

# Synthèse de la norme d'audit OSSTMM

## Maquette de Démonstration d'Intrusion et de Piratage informatique

### MDIP

<b>Approbation Client</b>		<input type="checkbox"/> Accepté avec observations
		<input type="checkbox"/> Accepté sans observation
<b>NOM :</b>	<b>DATE :</b>	<b>VISA :</b>
<b>Synthèse des observations :</b>		

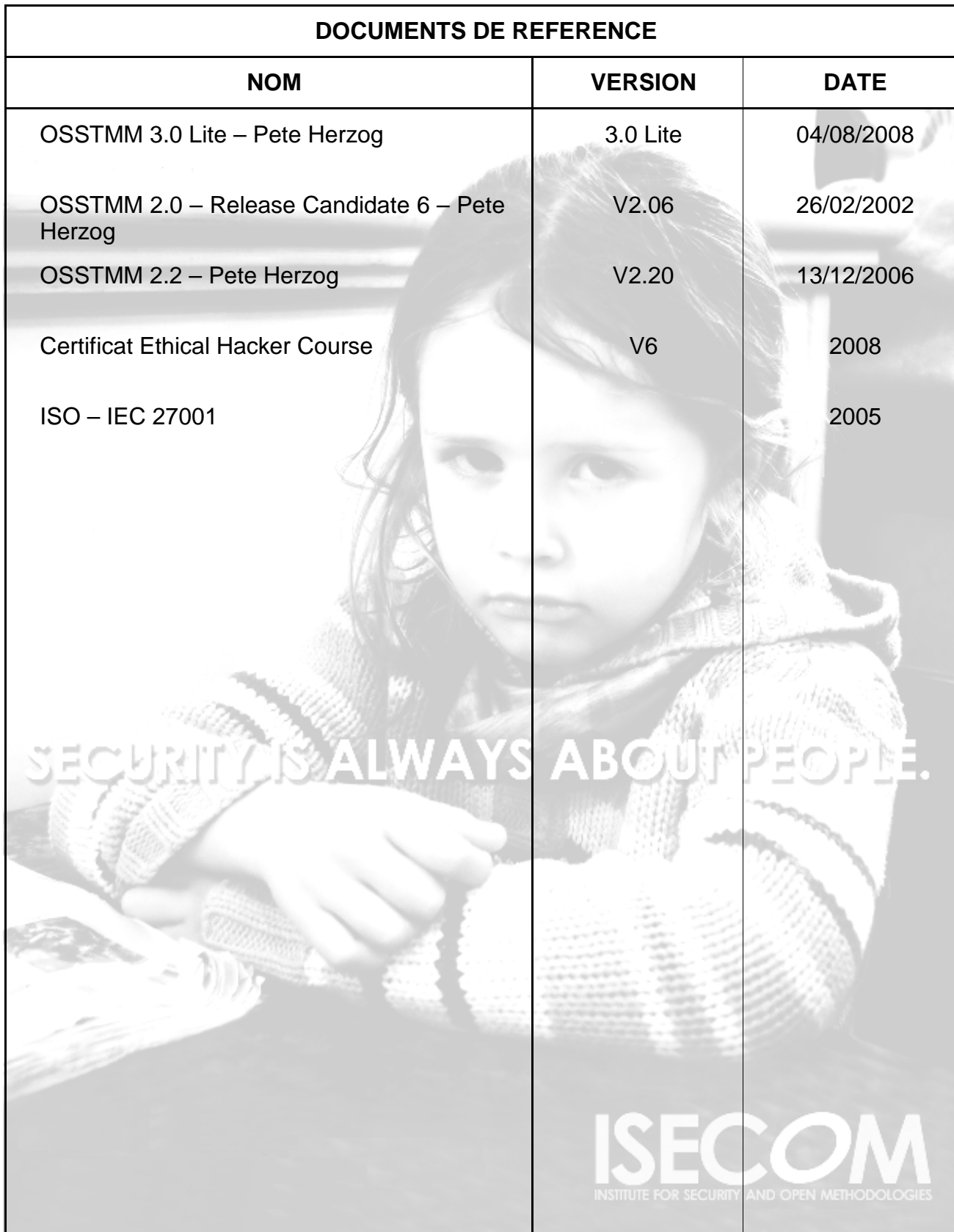
	Rédaction	Vérification	Approbation
Noms	B. Fantino		
Visas		P. Prestigiacomo	P. Prestigiacomo

**HISTORIQUE DES REVISIONS**

<b>VERSION</b>	<b>DATE</b>	<b>OBJET DE LA REVISION</b>
V1.0.1	13/01/2009	Création du document
V1.0.2	16/01/2009	Comparaison avec la version 2.2 de l'OSSTMM
V1.0.3	13/03/2009	Modifications « Axe méthodologique » et prise en compte réunion du 09 mars 2009

**DOCUMENTS DE REFERENCE**

<b>DOCUMENTS DE REFERENCE</b>		
<b>NOM</b>	<b>VERSION</b>	<b>DATE</b>
OSSTMM 3.0 Lite – Pete Herzog	3.0 Lite	04/08/2008
OSSTMM 2.0 – Release Candidate 6 – Pete Herzog	V2.06	26/02/2002
OSSTMM 2.2 – Pete Herzog	V2.20	13/12/2006
Certificat Ethical Hacker Course	V6	2008
ISO – IEC 27001		2005



SECURITY IS ALWAYS ABOUT PEOPLE.

**ISECOM**  
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

## Table des matières

1.	Introduction.....	6
1.1.	Historique .....	6
1.2.	Définitions et acronymes.....	6
1.3.	What is OSSTMM.....	6
1.4.	Concept OSSTMM.....	7
1.5.	Positionnement dans l'ISO 27001 .....	8
1.6.	A qui s'adresse cette méthodologie .....	8
2.	Conformité.....	9
2.1.	Lois.....	9
2.2.	Réglementation industrielle.....	9
2.3.	Politique de l'entreprise.....	9
3.	Type des tests OSSTMM .....	10
4.	Conduite de la méthodologie.....	11
4.1.	Security map.....	11
4.2.	Approche méthodologique par vecteur .....	12
4.2.1.	<i>The scope</i> .....	12
4.2.2.	<i>Vecteurs</i> .....	12
4.3.	Channels .....	12
4.3.1.	<i>COMSEC</i> .....	12
4.3.2.	<i>SPECSEC</i> .....	12
4.3.3.	<i>PHYSSEC</i> .....	13
4.4.	Les 4 phases .....	14
4.5.	Approche méthodologique par vecteur .....	13
4.6.	Les 17 modules en 4 phases .....	15
4.6.1.	<i>Schéma de principe de l'interaction des modules</i> .....	15
4.6.2.	<i>Descriptions des modules (en 4 phases A, B, C, D)</i> .....	16
4.7.	Liste des modules catégorisés en 6 sections de l'OSSTMM 2.2 .....	17
4.7.1.	<i>Internet Security</i> .....	17
4.7.2.	<i>Information Security</i> .....	17
4.7.3.	<i>Social Engineering</i> .....	18
4.7.4.	<i>Wireless Security</i> .....	18
4.7.5.	<i>Communications Security</i> .....	18
4.7.6.	<i>Physical Security</i> .....	18
4.8.	Conduite d'un test CEH .....	18
5.	Résultats OSSTMM.....	19
5.1.	Rapport STAR .....	19

	<i>Type</i>	<i>Entreprise</i>	<i>Rédacteur</i>	<i>Numéro</i>	<i>Version</i>
	REFERENCE	PRONETIS	B. Fantino	1	1.0.3
Projet MDIP					13/03/2009
5.2.	Résultats OSSTMM .....				19
5.3.	Validité et accréditation du rapport.....				19
5.4.	Evaluation du risque .....				20
5.4.1.	<i>Sécurité</i> .....				20
5.4.2.	<i>Respect de la vie privée</i> .....				20
5.4.3.	<i>Pratique</i> .....				20
5.4.4.	<i>Utilisable</i> .....				20
6.	RAV .....				20
6.1.	Définition.....				20
6.2.	Fonction du RAV.....				20
6.3.	Composition du RAV .....				21
6.3.1.	<i>OPSEC</i> .....				21
6.3.2.	<i>Contrôles</i> .....				21
6.3.3.	<i>Class A</i> .....				21
6.3.4.	<i>Class B</i> .....				21
6.3.5.	<i>Limitations</i> .....				21
6.3.6.	<i>Schéma des limitations</i> .....				22
7.	Conclusion de l'étude de la méthodologie OSSTMM .....				23
8.	Dictionnaire des termes anglais à connaître.....				<b>Erreur ! Signet non défini.</b>

# 1. Introduction

Ce document a pour but d'expliquer la norme d'audit OSSTMM v3.0 et de la comparer, lorsque c'est possible, avec la méthodologie extraite des cours de Certificat Ethical Hacker v6 (CEH v6) mais également tenter de la positionner par rapport à la norme ISO-IEC 27001 2005. La finalité est de pouvoir l'appliquer lors des tests d'intrusion et de vulnérabilité.



: lien avec le CEH



: lien avec l'ISO 27001

## 1.1. HISTORIQUE

L'OSSTMM a vu le jour en 2000 et elle est le fruit de la volonté de plusieurs auditeurs en sécurité informatique, rassemblés sous l'ISECOM, de s'appuyer sur un standard rigoureux et pragmatique permettant non seulement de structurer les audits de sécurité, mais également de leur apporter une métrique. Chaque étape est découpée en item focalisé sur les détails techniques.

## 1.2. DEFINITIONS ET ACRONYMES

**CEH** : Certificat Ethical Hacker : certificat attestant de la connaissance et de son utilisation « White Hat » des techniques des tests d'intrusion et plus généralement de piratage informatique

**ISO 27001** : Norme internationale de Système de Gestion de la Sécurité Informatique (ISMS) décrivant les exigences pour la mise en place d'un ISMS destiné à définir les systèmes de sécurité pour assurer l'amélioration continue de la sécurité des SI.

**OSSTMM** : Open Source Security Testing Methodology Manual

**ISECOM** : Institute for Security and Open Methodologies

**ISMS** : Information Security Management System

## 1.3. WHAT IS OSSTMM

Un audit OSSTMM permet une mesure précise de la sécurité à un niveau opérationnel donné. Il s'agit d'un manuel de méthodologie de test de sécurité libre de droit, régulièrement mis à jours grâce à des centaines d'auditeurs faisant retour de leur expérience dans le domaine. On peut la définir comme :

- un standard permettant la mesure précise de la sécurité à un niveau donné indépendamment des hypothèses et des données,
- une méthodologie assurant une réelle mesure de la sécurité, cohérente et reproductible
- une méthodologie entièrement indépendante des lois et d'une quelconque entreprise ou fournisseur,
- une méthodologie pouvant être librement utilisée, employée et diffusée

En outre, il est spécifié qu'un audit ne peut être qualifié d'audit OSSTMM que s'il respecte les critères suivants :

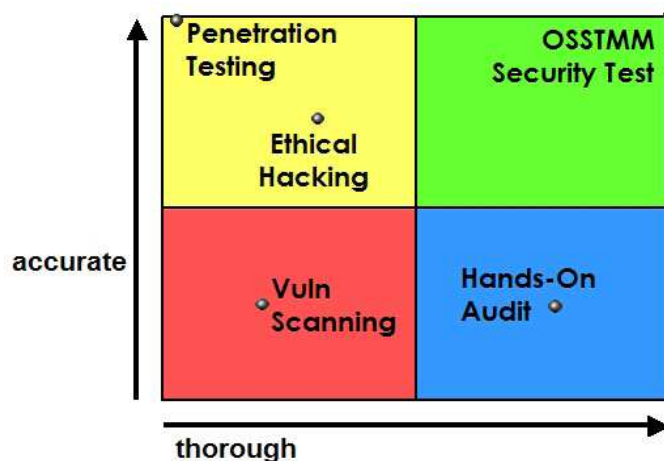
- les tests sont quantifiables
- ils sont cohérents et répétables
- leur validité est permanente
- l'analyse est basée sur le concept et non pas sur les données ou les matériels
- l'audit est approfondi
- conforme à la législation en vigueur et au respect de la vie privée

Ainsi, les éléments suivants doivent être préalablement définis et pris en compte afin de respecter la méthodologie :

1. Date et du test
2. Durée du test
3. Implication des auditeurs et des analystes
4. Type de test
5. Périmètre
6. Index (méthode d'énumération)
7. Vecteurs testés
8. Vérification des tests et des calculs des paramètres permettant d'assurer le niveau de protection, de la perte de contrôle, et les limites de sécurité
9. Tous les tests, qu'ils soient faits, ou pas, ou partiellement doivent être notifiés
10. Tous les résultats doivent être publiés
11. Les marges d'erreurs doivent être précisées
12. Identifier les processus qui influencent le périmètre de sécurité
13. Identifier les inconnues et les anomalies

#### 1.4. CONCEPT OSSTMM

Ce que propose en premier lieu l'OSSTMM, c'est une méthode scientifique pour spécifier précisément un audit de sécurité et les résultats obtenus aux tests afin de les exploiter en les corrélant et en pouvant les « rejouer ».



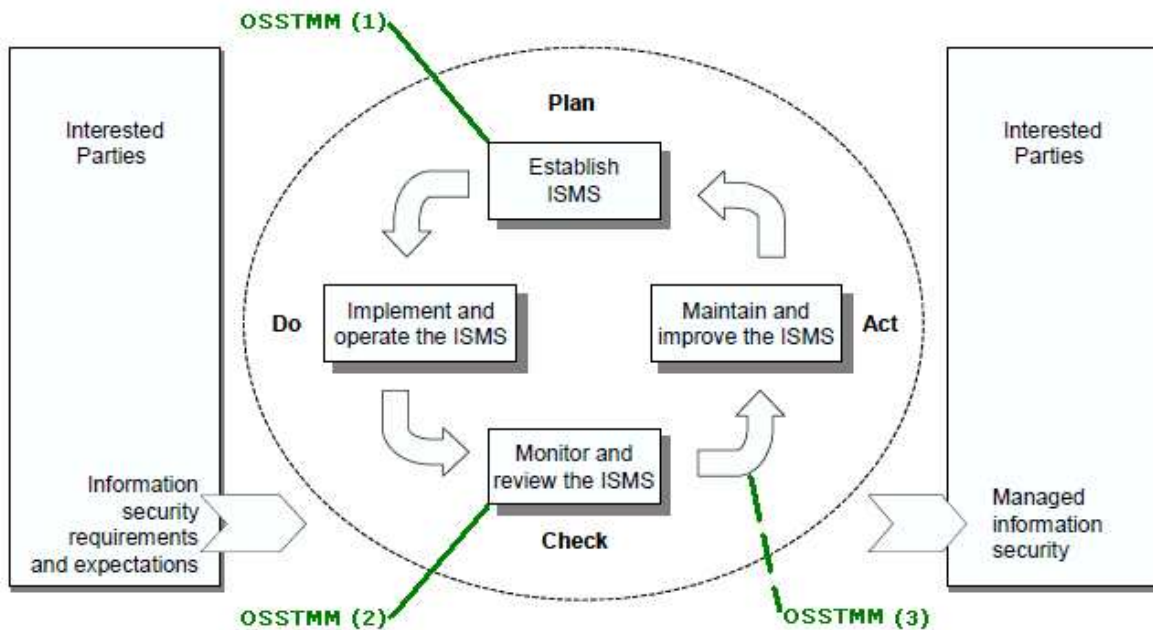
## 1.5. POSITIONNEMENT DANS L'ISO 27001



Exigence 4.2.1 : définition de la méthode d'analyse de risques (source : CLUSIR)

L'OSSTMM, en détail peut se positionner sur trois phases de SMSI proposé par la norme ISO 27001

- (1) au niveau « Plan », l'OSSTMM dans sa phase « Regulatory » plus particulièrement le module « Review »
- (2) an niveau « Monitoring », l'OSSTMM dans sa phase « Information Phase » et aussi entre la
- (3) elle peut s'insérer aussi entre la phase « Monitoring » et « Improving » grace aux éléments qu'il est nécessaire de corriger pour atteindre le niveau de sécurité voulu (les résultats permettent d'effectuer les recommandations)



Cependant, afin de permettre une bonne démarche PDCA, on peut placer l'OSSTMM en amont et ainsi utiliser les résultats en input du processus PDCA.

## 1.6. A QUI S'ADRESSE CETTE METHODOLOGIE

Elle est destinée aux spécialistes des tests d'intrusion mais aussi à l'ensemble des personnes souhaitant acquérir ou compléter leurs compétences en sécurité. Indéniablement elle peut être utile aux architectes SI ainsi qu'aux développeurs afin d'améliorer la mise en place et la création des protections.

## 2. Conformité

La conformité consiste à cadrer les audits dans le respect des règles, de la législation gouvernementale, industrielle et de la politique de l'entreprise de la cible concernée. L'OSSTMM distingue donc trois types de conformité :

### 2.1. LOIS

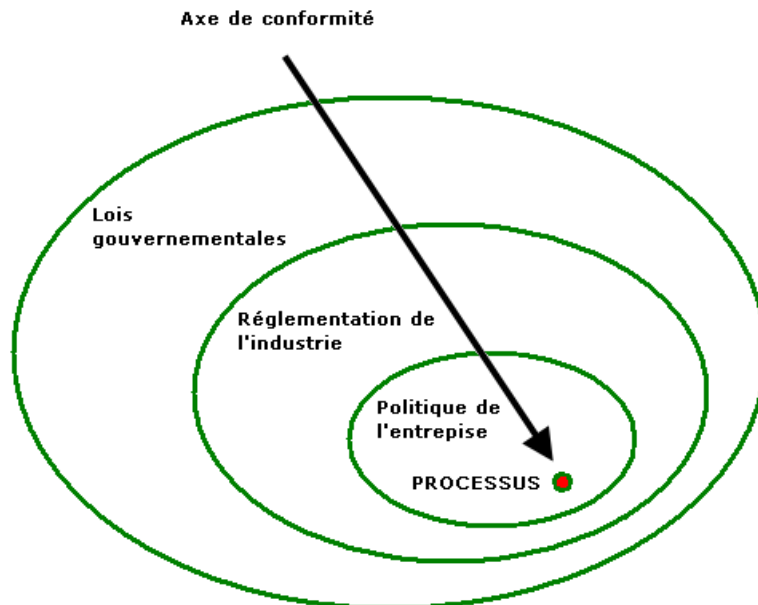
Consiste à se conformer avec les lois en vigueur dans l'état dans lequel l'audit est effectué.

### 2.2. REGLEMENTATION INDUSTRIELLE

Consiste à se conformer avec les lois en vigueur spécifique à l'industrie dans laquelle l'audit est effectué.

### 2.3. POLITIQUE DE L'ENTREPRISE

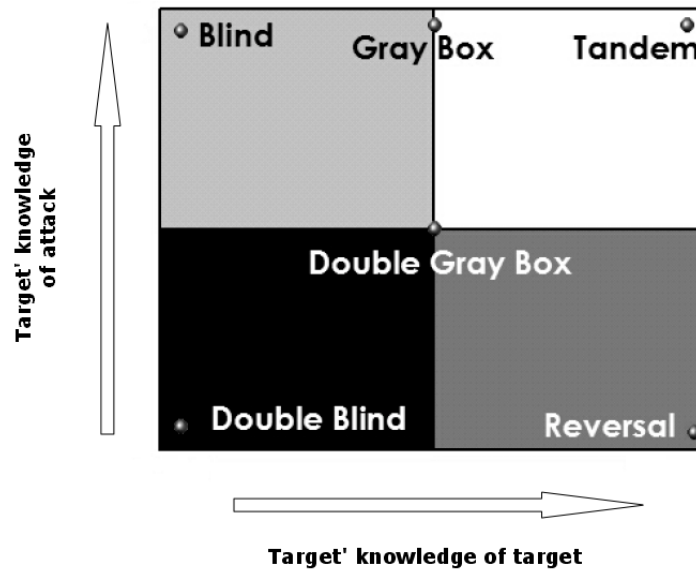
Consiste à se conformer avec les règlements mis en place dans la politique de l'entreprise dans laquelle l'audit est effectué.



Pour un test CEH, il est nécessaire également de se conformer aux lois en vigueur dans le pays où est conduit le test.

### 3. Type des tests OSSTMM

Ce sont les types « classiques »

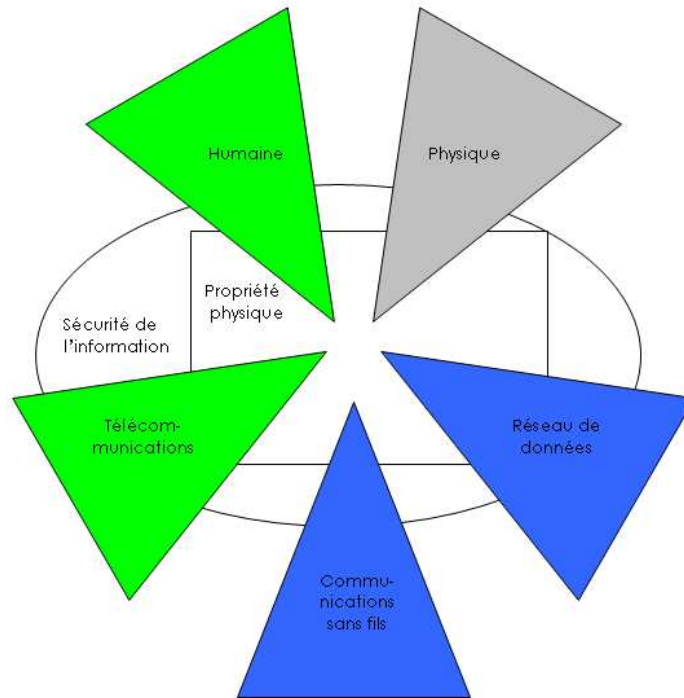


- **Blind** : les tests s'effectuent sans connaissance préalable des défenses, des systèmes et des vecteurs utilisés. La cible est préparée et connaît les détails de l'audit. Ce test est comparé au Ethical Hacking pour les channels COMSEC et SPECSEC et conduit comme un War Gaming ou Role Playing.
- **Double Blind** : les tests s'effectuent sans connaissance préalable des défenses, des systèmes et des vecteurs utilisés. La cible n'est pas informée de la teneur de l'audit. Ce test permet de mesurer les compétences de celui qui est soumis au test et sa capacité à faire face aux perturbations inattendues. Ce test est comparé au Black Box Audit ou Pénétration Test.
- **Grey Box** : les tests s'effectuent en ayant une connaissance limitée des défenses et des systèmes, mais complète des vecteurs utilisés. La cible est préparée pour l'audit et aux éventuelles perturbations. L'audit « Grey Box » est orienté sur l'efficacité de la cible à faire face. La profondeur du test dépend autant de la qualité de l'information transmise à l'auditeur que de ses connaissances techniques. Ce test est comparé à un test de vulnérabilité.
- **Double Grey Box** : similaire au test Grey Box. La cible connaît le périmètre et le planning des tests. Comparable au «White Box Audit »
- **Tandem** : permet de tester les protections et les contrôles mis en place sur la cible. La cible et l'auditeur connaissent tous les détails de l'audit et de la cible. Il ne permet pas de mesurer l'efficacité de la cible quant aux réactions face aux perturbations inattendues mais en revanche, teste la rigueur de l'exécution de tous les tests et des réponses associées. Appelé aussi « In House Test » ou « Crystal Box Audit » (l'auditeur est souvent « interne »)
- **Reversal** : l'auditeur a une connaissance parfaite des processus de sécurité et de la sécurité opérationnelle, mais la cible ne sait rien de la nature. Appelé aussi « Read Team Exercice ».

## 4. Conduite de la méthodologie

La méthodologie s'applique sur les éléments mais aussi sur leurs actions et interactions. Les tests dits « passifs » permettent d'enregistrer, de recouper et d'analyser tout ce qui est « traité » par la cible. Les tests dits « actifs » mesurent l'activité générée par l'audit.

### 4.1. SECURITY MAP

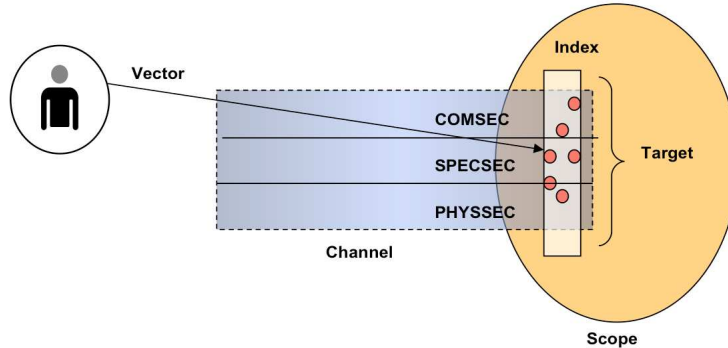


La carte de sécurité se compose de 5 domaines (abordés au paragraphe 4.3) :

- Personnel (COMSEC)
- Physique (COMSEC)
- Communications sans fils (SPECSEC)
- Réseaux de données (PHYSEC)
- Télécommunications (PHYSEC)

## 4.2. APPROCHE METHODOLOGIQUE PAR VECTEUR

### 4.2.1. THE SCOPE



L'audit du scope est défini par la combinaison du channel, du type de test, du vecteur et des index de la cible.



*Exigence 4.2.1 « Définition de l'ISMS » : chapitre délimitant la portée et les limites de l'ISMS (politique, business, objectif)*

### 4.2.2. VECTEURS

Un vecteur (une perspective) se définit par une quantité de « direction » ; par exemple, si l'auditeur teste la sécurité physique d'une porte, il y aura au moins deux vecteurs : de l'intérieur vers l'extérieur et de l'extérieur vers l'intérieur.

## 4.3. CHANNELS

Les 3 vecteurs se composent de 5 domaines.

### 4.3.1. COMSEC

Composante Humaine : toutes les interactions humaines, physiques ou psychologique

Composante Physique : toutes les interactions « non électroniques par nature », (accès physique, contrôle d'identité, alimentation de secours, sécurité incendie...)



*Dans le CEH, thème abordé par le « Social Engineering » pour la composante humaine*

### 4.3.2. SPECSEC

Communications sans fils : cet item concerne toutes les communications sans fils, transmission de signaux, ondes et les ondes électromagnétiques (ELSEC : communication électronique, SIGSEC : signaux, EMSEC : propagation des câbles)

### 4.3.3. PHYSSEC

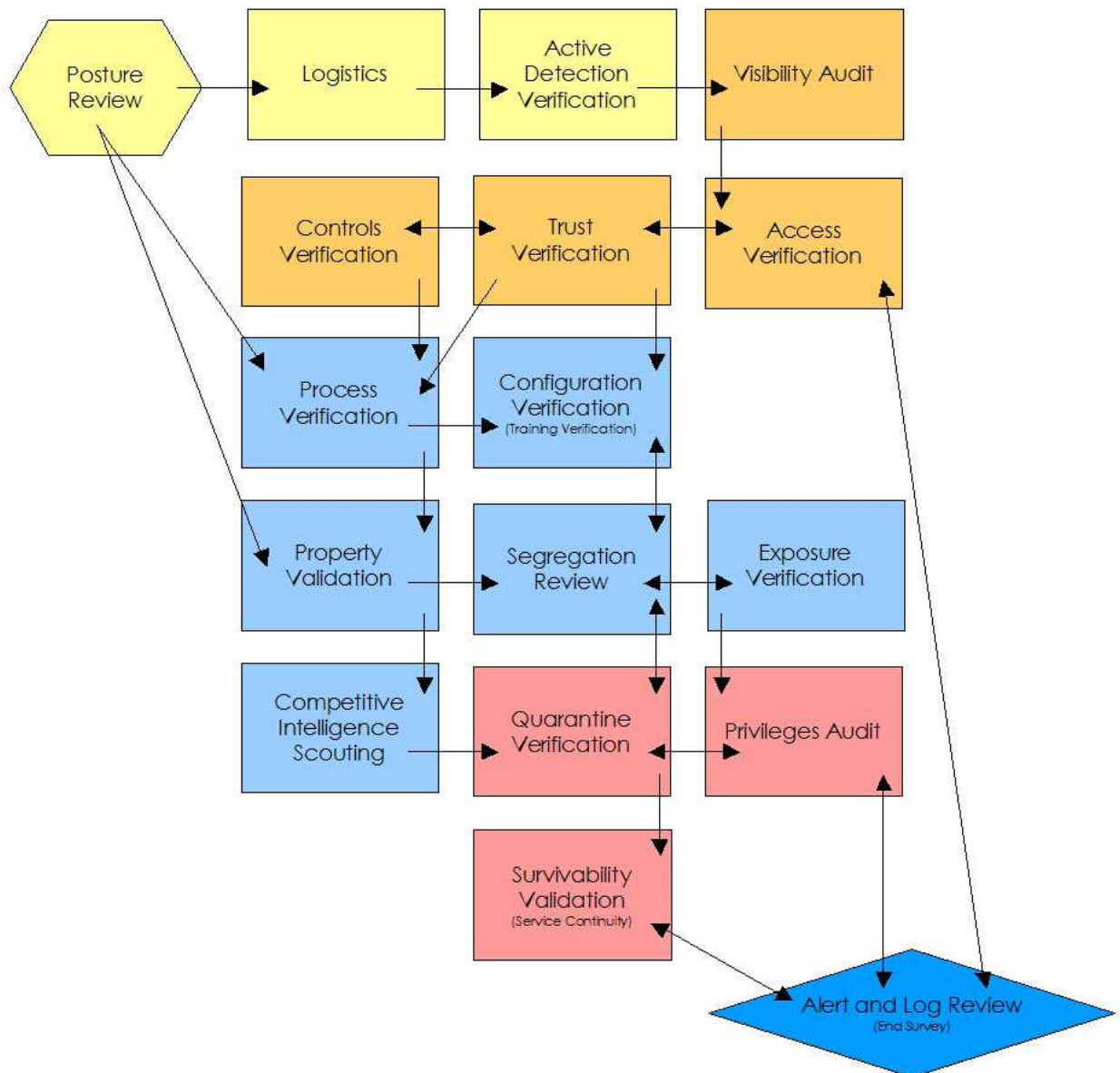
Réseaux de données : concerne tous les systèmes électroniques, analogiques ou numériques, utilisés sur des réseaux

Télécommunications : comprend les réseaux de télécommunications, analogiques ou numériques, utilisant le téléphone ou les lignes téléphoniques

Cette classification en vecteurs et domaines peut être réorganisée mais elle permet cependant une approche orientée « communication » et « interaction ».

### 4.4. APPROCHE METHODOLOGIQUE PAR VECTEUR

La méthodologie s'applique de la façon suivante : une étendue (environnement) d'étude comprend 3 channels applicables à 5 domaines testés selon 17 modules, eux-mêmes sous catégorisés en 5 sections :



#### 4.5. LES 4 PHASES

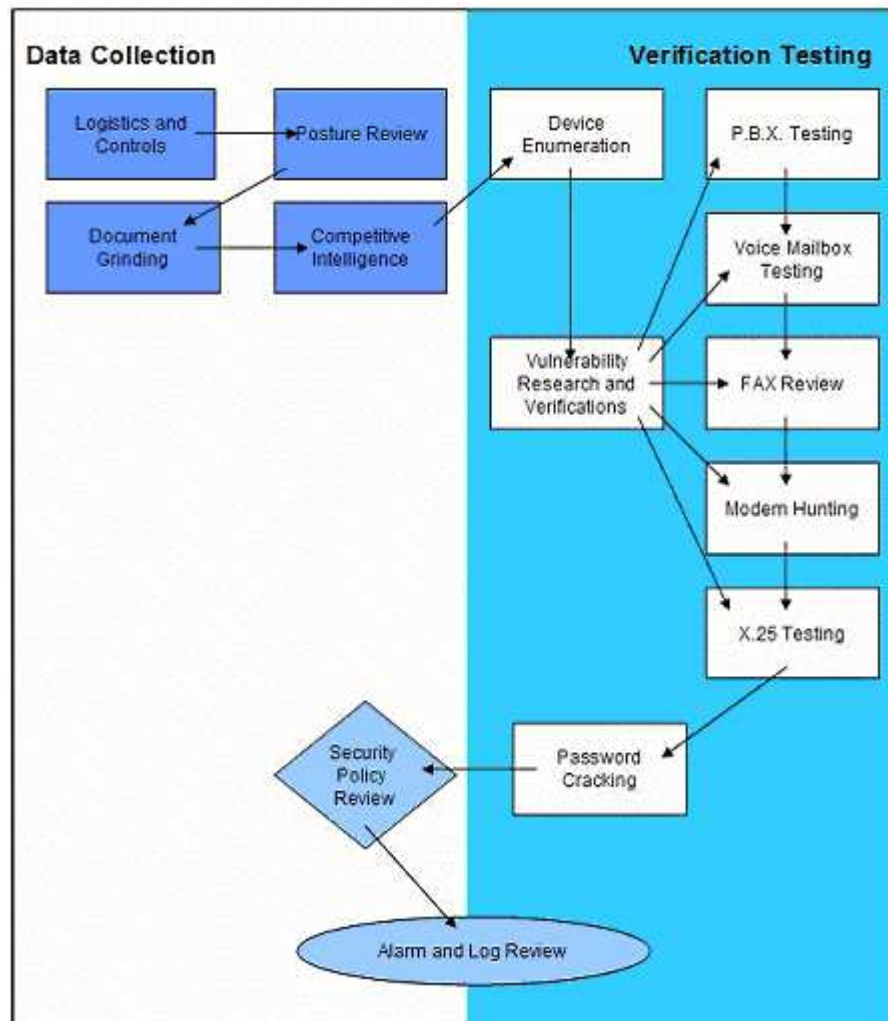
- Regulatory Phase (A)
- Definitions Phase (B)
- Information Phase (C)
- Interactive Controls Test Phase (D)

#### 4.6. ILLUSTRATION DE L'APPROCHE PAR VECTEUR

Afin d'illustrer la méthode par vecteur, le schéma ci-dessous représente son application à « Physec » Partie « Communications » selon un scope défini. La colonne de gauche comprend les phases « Regulatory Phase (A) », Definitions Phase (B) et Information Phase (C) et la colonne de droite « Interactive Controls Test Phase (D) ». Ce développement porte sur :

- PBX
- Voice Mailbox
- FAX
- Modem
- X 25

On note toute fois que ce schéma est issu de l'OSSTMM 2.2 (énuméré au paragraphe 4.7.5)



## 4.7. LES 17 MODULES EN 4 PHASES

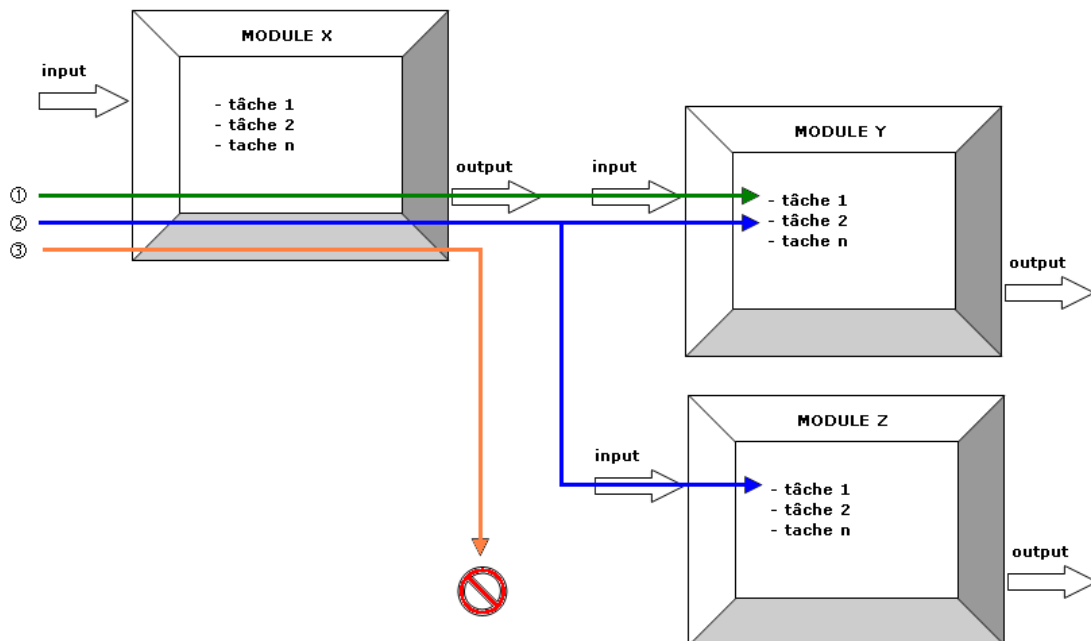
L'audit OSSTMM commence par une revue globale de la cible, en incluant, la politique, la culture d'entreprise, les normes, les lois et règlements qui conditionnent la cible. L'audit se termine par la comparaison avec les résultats obtenus quant aux alarmes, alertes, rapports et journaux générés. Il s'agit d'un concept circulaire où la première étape consiste à renseigner les exigences opérationnelles pour interagir avec la cible et où la dernière étape est une revue des renseignements obtenus grâce à l'audit.

*You know what you need to do, you do it and you check what you've done.*

L'organisation des tâches s'effectue en : Channel  $\Rightarrow$  Module  $\Rightarrow$  Tâche

La « Task » est décrite dans le module pour chaque channel d'audit abordé. Certains audits technologiques peuvent chevaucher les limites de deux ou plusieurs channels (par ex un réseau WiFi doit être testé par COMSEC – réseau de données – et SPECSEC – communication sans fils – ), c'est pourquoi la définition précise du périmètre des tests est importante. La méthodologie permet une approche d'audit de « l'extérieur vers le noyau » que les channels soient clairement définis et distincts ou qu'ils se chevauchent et soient multiples. Par conséquent il est indispensable qu'un auditeur anticipe le besoin de définir un audit avec des channels multiples. Parfois, ce n'est seulement que lors de l'audit qu'il devient évident que plusieurs « cibles » soient sous le même channel ou qu'une seule soit couverte par plusieurs channels.

### 4.7.1. SCHEMA DE PRINCIPE DE L'INTERACTION DES MODULES



- ① – L'output d'un module peut être l'input d'un autre
- ② – L'output d'un module peut être l'input de deux autres
- ③ – a) le module peut ne pas avoir d'input  
b) le module peut être ignoré (mais documenté)

c) si un module n'a pas de sortie, cela ne signifie pas forcément un test sans intérêt mais peut indiquer un niveau de sécurité supérieur (ou aussi : channel obstrué, module mal implémenté, tâches non applicables, résultat mal interprété)

#### 4.7.2. DESCRIPTIONS DES MODULES (EN 4 PHASES A, B, C, D)

- **A – Posture Review**  
*Description* : revue des règles, lois, règlements...  
*But* : situer précisément le scope
- **A – Logistics**  
*Description* : mesure des contraintes et des marges d'erreur (cadre, qualité du réseau, temps, planification)  
*But* : déterminer les limites de l'audit et améliorer les résultats
- **A – Active Detection Verification**  
*Description* : détermine les contrôles actifs et passifs  
*But* : connaître les possibles restrictions (filtrage : pare feu, IDS..)
- **B – Visibility Audit**  
*Description* : énumère tous les index auxquels l'audit s'applique  
*But* : limiter la portée de l'audit aux seuls résultats attendus
- **B – Access Verification**  
*Description* : liste les points d'accès et les authentifications requises  
*But* : connaître les possibles « points d'entrer »
- **B – Trust Verification**  
*Description* : énumère les relations d'approbations  
*But* : identifier les accès qui ne requièrent pas d'authentification
- **B – Controls Verification**  
*Description* : vérifie les critères ACID  
*But* : mesurer les process permettant les critères ACID
- **C – Process Verification**  
*Description* : mesure les règles et les procédures assurant la sécurité  
*But* : identifier les contrôles et les procédures et s'assurer que leur fonctionnement et efficacité correspondent au niveau de sécurité
- **C – Configuration Verification**  
*Description* : recherche les configurations nécessaires et attendues en deçà desquelles il y a « dysfonctionnement »  
*But* : explorer les configurations requises
- **C – Property Validation**  
*Description* : examine les informations et données définies dans le scope  
*But* : assurer la conformité des données avec les règles légales et éthiques
- **C – Segregation Review**  
*Description* : détermine les données d'entreprise et privées  
*But* : test la séparation entre les deux catégories.
- **C – Exposure Verification**  
*Description* : détermine la visibilité indirecte du scope de l'extérieur

	<i>Type</i>	<i>Entreprise</i>	<i>Rédacteur</i>	<i>Numéro</i>	<i>Version</i>
	REFERENCE	PRONETIS	B. Fantino	1	1.0.3
Projet MDIP					13/03/2009

*But* : test de découverte des informations permettant de compromettre la cible (accès)

○ **C – Competitive Intelligence Scouting**

*Description* : détermine la visibilité du scope de l'extérieur

*But* : test de découverte des informations pouvant nuire à l'entreprise en termes de concurrence (business intelligence).

○ **D – Quarantine Verification**

*Description* : mesure l'efficacité des réactions aux attaques

*But* : test le bon fonctionnement du comportement de la « quarantaine »

○ **D – Privileges Audit**

*Description* : étudier la liste des accès et des droits inhérents ainsi que leurs impacts

*But* : teste l'efficacité de la gestion des autorisations, privilèges et limites des droits

○ **D – Survivability Validation**

*Description* : mesure l'efficacité de la continuité et de la résistance des contrôles

*But* : teste les limites des contrôles

○ **D – Alert end Log Review**

*Description* : revue des écarts entre les tests effectués et l'activité réellement générée lors de l'audit

*But* : identifier les parties de l'audit qui sont exploitables et fiables

#### 4.8. LISTE DES MODULES CATEGORISES EN 6 SECTIONS DE L'OSSTMM 2.2

Il est intéressant de comparer l'approche modulaire de la version 2, regroupant les éléments technique à tester, et ceux de la version 3, plus conceptuels ou « abstraits ».

##### 4.8.1. INTERNET SECURITY

- Network Surveying
- Port Scanning
- System Identification
- Services Identification
- Vulnerability Research and Verification
- Internet Application Testing
- Router Testing
- Firewall Testing
- Intrusion Detection System Testing
- Trusted Systems Testing
- Password Cracking
- Denial of Service Testing
- Containment Measures Testing

##### 4.8.2. INFORMATION SECURITY

- Document Grinding
- Competitive Intelligence Scouting

	<b>Type</b>	<b>Entreprise</b>	<b>Rédacteur</b>	<b>Numéro</b>	<b>Version</b>
Projet MDIP	REFERENCE	PRONETIS	B. Fantino	1	1.0.3
					13/03/2009

- Privacy Review

#### **4.8.3. SOCIAL ENGINEERING**

- Request Testing
- Guided Suggestion Testing
- Trust Testing

#### **4.8.4. WIRELESS SECURITY**

- Wireless Networks Testing
- Cordless Communications Testing
- Privacy Review
- Infrared Systems Testing

#### **4.8.5. COMMUNICATIONS SECURITY**

- PBX Testing
- Voicemail Testing
- FAX review
- Modem Testing

#### **4.8.6. PHYSICAL SECURITY**

- Access Controls Testing
- Perimeter Review
- Monitoring Review
- Alarm Response Testing
- Location Review
- Environment Review

### **4.9. CONDUITE D'UN TEST CEH**

La conduite d'un tes CEH s'effectue en 6 étapes :

1. Présenter au client (cible) les pré-requis nécessaires
2. Rédiger le NDA (Non Disclosure Agreement) et le faire signer aux clients
3. Préparer une équipe et planifier l'Ethical Hacking
4. Conduire le test et analyser les résultats obtenus
5. Rédiger un rapport
6. Rendre les conclusions

Toutes les évaluations de sécurité nécessitent 3 étapes :

#### **A – La préparation : l'équivalent de « Posture Review » de l'OSSTMM**

Un accord est signé entre l'auditeur et l'audité, incluant non seulement le NDA mais également des clauses empêchant l'audité de poursuivre l'auditeur sur des événements dus aux faits de l'audit. Ce contrat définit aussi le périmètre de l'audit, l'activité évaluée, le planning et les ressources concernées.

#### **B – Le test :**

<i>Type</i>	<i>Entreprise</i>	<i>Rédacteur</i>	<i>Numéro</i>	<i>Version</i>
REFERENCE	PRONETIS	B. Fantino	1	1.0.3
Projet MDIP				13/03/2009

Rédaction du rapport technique d'évaluation basé sur les potentielles vulnérabilités trouvées.

### C – La conclusion

Les résultats de l'évaluation sont transmis à l'organisation et les actions correctives sont prises si nécessaire.

## **5. Résultats OSSTMM**

### **5.1. *RAPPORT STAR***

Afin de mesurer au mieux la politique de sécurité ainsi que les protections en place, l'utilisation de cette méthodologie devrait se conclure avec un rapport STAR. STAR a pour vocation de fournir une référence de sécurité qui pourra aussi être utilisée pour les tests suivants. L'ISECOM spécifie que ce rapport est contractuel (voir 5.3 « Validité et accréditation »). Ce rapport nécessite les informations définies dans le paragraphe 1.3 « What is OSSTMM » (Eléments suivants doivent être préalablement définis et pris en compte afin de respecter la méthodologie)

### **5.2. *LE CLICHE PRODUIT GRACE A L'OSSTMM***

Les résultats des tests sont souvent accompagnés de solutions recommandées sans que cela ne soit ni une obligation ni inclus dans la méthodologie.

La méthodologie doit être axée sur l'état actuel de sécurité, ce qui signifie à un instant donné avec des process donnés.

Un rapport d'audit OSSTMM montre le niveau réel de sécurité et des failles. Fausser les résultats du rapport peut conduire à vérifier les mauvaises sécurités et aussi montrer un niveau de sécurité inexact. Pour cela, l'auditeur doit accepter sa responsabilité et son obligation (contractuelle et limitée) pour la rédaction exacte et précise du rapport d'audit.

### **5.3. *VALIDITE ET ACCREDITATION DU RAPPORT***

Un test certifié OSSTMM, permet d'accréditer la sécurité opérationnel d'une cible, et nécessite d'être signé et accompagné par un STAR (doit être envoyé à l'ISECOM pour l'accréditation officielle OSSTMM). Cela permet de :

1. Servir de preuve quant au test réel
2. Rendre responsable l'auditeur du test
3. Transmettre un résultat clair au client
4. Transmettre une revue complète au client plutôt qu'un résumé technique
5. Fournir une métrique compréhensible.

## 5.4. EVALUATION DU RISQUE

La méthodologie OSSTMM tient compte de quatre dimensions afin de garantir un environnement de risque minimal lors du test :

### 5.4.1. SECURITE

Tous les tests doivent prendre en compte les pires cas dans les scénarios. Cela requiert de l'auditeur d'ignorer toutes considérations humaines ou émotionnelles.

### 5.4.2. RESPECT DE LA VIE PRIVEE

Tous les tests doivent prendre en compte le respect de la vie privée, en regard des lois et règlements ainsi que de l'éthique.

### 5.4.3. PRATIQUE

Tous les tests doivent être implémentés avec une complexité minimale, une viabilité maximale et une portée claire.

### 5.4.4. UTILISABLE

Tous les tests doivent être exécutés dans un cadre de sécurité. Les tests utilisés dans ce manuel sont effectués pour chercher un niveau de sécurité défini, aussi appelé niveau de sécurité pratique.

## 6. RAV

### 6.1. DEFINITION

Un RAV est le résultat d'un calcul prenant en compte les opérations de contrôles, de sécurité et de limitation représentant l'état actuel de protection. Il permet de définir l'investissement nécessaire pour atteindre la sécurité voulue (différence entre le niveau actuel et le niveau souhaité) et permet de « modéliser » les axes les moins sécurisés (priorisation des points à traiter en fonction des ressources et des failles). Il donne ainsi le spectre des protections les plus adaptées en fonction des contrôles à mettre en place sur les ressources définies. Le RAV permet en outre à chaque propriétaire d'actif, de définir la valeur qu'il « accepte ».



*Exigence 4.2.1 : critères d'acceptation des risques et niveau de risques acceptable (source : CLUSIR)*

### 6.2. FONCTION DU RAV

Il ne s'agit pas de représenter le risque selon la formule  $\text{Risque} = (\text{Menace} \times \text{Vulnérabilité} \times \text{Actifs})$  mais plutôt la prise en compte de l'impact d'un niveau de vulnérabilité donné conjugué avec le niveau de protection souhaité.

Le RAV mesure la porosité d'une cible (en effet, il accompagne forcément un audit...) et se compose de trois parties et 10 contrôles.

1 – Déterminer la porosité de la cible est défini par la mesure de ce qui est visible et qui peut interagir de l'extérieur avec le périmètre et aussi les interactions non authentifiées entre les index (à l'intérieur du périmètre)

2 – Déterminer des contrôles effectifs sont pondérés de 0.1 à 1 (0.1 = poreux)

3 – Déterminer les limitations des protections et des contrôles

### **6.3. COMPOSITION DU RAV**

#### **6.3.1. OPSEC**

Concerne la combinaison des protections (Visibilité des opérations, Accessibilité, Approbation)

#### **6.3.2. CONTROLES**

##### **6.3.3. CLASS A**

- Authentification (Autorisation + Identification)
- Indemnisation
- Résistance
- Subjugation (résultat des actions)
- Continuité

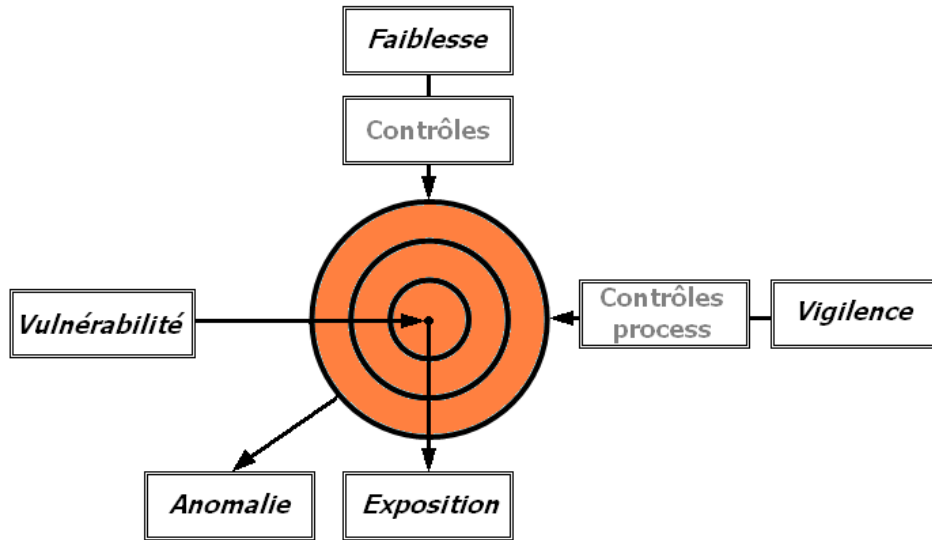
##### **6.3.4. CLASS B**

- Non-répudiation
- Confidentialité
- Protection de la vie privée
- Intégrité
- Alerte

##### **6.3.5. LIMITATIONS**

- Vulnérabilité
- Faiblesse
- Inquiétudes
- Exposition
- Anomalie

### 6.3.6. SCHEMA DES LIMITATIONS



<i>Type</i>	<i>Entreprise</i>	<i>Rédacteur</i>	<i>Numéro</i>	<i>Version</i>
REFERENCE	PRONETIS	B. Fantino	1	1.0.3
Projet MDIP				13/03/2009

## 7. Conclusion de l'étude de la méthodologie OSSTMM

C'est une méthode qui se veut rigoureuse et scientifique, un manuel permettant de gérer un audit comme un projet en décrivant l'approche technique à utiliser. Depuis la version 2.2 l'OSSTMM n'est plus considéré comme une méthode d'Ethical Hacking, mais plutôt comme une approche permettant de mesurer des systèmes opérationnels sur l'ensemble des volets d'un SI (infrastructures, applications, process, personnels). Cela a pour conséquence directe de limiter le parallèle entre le CEH et l'OSSTMM, par définition du CEH est vraiment une méthode de piratage, l'OSSTMM d'audit.

La norme ISO 27001 et la méthode OSSTMM sont complémentaires. En effet, l'OSSTMM s'inscrit dans l'ISMS défini par la 27001 pour matérialiser les risques des SI. Au-delà des résultats d'audit cette méthode apporte les recommandations priorisées et la formalisation du rapport d'audit permettant d'améliorer le niveau de sécurité et de fournir un tableau de bord opérationnel (d'une métrique de sécurité (RAV)).