

"A goal without a method is nonsense."
Edwards Deming



Point sur les méthodes de sécurité

Jean François Mahé
Apicil

Pierre Yves Ducas
CGEY

Raphael Peuchot
Lamy Lexel

Samuel Janin
AQL

Eric Deronzier
Ysosecure



- 1 Objectifs d'une méthode de sécurité
- 2 Champ de l'étude
- 3 Présentation des méthodes de sécurité
- 4 Cas des méthodes de sécurité des développements
- 5 Liens entre les méthodes de sécurité et les normes
- 5 Présentation grille finale



① Objectifs d'une méthode de sécurité ?



Norme ou méthode

Norme ou méthode ?

Une **norme** peut être définie ainsi : C'est un document de référence basé sur un consensus couvrant un large intérêt industriel ou économique et établi par un processus volontaire.

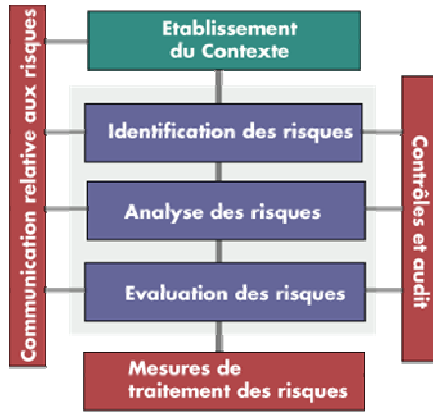
A la différence, **une méthode** est un moyen d'arriver efficacement à un résultat souhaité, précis. Mais une méthode n'intègre pas la notion de document de référence, ni la notion de consensus. Il ne faut donc pas opposer norme et méthode, mais plutôt les associer, une méthode sera « l'outil » utilisé pour satisfaire à une norme.

- L'intérêt d'utiliser une méthode de sécurité :
 - Approche globale et complète : étapes structurées et cohérentes
 - Uniformité : assurer une cohérence d'analyse
 - Rapidité / efficacité : optimiser les coûts
 - Éviter une approche trop technicienne
 - « neutraliser » la sensibilité du RSSI

- L'intérêt d'utiliser une méthode de sécurité diffusée :
 - Possibilité d'avoir un retour d'expérience par groupe utilisateur
 - Évolution méthode et outillage associé

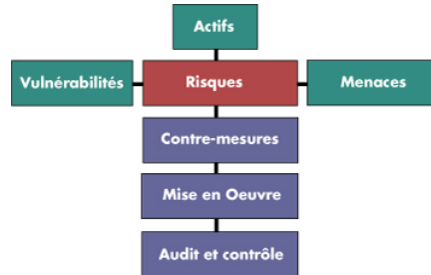
- Les risques de l'utilisation d'une méthode :
 - Lourdeur et durée d'exécution
 - MEO par des externes : pas de capitalisation en interne
 - Pas d'intelligence dans sa réalisation : résultats disproportionnés
 - Incompatible avec la typologie ou la culture d'entreprise

- La difficulté est d'avoir digéré la méthode
 - Pour comprendre les séquences clefs et le superflu
 - Pour savoir simplifier la démarche en liaison avec le contexte



Synthèse du processus de management du risque (ISO 13335-2)

Définition donnée dans la norme ISO 13335 -2 (appelée GMITS)



© Copyright Yseseure

② Champ de l'étude

- BDS Risk Assessor
- BDSS (Bayesian Decision Support System)
- Buddy System
- COBRA
- CRAMM (CCTA Risk Analysis and Management Method)
- EBIOS
- LAVA (Los Alamos Vulnerability Analysis)
- MARION
- MELISA
- OCTAVE
- RiskPAC
- RiskWatch
- Security By Analysis (SBA)
- SISSI
- XRM (eXpert Risk Management)

Il existe environ 200 méthodes de gestion des risques, dont plus de 80% sont mortes ou confidentielles

- Critères de sélection :
 - Diffusion
 - Adéquation à l'environnement PME - Midmarket
 - Capacité à l'utiliser en interne
 - Disponibilité en France/Europe
 - Pérennité
 - ...
- 6 méthodes retenues :
 - Marion Mehari Cobra Cobit Octave Ebios (Ulysse Cramm CMM)



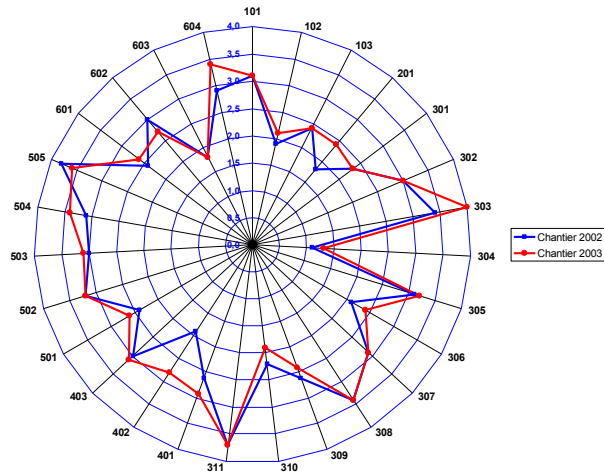
③ Présentation des méthodes de sécurité



La Méthode MARION

- MARION (Méthode d'Analyse des Risques Informatiques Orientée par Niveaux)
- Origine : CLUSIF et l'APSAD
- Date de création : 1984
- Objectif :
 - Elle permet d'évaluer le niveau de sécurité d'une entreprise au travers d'un questionnaire comportant 27 chapitres répartis en 6 grands thèmes
 - > Sécurité organisationnelle
 - > Sécurité physique
 - > Continuité
 - > Organisation informatique
 - > Sécurité logique et exploitation
 - > Sécurité des applications
- Société éditrice : CLUSIF
- Diffusion :
 - Le logiciel Sphynx manager et la base référentielle sont disponibles auprès de la société COGIS
 - La dernière mise à jour a été faite en 1998. Elle n'est actuellement plus maintenue.

Chantier MARION



13

La Méthode MARION

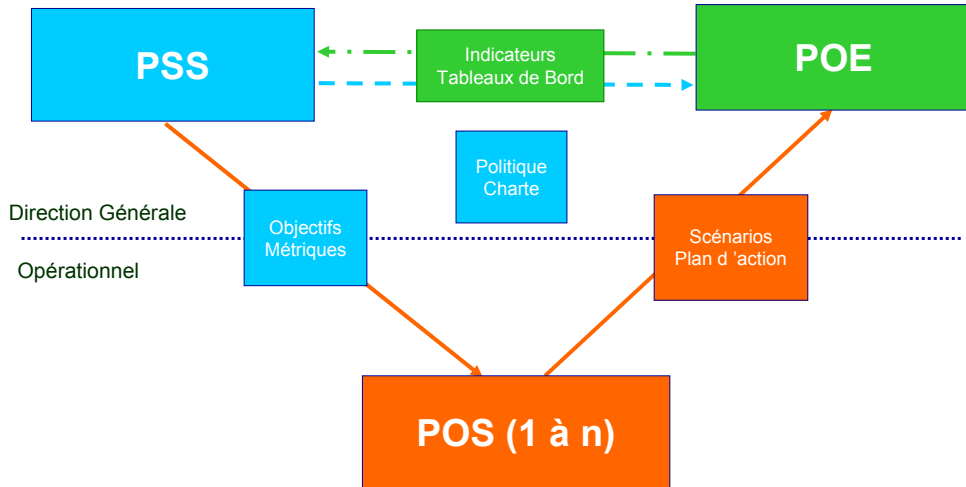
Critères	Description	Commentaires	Note	Explication
Couverture	Identification des actifs	matériels, logiciels, information, ..	-	
	Identification des menaces		-	
	Analyse des vulnérabilités	techniques et organisationnelles	+++	
	Evaluation des risques	qualitative/quantitative	-/-	
	Mesures de protection		-	
	Contrôle et audit	Etablissement contrôles et TDB	-	
Adaptabilité	Taille de l'entreprise	TPE/PME/Moyenne Entreprise	++	
	Typologie d'entreprise	centralisée/décentralisée	-	
	Ajout ou personnalisation de critères	législation nationale, réglementaire	+	
	Architecture du SI	couverture technologique	+	
Utilisation	Qualité documentaire, étude de cas		+	
	Modèle : formulaires, grilles		-/-	
	Questionnaires	disponibilité bases de connaissance	++	
	Disponibilité d'un logiciel et qualité		++	
	Ressources requises	en interne et ressources externes	++	
	Durée d'un cycle	initial, revue (mini, maxi)	-	
	Formation	Disponibilité	-/+ ++	
	Prix des licences	acquisition, formation, évolutions	++	
Langue	français / anglais	+		
Pérennité	Crédibilité organisme		++	
	Groupe utilisateur		-	
	Reconnaissance internationale		-	
Note globale				

14

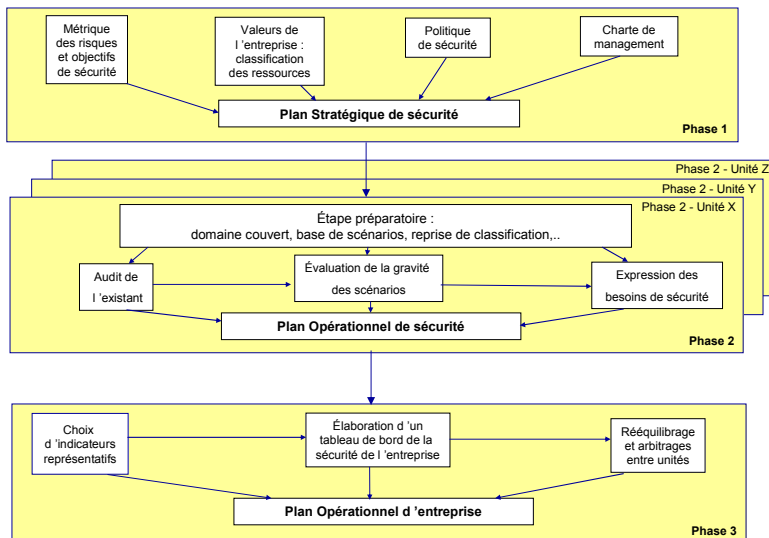
- Origine : La Méthode Harmonisée d'Analyse de Risques (MEHARI) a été élaborée par la Commission Méthodes du CLUSIF (Club de la Sécurité des Systèmes d'Information Français) à partir des méthodes MARION et MELISA.
- Date de création : 1992
- Objectifs : de proposer, au niveau d'une activité comme à celui d'une entreprise, un plan de sécurité qui se traduit par un ensemble cohérent de mesures permettant de pallier au mieux les failles constatées et d'atteindre le niveau de sécurité répondant aux exigences des objectifs fixés.
- Société éditrice : CLUSIF
- Diffusion : Le guide MEHARI comprend la description de la démarche, les techniques, la base de connaissances (menaces génériques, vulnérabilités spécifiques, classes de fonctionnalités et répertoires des fiches spécimen).
- Un logiciel RISICARE est disponible auprès de la société BUC S.A.

- Le modèle de risque MEHARI se base sur :
 - Six facteurs de risque indépendants : trois influant sur la potentialité du risque et trois influant sur son impact ;
 - Six types de mesures de sécurité, chacun agissant sur un des facteurs de risque (structurelle, dissuasive, préventive et de protection, palliative et de récupération).
- Les phases de MEHARI sont les suivantes :
 - Phase 1 : établissement d'un plan stratégique de sécurité (global)
 - Phase 2 : établissement de plans opérationnels de sécurité réalisés par les différentes unités de l'entreprise ;
 - Phase 3 : consolidation des plans opérationnels (global).

Synoptique de la démarche MEHARI



Conduite d'un projet MEHARI



Critères	Description	Commentaires	Note	Explication
Couverture	Identification des actifs	matériels, logiciels, information, ...	+++	
	Identification des menaces		+++	
	Analyse des vulnérabilités	techniques et organisationnelles	+++	
	Evaluation des risques	qualitative/quantitative	+ / ++	
	Mesures de protection		-	
	Contrôle et audit	Etablissement contrôles et TDB	-	
Adaptabilité	Taille de l'entreprise	TPE/PME/Moyenne Entreprise	++	
	Typologie d'entreprise	centralisée/décentralisée	++	
	Ajust ou personnalisation de critères	légalisation nationale, réglementaire	++	
	Architecture du SI	couverture technologique	+	
Utilisation	Qualité documentaire, étude de cas		+++	
	Modèle : formulaires, grilles		+ / ++	
	Questionnaires	disponibilité bases de connaissance	++	
	Disponibilité d'un logiciel et qualité		+++	
	Ressources requises	en interne et ressources externes	++	
	Durée d'un cycle	initial, revue (mini, maxi)	-	
	Formation	Disponibilité	- / ++	Uniquement pour personnel administration
Prix des licences	acquisition, formation, évolutions	+++		
	Langue	français / anglais	++	
Pérennité	Crédibilité organisme		+++	
	Groupe utilisateur		++	
	Reconnaissance internationale		+	

- Logiciel d'audit s'appuyant sur :
 - La norme ISO 17799
 - L'analyse du risque
- Éditeur : C&A Systems Security Ltd (UK)
- Langue : Anglais
- Maintenu en 2004 : Oui
- Coût : 1000 à 2000 US\$

- Logiciel d'audit s'appuyant sur
 - La norme ISO 17799
 - L'analyse du risque
 - Dans des environnements pré-configurés
 - Possibilité de créer ses propres questionnaires

- La norme ISO 17799
 - 200 questions sur les 10 sections de la norme
 - Édite un rapport avec les possibilités suivantes :
 - Introduction
 - Description du périmètre
 - Graphique des résultats
 - Résultats de l'audit (ISO COMPLIANCE REPORT)
 - Recommandations
 - Liste des questions et des réponses
 - Gère la dépendance des questions

■ L'analyse du risque

– 4 modes pré-configurés :

High Level Risk Assessment

IT Security Risk Assessment

– Possibilité de construire le périmètre par thème (parmi 21)

IT & Business Operational Risk Assessment

E-commerce Infrastructure Risk Assessment

Question Module: ASSETCLA - Asset Classification and Control (Sec 5)

Question 1 - Completion is REQUIRED. Please select only ONE response.

Are any inventories maintained of hardware, software and data assets?

No

Yes

Go to question 4

HELP TEXT

Sorry, there is no help text available for this question.

Question 2 - Completion is REQUIRED. Please select only ONE response.

Do assets have a nominated owner?

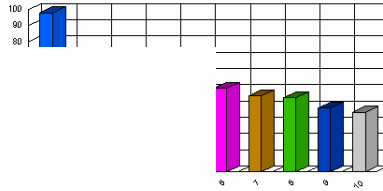
No

Yes

HELP TEXT

Sorry, there is no help text available for this question.

Assessment Of Non-Compliance (continued)



NAME OF POLICY : *1 Business Continuity Planning*
NON COMPLIANCE : 97.92 %
ASSESSMENT : OBJECTIVE

To counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

NAME OF POLICY : *2 Asset Classification and Control*
NON COMPLIANCE : 68.75 %
ASSESSMENT : OBJECTIVE

To maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

Improvements Required (continued)

Risk Category: Asset Classification and Control

NUMBER	TEXT
30	An inventory should be drawn up and maintained of the important assets associated with each information system. (5.1.1)
313	Electronic messages should contain a marker indicating the classification of the most sensitive data in the message. This will enable the recipient to afford the message the correct level of security. (5.2.2)
311	Screen displays containing sensitive data should indicate the classification of the data at the top of the screen. (5.2.2)
312	Magnetic media containing classified data should be labelled with the appropriate classification. This will enable media to be stored to the same level of security afforded to its computer counterpart. (5.2.2)
412	Procedures should be established for information labelling and handling, in accordance with the organization's classification scheme. (5.2.2)

- **ISO 17799** (bon produit pour les petites structures)
 - 200 questions sur le référentiel ISO 17799
 - Simple d'emploi
 - Rapport et graphique sur les 10 chapitres
 - Recommandations (avec rappel du chapitre de la norme)

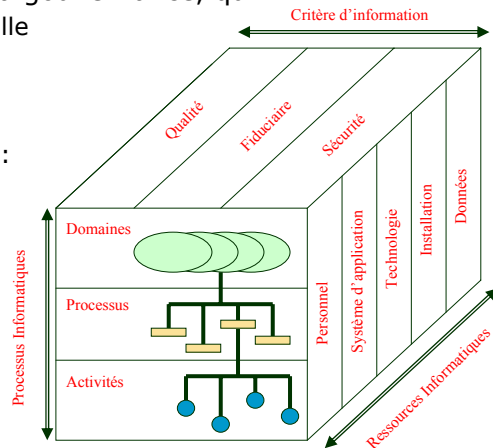
- **Risk Management** (Insuffisant)
 - Possibilité d'enrichir le questionnaire
 - Pas de notion de potentialité du risque
 - Pas de notion d'impact sur la marche de l'entreprise
 - Pas de notion de coût de prévention ou correction

Critères	Description	Commentaires	Note	Explication
Couverture	Identification des actifs	matériels, logiciels, information, ..	-	
	Identification des menaces		+	
	Analyse des vulnérabilités	techniques et organisationnelles	-	
	Evaluation des risques	qualitative/quantitative	-	
	Mesures de protection		-	
	Contrôle et audit	Etablissement contrôles et TDB	++	
Adaptabilité	Taille de l'entreprise	TPE/PME/Moyenne Entreprise	+++	
	Typologie d'entreprise	centralisée/décentralisée	-	
	Ajout ou personnalisation de critères	législation nationale, réglementaire	-	
	Architecture du SI	couverture technologique	-	
Utilisation	Qualité documentaire, étude de cas		+	
	Modèle : formulaires, grilles		+++	
	Questionnaires	disponibilité bases de connaissance	+++	
	Disponibilité d'un logiciel et qualité		+++	
	Ressources requises	en interne et ressources externes	++	
	Durée d'un cycle	initial, revue (mini, maxi)	+++	
	Formation	Disponibilité	-	
	Prix des licences	acquisition, formation, évolutions	+++	
Langue	français / anglais	++		
Pérennité	Crédibilité organisme		-	
	Groupe utilisateur		-	
	Reconnaissance internationale		-	

COBIT

■ Guide des bonnes pratiques de la gouvernance, qui :

- Établit une hiérarchie fonctionnelle
 - Domaines
 - Processus
 - Activités / Tâches
- Prend en compte Les impératifs :
 - De qualité
 - Fiduciaires
 - De sécurité
- Traite les ressources
 - Données
 - Systèmes d'application
 - Technologie
 - Installations
 - Personnel



- 4 grands domaines d'application des bonnes pratiques
 - Planification et organisation
 - Acquisition et mise en place
 - Distribution et support
 - Surveillance

- 7 éléments clés pour répondre aux impératifs (Qualité/Fiduciaire/Sécurité)
 - L'efficacité des processus
 - L'efficience de la mise à disposition de l'information
 - La confidentialité des données
 - L'intégrité des données
 - La disponibilité des données
 - La conformité aux lois et règlements
 - La fiabilité de l'information

- 34 fiches pratiques
 - Réparties sur les 4 grands domaines
 - Rappelant les éléments clés concernés
 - Rappelant les ressources concernées

		Efficacité	Efficience	Confidentialité	Intégrité	Disponibilité	Conformité	Fiabilité	Personnes	Applications	Technologie	Installations	Données
P01	Définir un plan informatique stratégique	P	S						x	x	x	x	x
P02	Définir l'architecture de l'information	P	S	S	S				x				x
...													
AMP01	Identifier les solutions	P	S							x	x	x	
...													
DS01	Définir les niveaux de service	P	P	S	S	S	S	S	x	x	x	x	x
...													
S1	Surveiller les processus	P	S	S	S	S	S	S	x	x	x	x	x
S2	Evaluer l'adéquation du contrôle interne	P	P	S	S	S	S	S	x	x	x	x	x
S3	Acquiescer une assurance indépendante	P	P	S	S	S	S	S	x	x	x	x	x
S4	Disposer d'un audit indépendant	P	P	S	S	S	S	S	x	x	x	x	x

- Rappel des éléments concernés
 - Grand chapitre parmi les 4
 - Planification et organisation, Acquisition et mise en place, Distribution et support, Surveillance
 - Points concernés parmi les 7
 - Efficacité, efficacité, confidentialité, intégrité, disponibilité, conformité, fiabilité
 - Ressources concernées parmi les 5
 - Personnes, Applications, Technologie, Installations, Données
- Définition des objectifs de contrôle
- Manière d'auditer
 - Acquérir la compréhension
 - Interroger : liste des personnes/fonctions
 - Obtenir : liste des informations, contrats, documentation, ...
 - Évaluer les contrôles (vérifier si :)
 - Vérifier la conformité (s'assurer que :)
 - Justifier le risque de ne pas atteindre les objectifs de contrôle
 - Effectuer (revues sur points précis, analyses comparatives, ...)
 - Identifier (performances, problèmes, faiblesses, ...)

- Traite de tout le fonctionnement de l'entreprise et pas seulement de la sécurité
- S'enrichit au fil des versions
- Est supervisé par l'AFAI
- N'a pas de support logiciel
- Laisse à l'auditeur le soin du scoring des informations

Critères	Description	Commentaires	Note	Explication
Couverture	Identification des actifs	matériels, logiciels, information, ...	+++	Indirectement
	Identification des menaces		+++	Indirectement
	Analyse des vulnérabilités	techniques et organisationnelles	+++	Indirectement
	Evaluation des risques	qualitative/quantitative	+ / ++	Indirectement
	Mesures de protection		-	
	Contrôle et audit	Etablissement contrôles et TDB	+++	
Adaptabilité	Taille de l'entreprise	TPE/PME/Moyenne Entreprise	+++	
	Typologie d'entreprise	centralisée/décentralisée	+++	
	Ajust ou personnalisation de critères	législation nationale, réglementaire	++	
	Architecture du SI	couverture technologique	+++	
Utilisation	Qualité documentaire, étude de cas			
	Modèle : formulaires, grilles			
	Questionnaires	disponibilité bases de connaissance		
	Disponibilité d'un logiciel et qualité			
	Ressources requises	en interne et ressources externes		
	Durée d'un cycle	initial, revue (mini, maxi)		
	Formation	Disponibilité		
Prix des licences	acquisition, formation, évolutions			
	Langue	français / anglais	+++	
Pérennité	Crédibilité organisme		+++	
	Groupe utilisateur		+++	
	Reconnaissance internationale		+++	

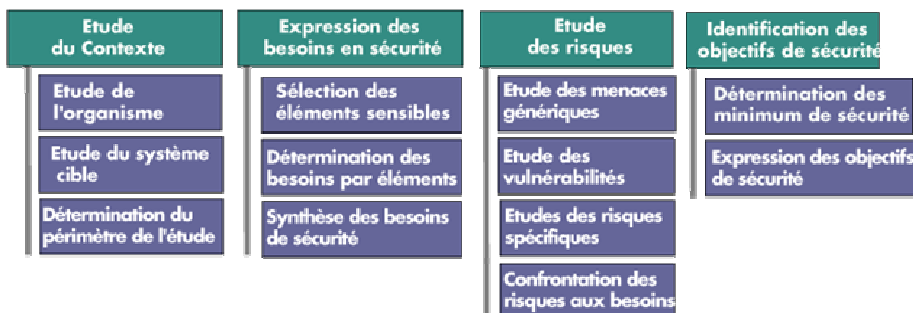


Ebios

- Origine : DCSSI
- Date de création : 1995
- Objectifs : EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est une méthode utilisée par l'Administration française depuis 1995.
- Société éditrice : DCSSI
- Diffusion : Le guide ÉBIOS comprend la description de la démarche, les techniques, la base de connaissances (menaces génériques, vulnérabilités spécifiques, classes de fonctionnalités et répertoires des fiches spécimen). Cette méthode n'utilise pas de questionnaire pour faire l'étude de la vulnérabilité.
- Un logiciel (licence GNU) est disponible auprès de la DCSSI

Synoptique de la démarche Ebios

Les 4 étapes de la méthode Ebios



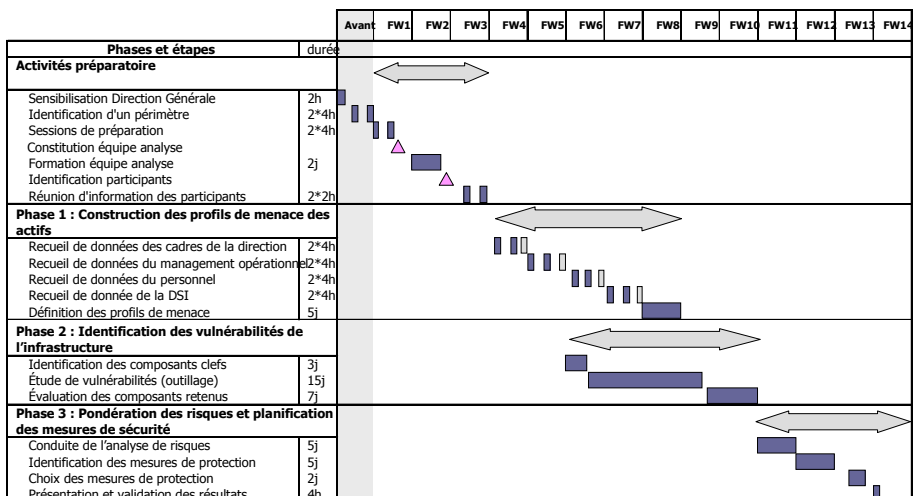
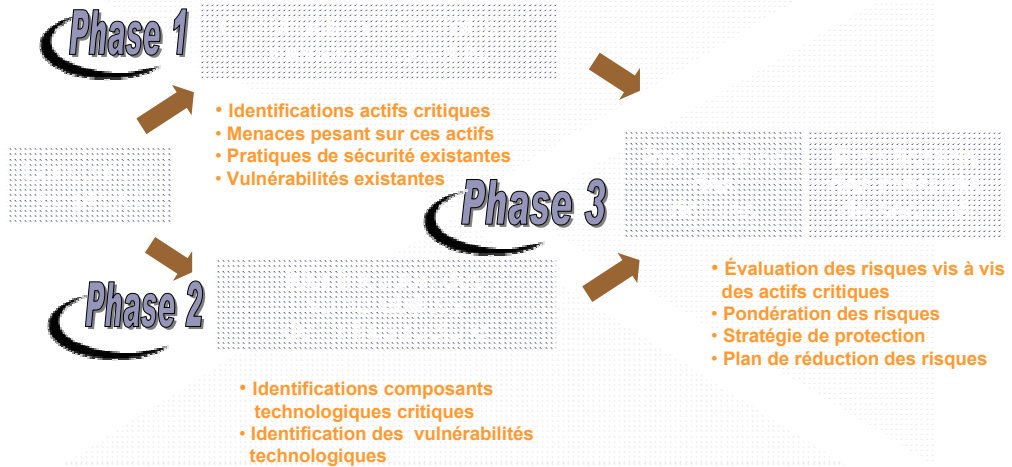
- Cette méthode est très orientée amont et elle n'intègre mal la partie évaluation des scénarios de risques, leur quantification, la définition de contrôles.

Critères	Description	Commentaires	Note	Explication
Couverture	Identification des actifs	matériels, logiciels, information, ...	+++	
	Identification des menaces		++	
	Analyse des vulnérabilités	techniques et organisationnelles	++	
	Evaluation des risques	qualitative/quantitative	+/-	
	Mesures de protection		-	
	Contrôle et audit	Etablissement contrôles et TDB	-	
Adaptabilité	Taille de l'entreprise	TPE/PME/Moyenne Entreprise	-	
	Typologie d'entreprise	centralisée/décentralisée	-	
	Ajout ou personnalisation de critères	législation nationale, réglementaire	++	
	Architecture du SI	couverture technologique	-	
Utilisation	Qualité documentaire, étude de cas		+++	
	Modèle : formulaires, grilles		+ / ++	
	Questionnaires	disponibilité bases de connaissance	-	
	Disponibilité d'un logiciel et qualité		+++	
	Ressources requises	en interne et ressources externes	++	
	Durée d'un cycle	initial, revue (mini, maxi)	-	
	Formation	Disponibilité	- / ++	Uniquement pour personnel administration
	Prix des licences	acquisition, formation, évolutions	+++	
Langue	français / anglais	++		
Pérennité	Crédibilité organisme		+++	
	Groupe utilisateur		++	
	Reconnaissance internationale		-	

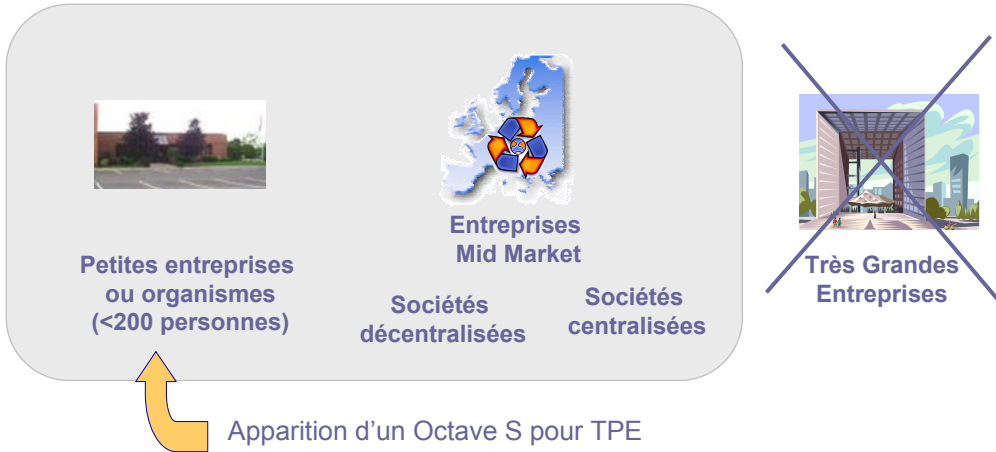
- Origine : Carnegie Mellon
- Date de création : 1990
- Objectifs : Autoévaluation (concepteurs se sont inspirés de Marion puis Mehari).
- Société éditrice : Carnegie Mellon
- Diffusion : Essentiellement Nord Amérique
- Pas de logiciel de support à la méthode, en revanche toute la documentation (doc, ppt ...) est en ligne sur le site de SEI

Principes	Qualités
Méthode auto-dirigée (menée en interne)	<ul style="list-style-type: none"> ■ Équipe interne d'analyse ■ Méthode structurée avec livrables ■ Permet une augmentation des compétences de l'équipe d'évaluation
Démarche adaptable	<ul style="list-style-type: none"> ■ Utilisation de catalogues de pratiques (int/ext) ■ Profils de menaces génériques ■ Intégration de catalogues de vulnérabilités
Focalisation sur les seuls éléments critiques	<ul style="list-style-type: none"> ■ Identification d'un périmètre d'évaluation ■ Activités ciblées sur ce périmètre
Analyse globales des risques	<ul style="list-style-type: none"> ■ Domaines organisationnels, technologiques et juridiques ■ Participation de compétences métier et technologiques

Les 3 phases principales



■ **Octave : Méthode de risk management adaptable à des contextes d'entreprise différents**



Critères	Description	Commentaires	Note	Explication	
Couverture	Identification des actifs	matériels, logiciels, information, ..	+++		
	Identification des menaces		++		
	Analyse des vulnérabilités	techniques et organisationnelles	++		
	Evaluation des risques	qualitative/quantitative	++		
	Mesures de protection		++		
	Contrôle et audit	Etablissement contrôles et TDB	-		
Adaptabilité	Taille de l'entreprise	TPE/PME/Moyenne Entreprise	+++		
	Typologie d'entreprise	centralisée/décentralisée	+++		
	Ajout ou personnalisation de critères	législation nationale, réglementaire	+		
	Architecture du SI	couverture technologique	-		
Utilisation	Qualité documentaire, étude de cas		+++	Méthode basée sur groupes de travail	
	Modèle : formulaires, grilles		+ / ++		
	Questionnaires	disponibilité bases de connaissance	-		
	Disponibilité d'un logiciel et qualité		-		
	Ressources requises	en interne et ressources externes	++		
	Durée d'un cycle	initial, revue (mini, maxi)	- / +		
	Formation	Disponibilité	- / -		Uniquement aux USA
	Prix des licences	acquisition, formation, évolutions	+++		Gratuit
Langue	français / anglais	-	Uniquement en Anglais		
Pérennité	Crédibilité organisme		+++	Réputation université	
	Groupe utilisateur		++		
	Reconnaissance internationale		+++		



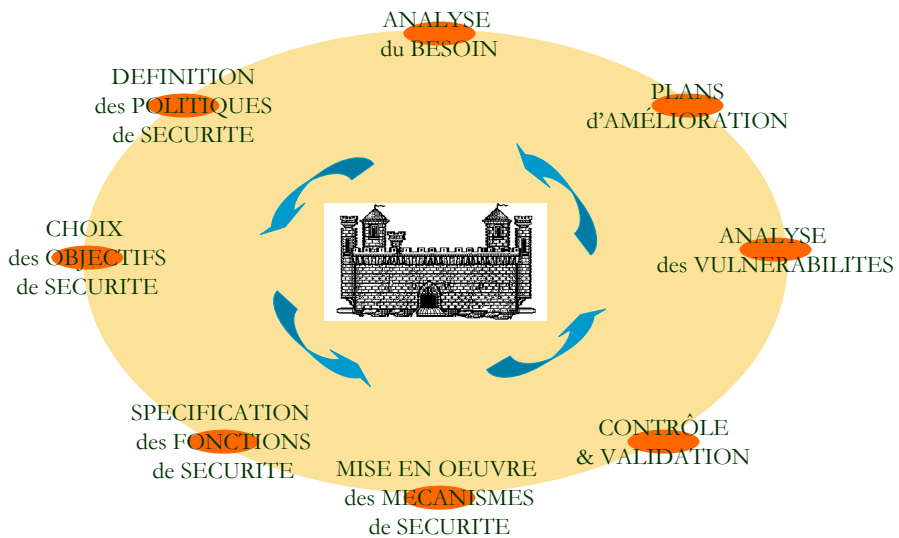
Les autres méthodes (Cramm, SEI CMM ... Ulysse)



Ulysse

-
- Origine : CCI Lyon
 - Objectifs : Sensibilisation petite PME/PMI
 - Pas une méthode de gestion des risques, mais un questionnaire de description du contexte, des vulnérabilités (2 onglets : humain/technique) et ensuite élaboration d'un plan d'action.
 - Orientée TPE, budget très limité, basée sur le know how des consultants qui sont intervenus.

④ Cas des méthodes de sécurité des développements



- Ne pas réinventer la roue
 - Les normes ITSEC et CC décrivent avec précision **TOUS** les concepts à prendre en compte dans la sécurité des développements
- Garder à l'esprit que la sécurité :
 - est une composante des caractéristiques **FONCTIONNELLES** du produit logiciel, s'intégrant dans son **ENVIRONNEMENT** d'utilisation
 - concerne à la fois le produit développé et le processus de développement (confidentialité et intégrité du **CODE**)
- Adapter la problématique sécurité aux méthodes de développement existantes et non l'inverse
 - Le savoir-faire et les pratiques des équipes de développement sont essentiels à notre problématique sécurité, il faut obtenir leur **ADHESION** et s'adapter à leurs méthodes
 - Le processus d'intégration de la sécurité dans les développements doit permettre de **CAPITALISER** sur le savoir-faire SSI

Environnement de développement

Sécurité des **développements**

Cycle de vie

Outils et **techniques**

Gestion de configuration

Correction d'anomalies

Produit ou système IT

Spécifications

Conception

Implémentation

Tests fonctionnels

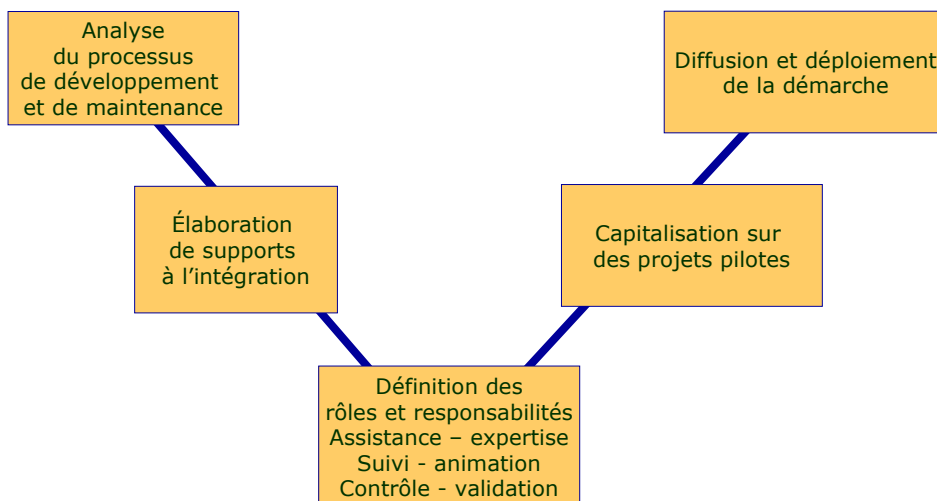
Environnement d'utilisation

Livraison

Installation, génération, démarrage

Guides, Utilisation/Administration

- Efficacité & assurance
 - mesure dans laquelle le système assure la sécurité dans le contexte de son exploitation réelle ou prévue
 - confiance qui peut être accordée à la sécurité fournie
- Les différentes analyses à réaliser
 - **Pertinence** : capacité du système dans son ensemble à offrir un niveau de sécurité conforme aux objectifs de sécurité en contrant réellement les menaces identifiées
 - **Cohésion** : capacité de chaque fonction et mécanisme de sécurité à ne pas réduire le niveau de sécurité mis en oeuvre par les autres fonctions ou mécanismes de sécurité
 - **Résistance** : capacité de chaque mécanisme de sécurité à résister à une attaque directe contre des défauts qui lui sont propres
 - **Facilité d'emploi** : s'assurer qu'il n'existe pas de cas d'utilisation du système de sécurité qui pourrait être non sûr alors que ses utilisateurs le croiraient sûr
 - **Vulnérabilités** : identifier les vulnérabilités résiduelles afin de prendre des mesures les rendant inexploitable



- www.ssi.gouv.fr

- ITSEC & CC :

- Définition complète des concept des sécurité dans les développement

- Catalogues d'exigences pour l'efficacité et l'assurance de sécurité

- Catalogue des PP :

- Recueils d'exigences complètes et cohérentes pour des produits ou systèmes types (Firewalls, IGC, etc.)

- Documentation générale :

- DSIS - modalités techniques et organisationnelles de la gestion d'une évaluation certifiée parallèle à un développement pour assurer une Vérification d'Aptitude à la SSI dans les recettes des marchés

- FEROS – Fiche d'expression rationnelle des objectifs de sécurité

- GARDE – Guides de rédaction pour l'évaluation de la sécurité des technologies de l'information



⑤ Liens entre les méthodes de sécurité et les normes

- ISO17799 ne précise aucune obligation quant à la méthode d'analyse de risques, chaque organisation ayant ses besoins et spécificités propres.
 - Il existe différentes méthodes reconnues dont le choix dépendra du contexte d'utilisation (application, type de résultat attendu, spécificité du domaine, compatibilité avec le référentiel de l'entité...).
- Les plus connues en France sont notamment MEHARI-CLUSIF, EBIOS-DCSSI.
 - Ces méthodes ont leurs propres référentiels qui ne couvrent pas toujours strictement le spectre de l'ISO17799.
 - Il peut ainsi être nécessaire de retravailler les bases de connaissances et prendre en compte certains aspects de l'ISO17799 pour obtenir une couverture complète de la sécurité par rapport à ce référentiel.

- L'analyse des risques de la méthode MEHARI permet de choisir des mesures de sécurité appropriées à l'entité.
- Ces mesures peuvent être issues de la base de connaissances MEHARI ou de l'ISO17799.
 - C'est la raison pour laquelle la Commission Méthodes du CLUSIF a corrélié la base de connaissances de la méthode afin de couvrir l'ensemble des mesures de la norme.
- Riscare propose de reformater les questions d'évaluation sous l'angle ISO 17799

- En ce qui concerne la méthode OCTAVE, développée par l'université de Carnegie Mellon :
 - une méthode d'identification des actifs
 - une démarche d'analyse des vulnérabilités
 - une méthode de pondération des risques

- L'analyse des risques de la méthode OCTAVE permet de choisir des mesures de sécurité issues de la base de connaissances OCTAVE ou définies à partir de l'ISO17799.



⑤ Grille finale

Critères	Description	Marton	Mehari	Octave	Ebios	Cramm	CMM	Cobit	Cobra
Couverture	Identification des actifs Identification des menaces Analyse des vulnérabilités Evaluation des risques Mesures de protection Contrôle et audit								
Adaptabilité	Taille de l'entreprise Typologie d'entreprise Ajout ou personnalisation de critères Architecture du SI								
Utilisation	Qualité documentaire, étude de cas Modèle : formulaires, grilles Questionnaires Disponibilité d'un logiciel et qualité Ressources requises Durée d'un cycle Formation Prix des licences Langue								
Pérennité	Crédibilité organisme Groupe utilisateur Reconnaissance internationale								

A définir suivant contexte entreprise