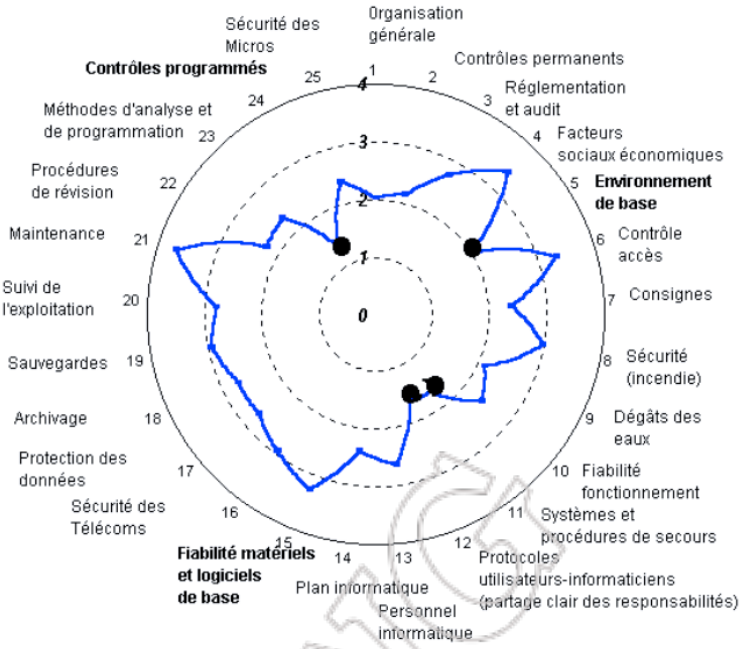
Principes :

- Le risque est mesuré par sa gravité : évaluation de ses conséquences / impacts et de sa potentialité (depuis 1993).
- 6 thèmes :
  - la sécurité organisationnelle

  - la sécurité physique
  - la continuité de service
  - l'organisation informatique
  - la sécurité logique et l'exploitation
  - la sécurité des applications
- 17 menaces :
  - Accidents physiques
  - Malveillance physique
  - Panne du SI
  - Carence de personnel
  - Carence de prestataire
  - Interruption de fonctionnement du réseau
  - Erreur de saisie
  - Erreur de transmission
  - Erreur d'exploitation
  - Erreur de conception / développement
  - Vice caché d'un progiciel
  - Détournement de fonds
  - Détournement de biens
  - Copie illicite de logiciels
  - Indiscrétion / détournement d'information
  - Sabotage immatériel
  - Attaque logique du réseau
- Phases :
  - Phase 1 - préparation : établissement des objectifs de sécurité et du périmètre de l'analyse. Découpage du périmètre en briques fonctionnelles.
  - Phase 2 : audit des vulnérabilités, grâce à un questionnaire contenant 27 facteurs de sécurité répartis sur un questionnaire de 600 questions ; pondération et synthèse sous forme de rosace
  - Phase 3 : analyse des risques et répartition en deux catégories : majeurs et simples. Pour l'analyse, pour chaque groupe fonctionnel (phase 1), chaque fonction est revue pour fixer les chemins d'attaque possibles avec leur impact et leur vraisemblance. Les groupes fonctionnels sont enfin classés en fonction de l'impact et la vraisemblance de leurs risques.
  - Phase 4 : définition du plan d'action pour atteindre une note globale correspondant aux objectifs de sécurité de l'entreprise. Le plan définit les mesures et les moyens pour les mettre en œuvre (coûts, délais). Il classe les mesures pour qu'elles puissent être mises en œuvre efficacement.

La méthode permet de produire des rosaces de risques, représentant le niveau de risques sur un ensemble de critères choisis parmi ceux du référentiel Marion :

Tableau 1
Rosace Marion et valeurs révélées par l'enquête du Secrétariat général de la Commission bancaire
(1991-1992)



Avantages :

- Possibilité de se comparer aux autres entreprises d'un même secteur d'activité au travers de la note acquise
- Existence de bases de connaissance mises à jour annuellement

MELISA

Méthode d'auto audit développée initialement par la DGA (Direction générale de l'Armement) et la DCN (Direction des constructions navales) en 1985, puis étendue.

La méthode a été rachetée par la société CF6 pour un usage interne (conseil). Au rachat de CF6 par Telindus ; la méthode a été abandonnée.

Principes :

- Le risque est mesuré au travers de l'analyse des vulnérabilités grâce à l'étude d'évènements, mini-scénarios imagés et détaillés (environ 600 par base de connaissance).
- La vulnérabilité est considérée comme la résultante de la gravité des conséquences de l'évènement (impact), le risque de non détection de l'évènement, sa facilité de réalisation et du "facteur d'exposition structurelle" (id. la vulnérabilité liée aux sujets).
- Pour chaque mini-scénario, le choix d'une parade permet d'évaluer la vulnérabilité résiduelle.

Avantages :

- Approche concrête

- Existence de bases de connaissance mises à jour annuellement, spécialisées par type de système et types de sensibilité (S : sensible, P : vitales, R : réseaux).

MEHARI

Méthode développée par le CLUSIF (Club de la Sécurité Informatique Français) en 1996 en partant des concepts de MARION et MELISA.

Elle est déclinée en plusieurs versions :

- La version standard pour la mise en œuvre d'un SMSI conforme ISO 27001 pour des organisations où les responsabilités opérationnelles peuvent être concentrées.
- La version expert pour tout type d'organismes
- La version pro pour les petites et moyennes entités
- La version manager pour rentrer rapidement dans le vif du sujet.

Principes :

- Le risque est mesuré au travers de l'étude de 6 facteurs de risques et 6 mesures de sécurité.
- La potentialité est considérée liée à 3 paramètres :
  - L'exposition naturelle (attrait, ciblage),
  - Le niveau de risque pour l'agresseur (risque d'être identifié et sanctionné),
  - Le niveau des moyens requis (intellectuels, matériels, temps)
- L'impact est considéré lié à 3 paramètres :
  - La circonscription des dommages (matériels, données),
  - Les capacités de reprise (opérations, flux financiers, communication),
  - La capacité de récupération financière.
- Les 6 mesures sont considérées comme ayant une influence sur un des facteurs :
  - Les mesures structurelles : localisation, architecture, organisation ;
  - Les mesures dissuasives : identification, journalisation, sanctions ;
  - Les mesures préventives : contrôle d'accès, détection, interception ;
  - Les mesures de prévention : détection, intervention, non propagation ;
  - Les mesures palliatives : restauration, reconfiguration, secours ;
  - Les mesures de récupération : assurances, actions en justice.
- La méthode introduit 16 familles de services, décomposés en sous-service, et une base de connaissance basée sur 12 familles de scénarios de 10 scénarios chacune en moyenne
- Depuis 1995, la méthode distingue plans stratégiques et opérationnels, ce qui revient en fait à distinguer :
  - Les mesures d'ordre global : mesures assurant la cohérence pour l'ensemble de l'entreprise ;
  - Les mesures d'ordre local : plans réalisés par chaque entité : ressources locales.
- Depuis 1996, une approche globale, basée sur la classification des ressources, l'analyse d'un nombre limité de scénarios et l'évaluation de l'effet global des mesures a été mise en œuvre.

Avantages :

- Application rapide

ERSI, CRAMM, OCTAVE

ERSI

La méthode ERSI a été conçue par le *Forum des Compétences* (https://www.forum-des-competences.org/nos-publications/).

La prise en compte du risque « Cyber » dans les modèles prudentiels

Ce groupe de réflexion du Forum des Compétences rassemble les responsables Sécurité et les responsables Risque Opérationnel des principaux acteurs du secteur financier, membres du Forum des Compétences, en partenariat avec le cabinet NOVAMINDS

Les objectifs de ce groupe sont les suivants :

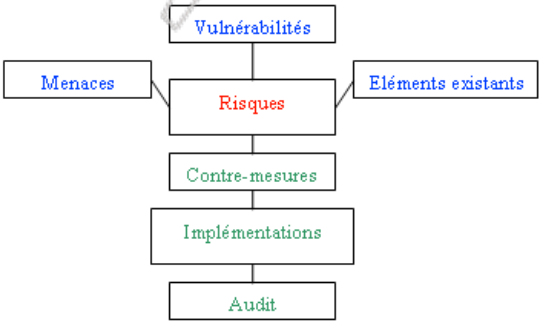
- Apporter un éclairage pédagogique sur le risque « Cyber » et les modèles prudentiels
- Partager sur les pratiques de place concernant la modélisation et le pilotage du risque « Cyber »
- Synthétiser les différentes pratiques illustrant la diversité des méthodologies possibles

Ce groupe de place aborde notamment les thèmes suivants :

- La définition, le périmètre, la taxonomie et la cartographie du risque « Cyber »
- Les organisations pour appréhender le risque « Cyber » dans les modèles prudentiels
- Les incidents internes et externes : un enjeu de qualité des données
- La prise en compte des dispositifs de maîtrise du risque dans la modélisation
- Les démarches de modélisation et modèles avancés
- Le processus d'évaluation de l'adéquation du capital interne

CRAMM

Méthode privée mise en place par Siemens en Angleterre en 1986.



étape 1 : l'identification et l'évaluation en termes de coût et d'impact en cas de compromission des éléments existants constituant le système d'information de l'entreprise (les équipements, les applications, les données…) ;
étape 2 : l'évaluation de la criticité des menaces et des vulnérabilités du système d'information ;
étape 3 : le choix de contre-mesures à mettre en place.

Octave

Octave (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) a été conçue par l'Université de Carnegie Mellon (à l'origine du 1er CERT).

OCTAVE est composée de 3 phases :

- Vision organisationnelle
  - Actifs
  - Menaces
  - Vulnérabilités organisationnelles
  - Exigences de sécurité
  - Règles existantes
- Vision technologique
  - Composants clefs
  - Vulnérabilités techniques
- Planification des mesures et réduction des risques
  - Evaluation des risques
  - Pondération des risques
  - Stratégie de protection
  - Plan de réduction des risques

Comparatif (source)

Méthode	Création	Popularité	Auteur	Soutenue par	Pays	Outils disponibles	Etat
EBIOS	1995	***	DCSSI	gouvernement	France	logiciel gratuit	
Melisa		**	DGA	armement	France		abandonnée
Marion	1980	**	CLUSIF	association	France		abandonnée
Mehari	1995	***	CLUSIF	association	France	logiciel Risicare	
Octave	1999	**	Université de Carnegie Mellon	universitaire	Etats-Unis	logiciel payant	
Cramm	1986	**	Siemens	gouvernement	Angleterre	logiciel payant	
SPRINT	1995	*	ISF	association	Angleterre	logiciel payant	
BS 7799		***		gouvernement	Angleterre		
SCORE	2004		Ageris Consulting	secteur privé	France	logiciel payant	
CALLIO	2001		CALLIO Technologies	secteur privé	Canada	logiciel payant	
COBRA	2001		C & A Systems Security Limited	secteur privé	Angleterre	logiciel payant	
ISAMM	2002		Evosec	secteur privé	Belgique		
RA2	2000		aexis	secteur privé	Allemagne	logiciel payant	