

Étude comparée des méthodes de gestion des risques

RESUME :

Ce rapport présente la norme ISO/IEC 27005, les méthodes EBIOS, MEHARI, OCTAVE /OCTAVE-S et IT-Grundschutz sous l'angle des objectifs, des processus et des outils.

AUTEURS :

S. Poggi

Mai 2005

O. Derrouazi

Mai 2009 (version mise à jour)



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie
et du Commerce extérieur



CENTRE DE RECHERCHE PUBLIC
HENRI TUDOR
www.tudor.lu



CASES

LUXEMBOURG

**CYBERWORLD AWARENESS AND
SECURITY ENHANCEMENT STRUCTURE**

CITI

SOMMAIRE

Introduction	7
1. ISO/IEC 27005	8
1.1 OBJECTIFS.....	8
1.2 PROCESSUS.....	9
1.3 OUTIL.....	10
2. EBIOS.....	11
2.1 OBJECTIFS.....	11
2.2 PROCESSUS.....	12
Préalable	13
Etape 1 : Etude du contexte.....	13
Etape 2 : Expression des objectifs de sécurité	13
Etape 3 : Etude des menaces	14
Etape 4 : Identification des besoins de sécurité	14
Etape 5 : Détermination des exigences de sécurité.....	15
Résultats d’une étude EBIOS.....	15
2.3 OUTILS.....	16
Logiciel	18
3. MEHARI	21
3.1 OBJECTIFS.....	21
3.2 PROCESSUS.....	21
Analyse des situations de risque.....	22
Etape 1 : Evaluation de l’exposition naturelle	22
Etape 2 : Evaluation des facteurs de dissuasion et prévention	23
Etape 3 : Evaluation de la potentialité.....	23
Etape 4 : Evaluation de l’impact intrinsèque	24
Etape 5 : Evaluation des facteurs de protection, palliation et récupération.....	24
Etape 6 : Evaluation de la réduction d’impact, évaluation de l’impact	25
Etape 7 : Evaluation globale du risque.....	25
En résumé	26

Version 2009

CITI

3.3 OUTIL.....	26
OCTAVE / OCTAVE-S.....	28
4.1 OBJECTIFS.....	28
4.2 PROCESSUS.....	28
Phase 1 : Vue organisationnelle : Constitution des profils de menaces basés sur les actifs de l'entreprise.....	28
Phase 2 : Vue technique : Identification des vulnérabilités de l'infrastructure.....	29
Phase 3 : Développement de la stratégie de sécurité et planification.....	29
OCTAVE.....	29
Phase 1 : Vue organisationnelle.....	29
Phase 2 : Vue technique.....	30
Phase 3 : Développement de la stratégie.....	30
OCTAVE-S.....	31
Phase 1 : Vue organisationnelle.....	31
Phase 2 : Vue technique.....	31
Phase 3 : Développement de la stratégie.....	31
4.3 OUTILS.....	32
OCTAVE.....	32
OCTAVE-S.....	32
5. IT-Grundschutz.....	33
5.1 OBJECTIFS.....	33
5.2 PROCESSUS.....	34
Le standard 100-2 : la méthodologie de l'IT-Grundschutz.....	35
Etape1 : Initialisation du processus de sécurité IT.....	36
Etape 2 : Production du concept de sécurité.....	36
Etape 3 : Implémentation du concept de sécurité.....	36
Etape 4 : Maintien et amélioration.....	36
5.3 OUTILS.....	37
Synthèse.....	39
Table des figures.....	41
Version 2009	

CITI

ACRONYMES

BSI

Bundesamt für Sicherheit in der Informationstechnik

CERT /CC

Computer Emergency Response Team/ Coordination Center

CLUSIF

CLUb de la Sécurité de l'Information Français

DCSSI

Direction Centrale de la Sécurité des Systèmes d'Information

EBIOS

Expression des Besoins et Identification des Objectifs de Sécurité

FEROS

Fiche d'Expression Rationnelle des Objectifs de Sécurité

ISO

International Standardization Organization

MA

Méthodes d'Attaque

MEHARI

MEthode Harmonisée d'Analyse de Risques

OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation

PP

Protection Profile

PSSI

Politique de sécurité des systèmes d'information

CITI

RSSI

Responsable de la Sécurité des Systèmes d'Information

SEM

Survivable Enterprise Management

SI

Système d'Information

SSI

Sécurité des Systèmes d'Information

SSIC

Sécurité des Systèmes de l'Information et de la Communication

ST

Security Target

Introduction

De nos jours, les organismes sont dépendants des performances du SI (Système d'Information). Celui-ci contient toutes les données stratégiques et est ainsi devenu le centre névralgique de l'entreprise. Cette dépendance au SI entraîne des risques, qui peuvent remettre en cause la pérennité de l'entreprise.

L'analyse de risque permet d'identifier les dangers induits par les applications et les systèmes informatiques, d'évaluer les risques et de définir des barrières de protection qui vont les réduire à des niveaux acceptables.

Les méthodes de gestion des risques sont nombreuses et leurs approches peuvent être différentes. Il n'existe pas de bonne ou de mauvaise méthode de gestion des risques, puisqu'il y a une grande diversité dans les activités, dans les enjeux et dans les approches de la sécurité.

Dans ce document, sont présentés :

- La norme internationale ISO/IEC 27005 qui traite de la gestion des risques des SI (Système d'Information)
- Les méthodes les plus utilisées à savoir EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), MEHARI (Méthode Harmonisée d'Analyse de Risques), OCTAVE/OCTAVE-S (Operationally Critical Threat, Asset, and Vulnerability Evaluation/Small) et IT-Grundschutz

Pour chacune d'elles, les objectifs, les processus et les outils associés aux méthodes sont présentés de manière à en faciliter la comparaison.

CITI

1. ISO/IEC 27005

1.1 OBJECTIFS

L'**ISO/IEC 27005** (International Standardization Organization) donne des lignes directrices pour gérer les risques en sécurité de l'information. La norme étaye les concepts généraux spécifiés dans l'ISO/IEC 27001.

Elle a pour but d'aider à mettre en œuvre l'ISO/IEC 27001, la norme relative aux Systèmes de Management de la Sécurité de l'Information (SMSI), pour la partie gestion du risque. Pour comprendre cette norme internationale, il est important de connaître les concepts, modèles, processus et termes exposés dans l'ISO/IEC 27001 et l'ISO/IEC 27002 (Code de bonne pratique pour la gestion de la sécurité de l'information).

CITI

1.2 PROCESSUS

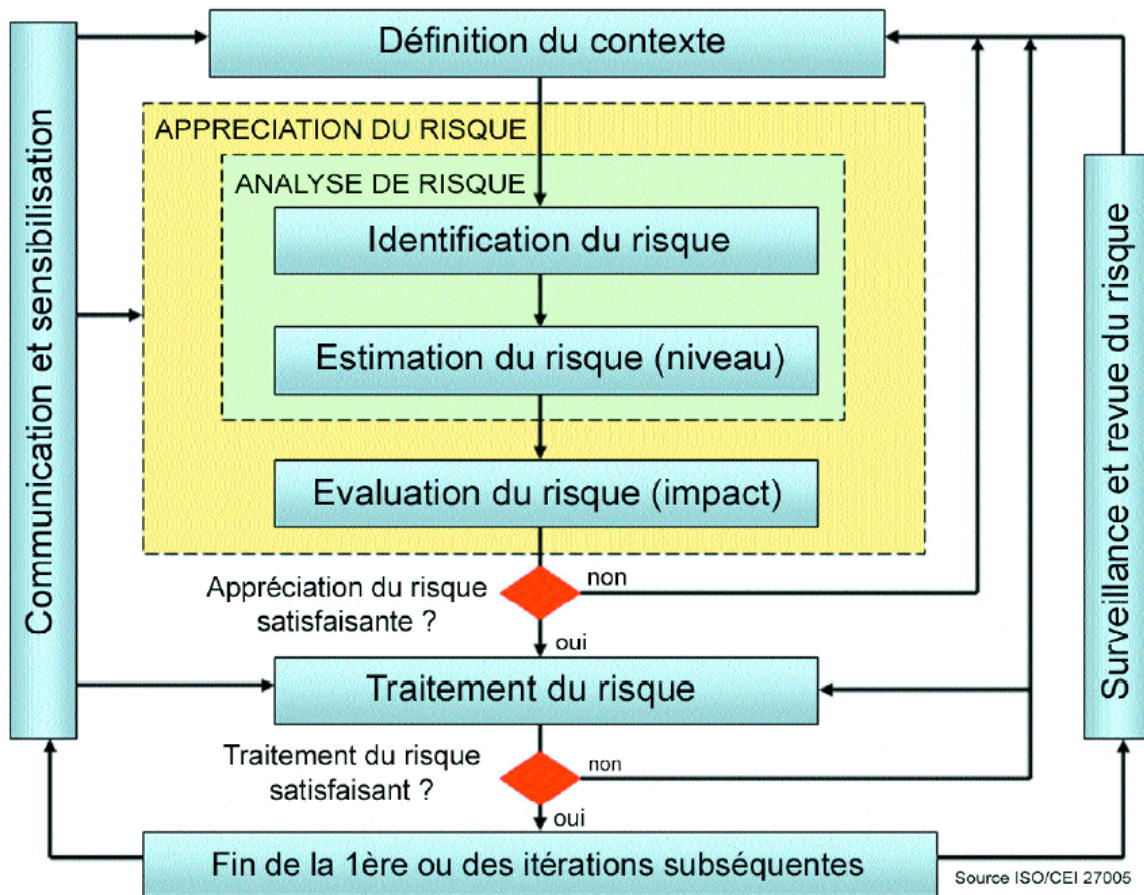


Figure 1-Processus ISO/IEC 27005

Le processus de gestion du risque en sécurité de l'information se décompose comme suit :

- Définition du contexte
- Identification du risque
- Estimation du risque
- Evaluation du risque
- Traitement du risque

CITI

Toutefois, l'ISO/IEC 27005 ne donne aucune méthodologie spécifique. Il appartient à chaque organisation de préciser son approche, en fonction du périmètre du SMSI, du contexte de gestion du risque ou du secteur d'activité.

1.3 OUTIL

L'outil logiciel le plus connu pour la norme ISO/IEC 27005 est SCORE ISMS (outil payant et disponible sur le marché) qui supporte actuellement EBIOS, MEHARI, AS/NZS 4360 prépare l'intégration de l'ISO/IEC 27005.

CITI

2. EBIOS

2.1 OBJECTIFS

La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), est une méthode d'appréciation et de traitement des risques, mais également un outil d'assistance à la maîtrise d'ouvrage. La méthode peut couvrir aussi bien un système déjà existant que s'inscrire dans une démarche d'amélioration. La démarche proposée par EBIOS apporte une vision globale et cohérente de la SSIC (Sécurité des Systèmes de l'Information et de la Communication). Elle fournit un vocabulaire et des concepts communs, elle permet d'être exhaustif et de déterminer des objectifs de sécurité adaptés au travers de cinq étapes. Elle permet aussi d'impliquer l'ensemble des acteurs du SI dans la problématique de sécurité.

De plus, un logiciel libre distribué gratuitement par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) permet de faciliter une étude EBIOS. Il permet en effet de consigner l'ensemble des résultats d'une étude et de produire les documents de synthèse nécessaires.

CITI

2.2 PROCESSUS

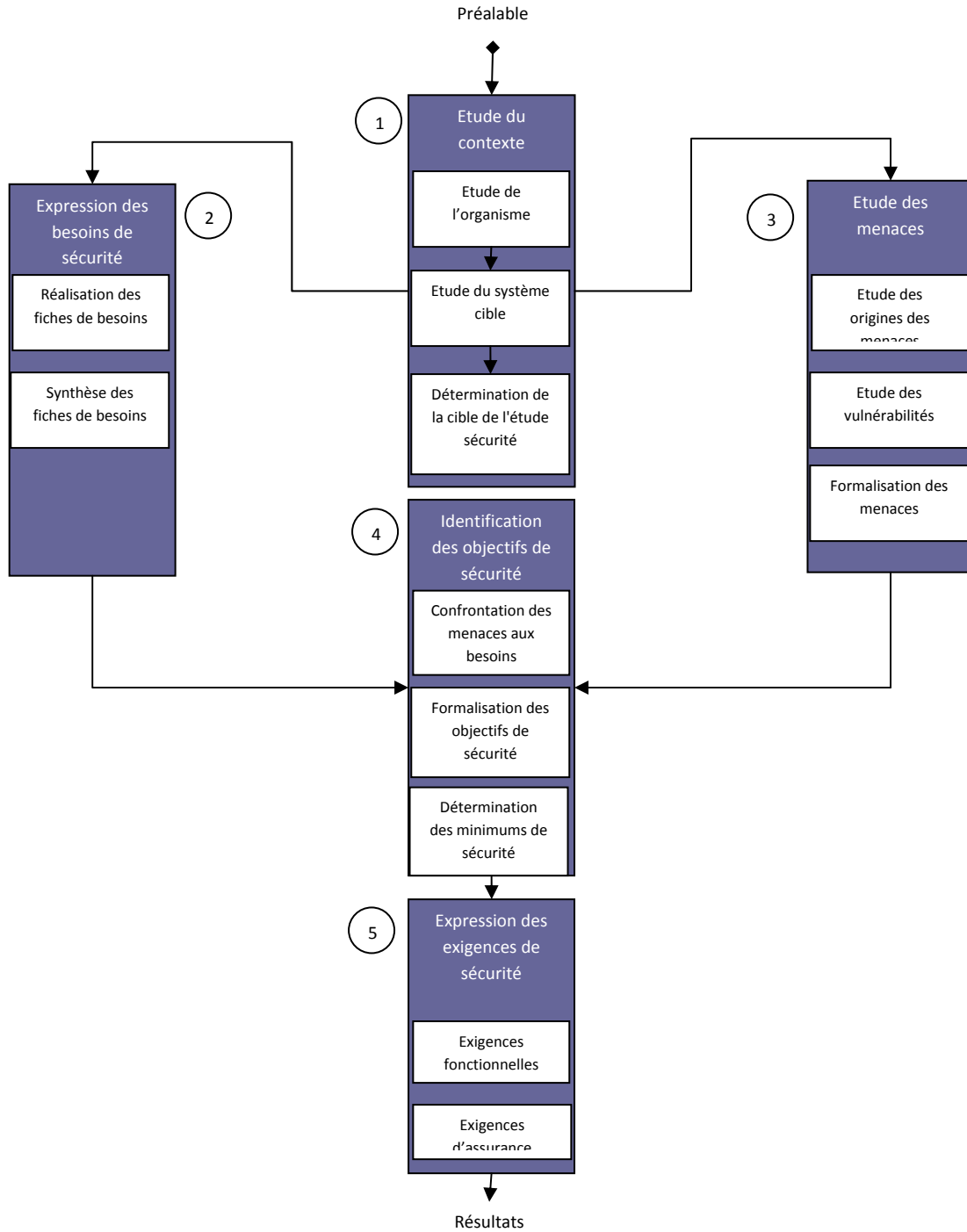


Figure 2-La démarche EBIOS

CITI

Préalable

Idéalement l'étude EBIOS s'appuie sur différents documents, existants ou à définir, relatifs à l'organisme, à son système d'information et au système à étudier. Par exemple le schéma directeur de l'organisme, la PSSI (Politique de Sécurité des Systèmes d'Information) et les spécifications générales du système.

Etape 1 : Etude du contexte

Activité 1.1 : Etude de l'organisme

Cette activité consiste à définir le cadre de l'étude, à identifier globalement le système cible et le situer dans son environnement pour déterminer précisément la cible de l'étude de sécurité. Des informations générales sur l'organisme concerné par le projet de sécurité doivent donc être réunies dans le but de mieux apprécier sa nature, son organisation et les contraintes qui pèsent sur celui-ci. Il est aussi nécessaire d'obtenir une vision fonctionnelle du système d'information de l'organisme. Le cadre réglementaire ne doit également pas être oublié.

Activité 1.2 : Etude du système cible

Cette activité a pour but de préciser le contexte d'utilisation du système à concevoir ou existant. Elle permet notamment de préciser pour le système les enjeux, le contexte de son utilisation, les missions ou services qu'il doit rendre et les moyens utilisés. Pour cela, il est nécessaire de préciser le sous-ensemble du système d'information de l'organisme constituant le système cible de l'étude et ses enjeux. Le système cible est alors décrit et sont recensées les hypothèses, les règles de sécurité et ses contraintes.

Activité 1.3 : Détermination de la cible de l'étude sécurité

Cette activité a pour but de recenser et décrire les entités sur lesquelles reposent les éléments essentiels du système cible (fonctions et informations).

Etape 2 : Expression des objectifs de sécurité

Activité 2.1 : Réalisation des fiches de besoin

Elles permettront aux utilisateurs d'exprimer les besoins de sécurité des éléments qu'ils manipulent habituellement dans le cadre de leur activité, d'une manière objective et cohérente selon les exigences opérationnelles du système et non selon les solutions techniques. Il s'agit d'une activité contribuant à l'estimation des risques et à la définition des critères de risques dans le processus de gestion des risques. On étudiera donc particulièrement les impacts dus au non-respect des besoins de sécurité exprimés.

CITI

Activité 2.2 : Synthèse des besoins de sécurité

Cette activité a pour but d'affecter aux éléments essentiels les besoins de sécurité qui résultent de la synthèse des valeurs attribuées par les utilisateurs. À l'issue de cette activité, il sera possible de disposer d'une vision objective et cohérente des besoins de sécurité du système cible.

Etape 3 : Etude des menaces

Cette étape a pour objectif la détermination des menaces pesant sur le système.

Activité 3.1 : Etude des origines des menaces

Cette activité a pour but de sélectionner les méthodes d'attaque qui sont pertinentes pour le système cible. Chacune des méthodes d'attaque est caractérisée par les critères de sécurité qu'elle peut affecter. Elle est associée à des éléments menaçants caractérisés selon leur type ou leur cause. Si les méthodes d'attaque composent des risques réels pour le système cible, le niveau des mesures de sécurité devra être cohérent avec ce potentiel d'attaque.

Activité 3.2 : Etude des vulnérabilités

Cette activité a pour objet la détermination des vulnérabilités spécifiques du système cible, provenant des caractéristiques des entités qui le composent, et éventuellement la caractérisation de celles-ci en termes de niveau.

Activité 3.3 : Formalisation des menaces

Cette activité a pour but de déterminer les menaces pouvant affecter le système cible. Elles résultent de l'association des méthodes d'attaque (activité 3.1) aux vulnérabilités retenues (activité 3.2). À l'issue de cette activité, il sera possible de disposer d'une vision objective et exhaustive des menaces réelles pesant sur le système cible.

Etape 4 : Identification des besoins de sécurité

Activité 4.1 : Confrontation des menaces aux besoins

Cette activité a pour but de déterminer les risques réels pesant sur le système cible. La confrontation des menaces aux besoins de sécurité permet de retenir et hiérarchiser les risques qui sont véritablement susceptibles de porter atteinte aux éléments essentiels. L'ensemble de ces risques devra être évalué, la plupart d'entre eux devant être couverts par des objectifs de sécurité.

Activité 4.2 : Formalisation des objectifs de sécurité

CITI

Cette activité a pour but de déterminer les objectifs de sécurité permettant de couvrir les risques, conformément à la détermination des niveaux de sécurité. La complétude de la couverture des risques par les objectifs de sécurité, en prenant en compte les hypothèses, règles de sécurité et contraintes, devra être démontrée.

Activité 4.3 : Détermination des niveaux de sécurité

Cette activité a pour but de déterminer le niveau de résistance adéquat pour les objectifs de sécurité. Elle permet également de choisir le niveau des exigences de sécurité d'assurance, ce qui permet d'être en adéquation avec la norme ISO/IEC 15408 (Critères Communs).

Etape 5 : Détermination des exigences de sécurité***Activité 5.1 : Détermination des exigences de sécurité fonctionnelles***

Cette activité a pour but de déterminer les exigences de sécurité fonctionnelles permettant de couvrir les objectifs de sécurité identifiés pour le système cible. Elle permet de décider de la manière dont chaque risque identifié devra être traité.

Activité 5.2 : Détermination des exigences de sécurité d'assurance

Cette activité a pour but l'expression complète des exigences de sécurité d'assurance de la cible de l'étude de sécurité. Elles sont sélectionnées selon le niveau d'assurance choisi lors de la détermination des niveaux de sécurité. Elles constituent le fondement de la confiance dans le fait qu'un système cible satisfait à ses objectifs de sécurité.

Résultats d'une étude EBIOS

La méthode permet d'identifier des objectifs et exigences de sécurité à la suite d'une appréciation de risques. Elle permet donc de contribuer à la réalisation d'un schéma directeur SSI (Sécurité des Systèmes d'Information), d'une PSSI, d'un plan d'action SSIC, d'une FEROS (Fiche d'Expressions Rationnelles des Objectifs de Sécurité), d'un cahier des charges, d'un PP (Protection Profile) ou d'une ST (Security Target) au sens de l'ISO/IEC 15408.

2.3 OUTILS

Il existe cinq documents de support à EBIOS fournis directement par la DCSSI.

Un document d'« Introduction » qui présente le contexte, l'intérêt et le positionnement de la démarche EBIOS. Elle contient aussi une bibliographie, un glossaire et des acronymes.

Un document intitulé « Démarche » qui expose le déroulement des activités de la méthode. Chaque activité est organisée de la façon suivante : préalable, données en entrée, actions, données en sortie, conseils pratiques. Les étapes sont présentées de façon claire et accompagnées de schémas.

Le document appelé « Techniques » est un guide d'accompagnement qui contient des moyens pour réaliser une étude EBIOS. Les concepts autour de chaque activité sont ainsi présentés plus avant.

Le document « Outillage pour l'appréciation des risques SSI » est la première partie de la base de connaissance de la méthode. Elle contient une typologie des types et sous-types d'entités pouvant être soumises à une étude EBIOS. On y trouvera les méthodes d'attaque les plus répandues avec leurs principales atteintes sur les critères de sécurité (Confidentialité – Intégrité – Disponibilité). La dernière partie du document est une synthèse des deux parties précédentes, c'est à dire qu'elle présente pour chaque type et sous-types, les méthodes d'attaque auxquelles les entités sont exposées.

Type d'entités	MA	Vulnérabilité
RES	5	Supports accessibles à des personnes non autorisées

Figure 3-Exemple d'identification de risque pour une entité

L'exemple ci-dessus signifie que les entités RES (réseaux) sont vulnérables aux MA (méthodes d'attaque) de type 5, à savoir la destruction de matériels ou de supports. La vulnérabilité est employée ici, si les supports sont accessibles à des personnes non autorisées. La méthode d'attaque 5 portant atteinte à l'intégrité et à la disponibilité. A noter que ce document est réutilisé lors des activités 1.3 et 3.1.

Le document « Outillage pour le traitement des risques SSI » (indispensable pour les activités 4.2 et 5.1) est la deuxième partie de la base de connaissance de la méthode. Elle contient en première partie une base d'objectifs de sécurité génériques par type d'entités. La seconde partie permet la compatibilité avec deux autres standards internationaux : ISO/IEC 15408 et ISO/IEC 27002. Elle présente les exigences de sécurité fonctionnelles génériques proposées dans ces référentiels. D'autres exigences de sécurité fonctionnelles sont également présentées. La dernière partie du document est une synthèse des deux

CITI

parties précédentes mais aussi du document sur l'appréciation des risques. Il présente pour chaque vulnérabilité de chaque type et sous-type d'entité, les objectifs et les exigences de sécurité réduisant la vulnérabilité.

Si l'on reprend l'exemple précédent, cela donne :

Type d'entités	MA	Vulnérabilité	Objectif de sécurité	Exigence de sécurité
RES	5	Supports accessibles à des personnes non autorisées	ORG_01	BPE_ZOS.2.1
RES	5	Supports accessibles à des personnes non autorisées	ORG_01	BPE_SEM.1.1
RES	5	Supports accessibles à des personnes non autorisées	ORG_01	CET_EGT.2.3
RES	5	Supports accessibles à des personnes non autorisées	ORG_01	BPE_ZOS.1.1

Figure 4-Exemple de traitement des risques pour une entité

L'exemple ci-dessus signifie que les entités réseaux sont vulnérables aux MA de type 5, à savoir la destruction de matériels ou de supports, si les supports sont accessibles à des personnes non autorisées. Afin de diminuer la vulnérabilité, il est recommandé d'accomplir l'objectif de sécurité ORG_01. Si l'on se réfère au code correspondant cela signifie que l'organisation doit protéger les équipements et supports contre l'accès physique par des personnes non autorisées. Cela veut dire qu'il faut remplir les exigences de sécurité suivantes :

- *BPE_ZOS.2.1* : Les zones de sécurité doivent être protégées par des mesures de maîtrise appropriées à l'entrée pour faire en sorte que seul le personnel autorisé puisse y avoir accès.
- *BPE_SEM.1.1* : Le matériel informatique doit être situé et protégé de façon à réduire les risques présentés par les menaces et les dangers liés à l'environnement et les occasions d'accès non autorisés.
- *CET_EGT.2.3* : A partir de sa prise en charge, l'interlocuteur interne est responsable d'un visiteur jusqu'à son départ. Il doit notamment s'assurer que la visite se déroule en accord avec les principes de sécurité énoncés dans la politique de sécurité.
- *BPE_ZOS.1.1* : Les organismes doivent utiliser des périmètres de sécurité pour protéger les zones qui contiennent des infrastructures de traitement de l'information.

On pourra trouver également sur le site de la DCSSI dans la rubrique « les meilleures pratiques », des documents destinés à formaliser les résultats d'une étude EBIOS sous forme d'un schéma directeur SSI, d'une PSSI, d'un plan d'action SSIC, d'une FEROS, d'un cahier des charges, d'un PP, d'une ST, etc.

CITI

Logiciel

La méthode EBIOS est également disponible sur CD-ROM sur simple demande à la DCSSI. Ce CD-ROM contient la documentation et le logiciel d'assistance.

Ce logiciel permet de simplifier la réalisation d'une étude EBIOS. Il intègre ainsi toute une série d'aides très intéressantes comme des questionnaires ou des listes de contraintes. De plus il implémente la base de connaissance EBIOS. Il permet également de générer automatiquement une FEROS en fonction des données d'une étude réalisée à l'aide du logiciel.

Le logiciel d'assistance propose également un exemple d'étude EBIOS et un module d'auto-formation.

CITI

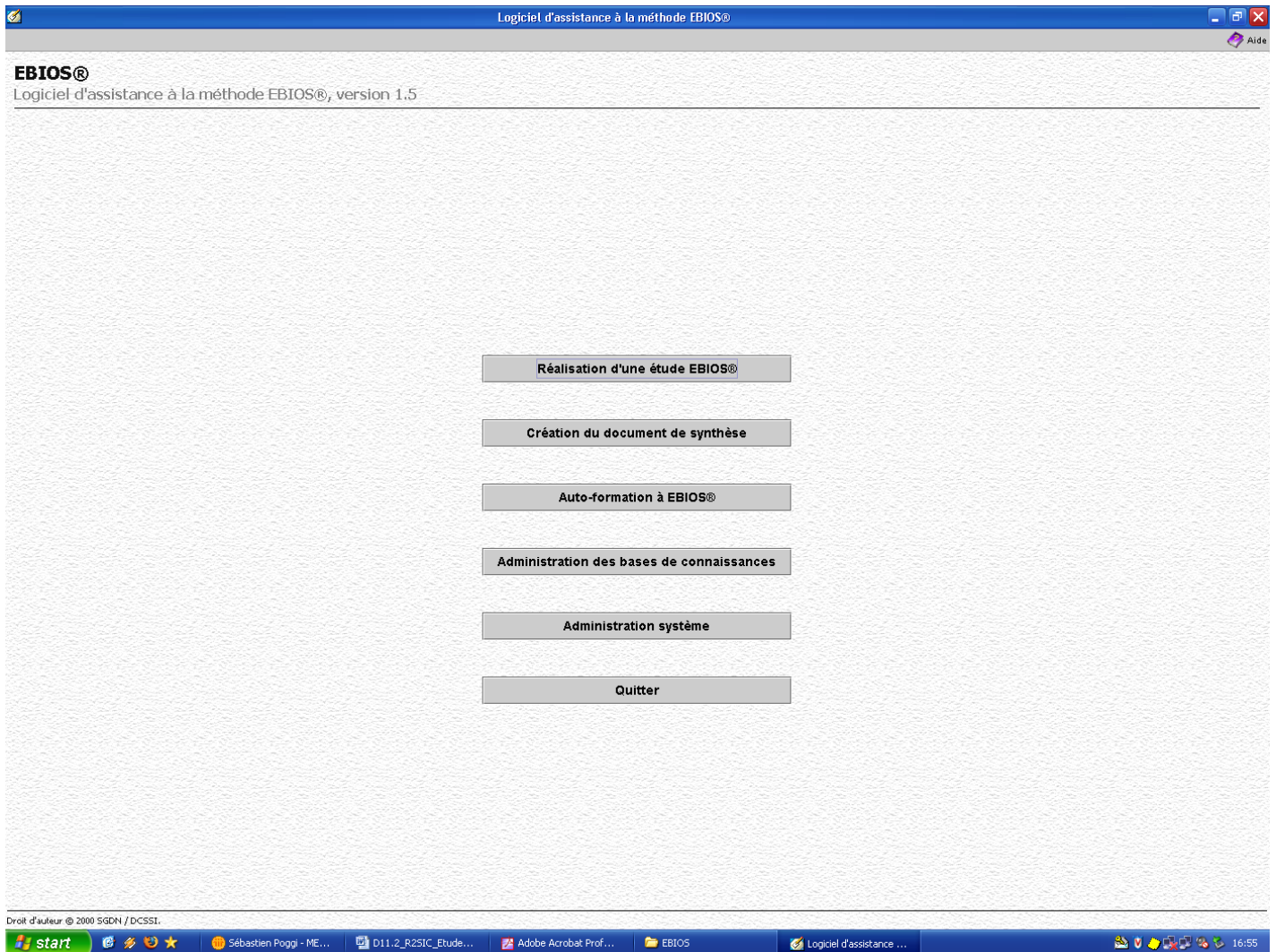


Figure 5-Copie d'écran du logiciel d'assistance à la méthode EBIOS

CITI

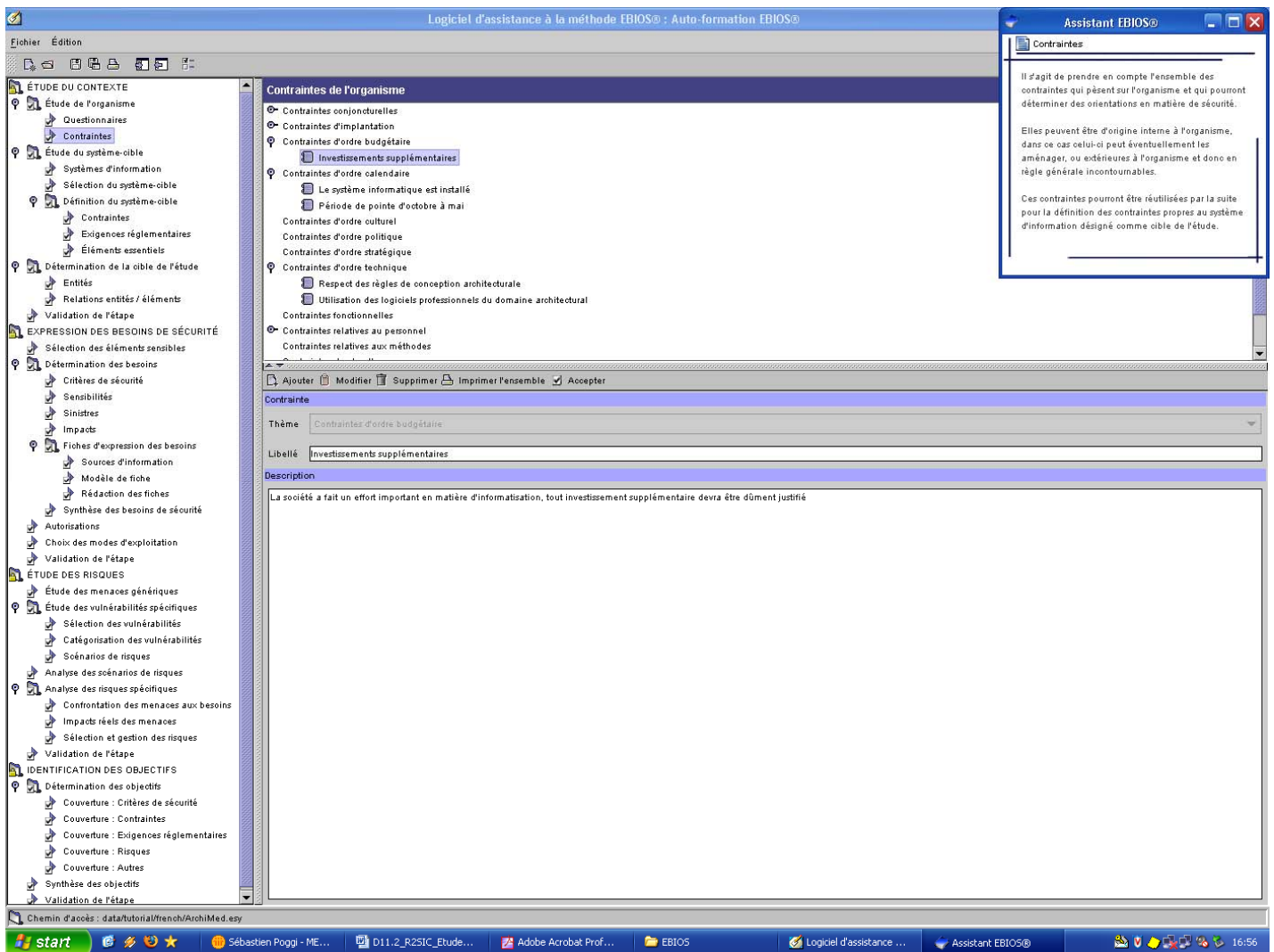


Figure 6-Copie d'écran du logiciel d'assistance à la méthode EBIOS

CITI

3. MEHARI

3.1 OBJECTIFS

MEHARI est utilisé pour aider les RSSI (Responsable de la Sécurité des Systèmes d'Information) dans leur tâche de management de la sécurité des systèmes d'information.

MEHARI est avant tout une méthode d'analyse et de management des risques. En pratique, MEHARI et l'ensemble de ses bases de connaissances sont bâtis pour permettre une analyse précise des risques, quand cela sera jugé nécessaire, sans pour autant imposer l'analyse des risques comme une politique majeure de management.

3.2 PROCESSUS

Pour cette partie il convient de se focaliser sur l'analyse des situations de risque qui est l'un des processus de la méthode MEHARI.

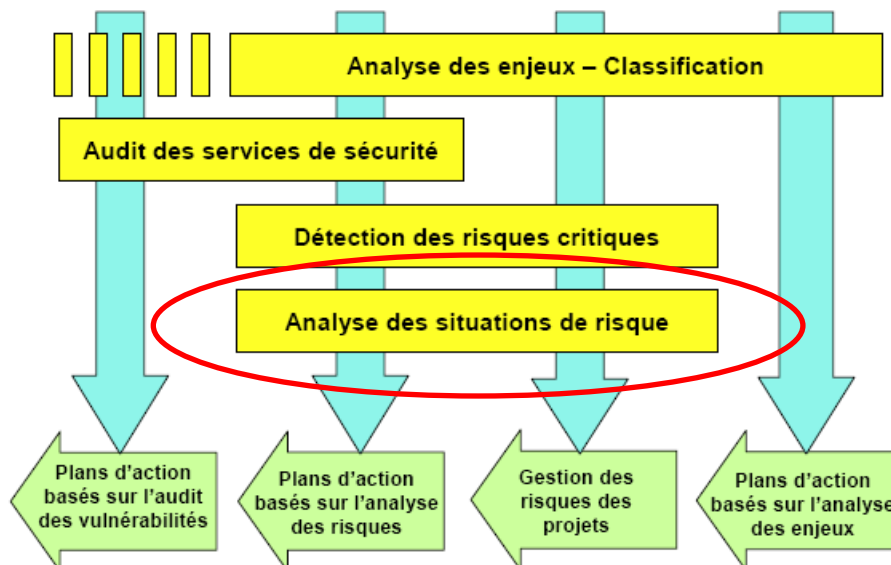


Figure 7-Processus MEHARI

CITI

Analyse des situations de risque

Le processus d'analyse d'une situation de risque comprend une démarche de base, éventuellement assistée par des automatismes, selon la manière dont la situation est décrite et selon l'existence ou non d'un audit préalable des services de sécurité.

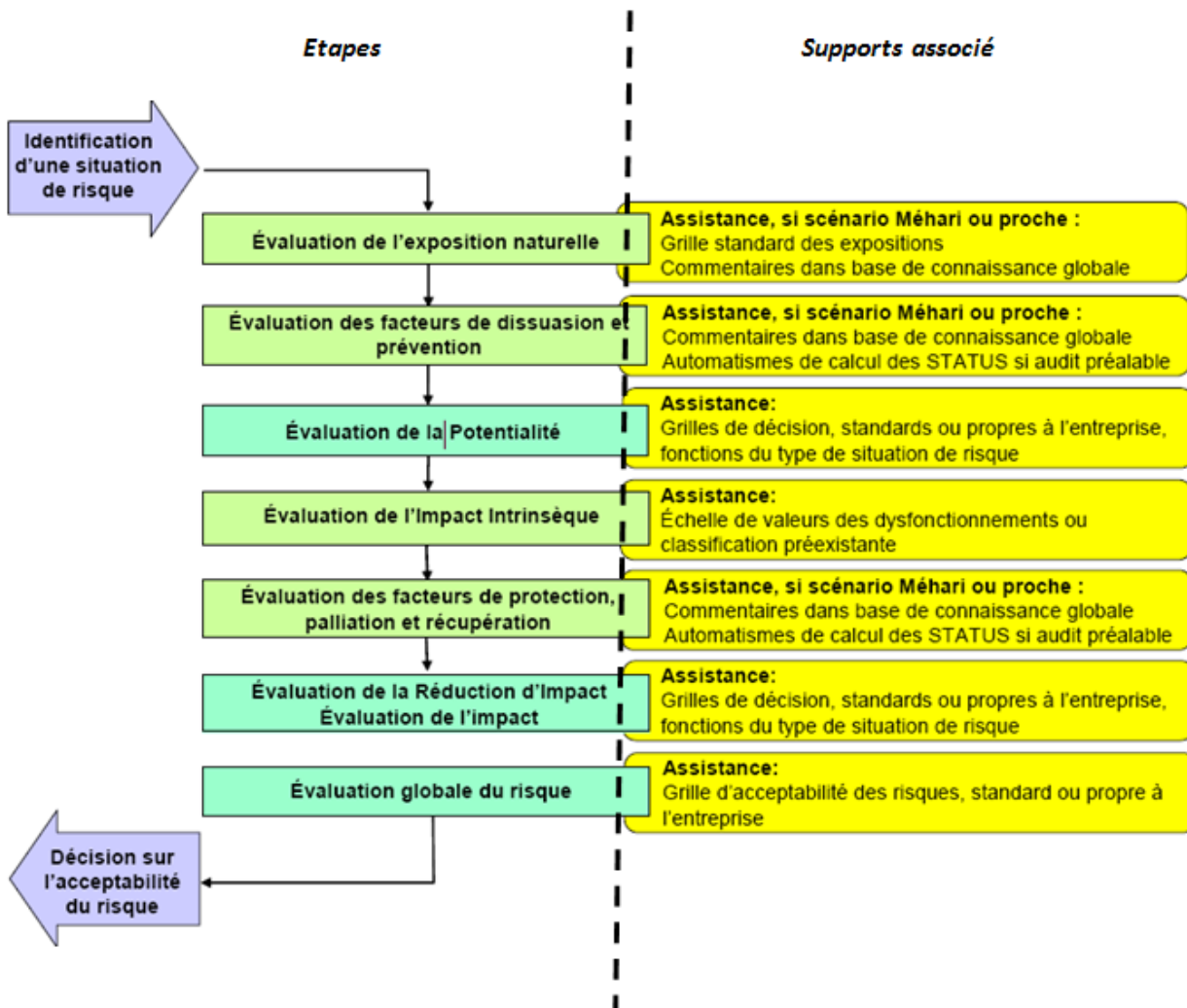


Figure 8-Processus d'analyse des risques

Etape 1 : Evaluation de l'exposition naturelle

Cette étape se divise en deux parties. Tout d'abord l'exposition naturelle standard et deuxièmement l'exposition naturelle spécifique.

Version 2009

CITI

Exposition naturelle standard

Les scénarios 1 de la base de connaissances MEHARI se réfèrent à une liste limitée d'événements de base, qu'il s'agisse d'accidents, d'erreurs ou d'actes volontaires, pour lesquels une évaluation a priori de l'exposition est donnée.

Par exemple, il est estimé que l'exposition naturelle « standard » d'une entreprise à un incendie est de niveau 2 (plutôt improbable), à une panne d'équipement informatique de niveau 3 (plutôt probable) et à une erreur pendant un processus de saisie de niveau 4 (très probable).

La liste de ces événements et de l'exposition naturelle standard est donnée en annexe 1 de la méthode.

Exposition naturelle spécifique

Il doit être clair que l'évaluation standard proposée n'est qu'une évaluation par défaut et que l'évaluation directe de l'exposition de l'entreprise à la situation de risque analysée est de loin préférable.

Étape 2 : Evaluation des facteurs de dissuasion et prévention

Les facteurs de réduction tels que la dissuasion, la prévention, la protection, la palliation et la récupération sont proposés par les bases de connaissances de MEHARI en fonction de la qualité des services de sécurité si celle-ci a été évaluée par un audit. La définition des niveaux de facteur de réduction de risque est donnée en annexe 4 de la norme.

Étape 3 : Evaluation de la potentialité

La potentialité du risque représente, en quelque sorte, sa probabilité d'occurrence, bien que cette occurrence ne soit pas modélisable en termes de probabilité. Cette potentialité est fonction du contexte et des mesures de sécurité en place.

L'évaluation de la potentialité est faite sur une échelle comprenant 4 niveaux, présentés ci-après.

Échelle de potentialité

Niveau 4 : Très probable

A ce niveau, il est raisonnable de penser que le scénario se produira très certainement et vraisemblablement à court terme.

Quand le risque survient, personne n'est surpris.

Niveau 3 : Probable

Il s'agit là des scénarios dont il est raisonnable de penser qu'ils pourraient bien se produire, à plus ou moins court terme. L'espoir que le risque ne survienne pas n'est pas insensé mais dénote un certain optimisme.

La survenance du risque déçoit, mais ne surprend pas.

CITI

Niveau 2 : Improbable

Il s'agit là de scénarios dont il est raisonnable de penser qu'ils ne surviendront pas. L'expérience passée montre d'ailleurs qu'ils ne sont pas survenus. Ils demeurent néanmoins « possibles » et ne sont pas complètement invraisemblables.

Niveau 1 : Très improbable

A ce niveau, l'occurrence du risque est tout à fait improbable. De tels scénarios ne sont pas strictement impossibles car il existe toujours une infime probabilité pour que cela se produise.

Niveau 0 : Non envisagé

Les scénarios réellement impossibles n'ont pas à faire partie de la base des scénarios à étudier. Ce niveau est utilisé pour classer les scénarios que l'organisation a décidé de ne pas analyser.

Etape 4 : Evaluation de l'impact intrinsèque

L'impact intrinsèque est une estimation maximaliste des conséquences du risque, en dehors de toute mesure de sécurité.

La démarche d'évaluation des impacts intrinsèques consiste à remplir un tableau d'impact intrinsèque, basé sur celui fourni en Annexe 3 de la méthode, dont un extrait est donné ci-dessous.

Tableau d'impact intrinsèque			
Classification des données, informations et éléments d'infrastructure	D	I	C
Données et informations			
D01 Fichiers de données ou bases de données applicatives			
D07 Courrier et télécopies			
.../...			
Infrastructure informatique et télécom			
R02 Équipements et câblage des réseaux locaux			
S01 Systèmes centraux, serveurs applicatifs, ...			

Figure 9-Tableau d'impact intrinsèque

Le remplissage de ce tableau s'effectue en transcrivant le niveau de conséquence d'une atteinte à la disponibilité (D), l'intégrité (I) ou la confidentialité (C) de chaque type de ressource identifié (cependant certaines cases n'ont pas à être remplies car cela n'aurait aucun sens : par exemple l'intégrité du personnel d'exploitation).

Etape 5 : Evaluation des facteurs de protection, palliation et récupération

Même processus que pour l'étape 2.

CITI

Etape 6 : Evaluation de la réduction d'impact, évaluation de l'impact

L'évaluation de la réduction d'impact aussi appelé STATUS-RI se fait à partir de trois autres indicateurs appelés STATUS d'impact (STATUS-PROT pour protection, STATUS-PALL pour palliation, STATUS-RECUP pour récupération) et en utilisant la grille correspondant à la nature du scénario (Disponibilité, Intégrité, Confidentialité)

Exemple :

Prenons le scénario « Altération de données par erreur lors de la saisie » qui est de nature Intégrité.

Si nous avons :

STATUS-PROT=2, STATUS-PALL=2, STATUS-RECUP=4

Selon la grille proposée en annexe de la méthode on obtient :

		PALL			
		1	2	3	4
RECUP	1	1	2	3	3
	2	1	2	3	3
	3	2	2	3	3
	4	2	3	3	4

Figure 10-Grille de réduction d'impact

La réduction d'impact est égale à 3.

Etape 7 : Evaluation globale du risque

Dans cette étape on décide de la manière de gérer le risque, en fonction de son impact et de sa potentialité : l'accepter, le refuser ou le transférer.

CITI

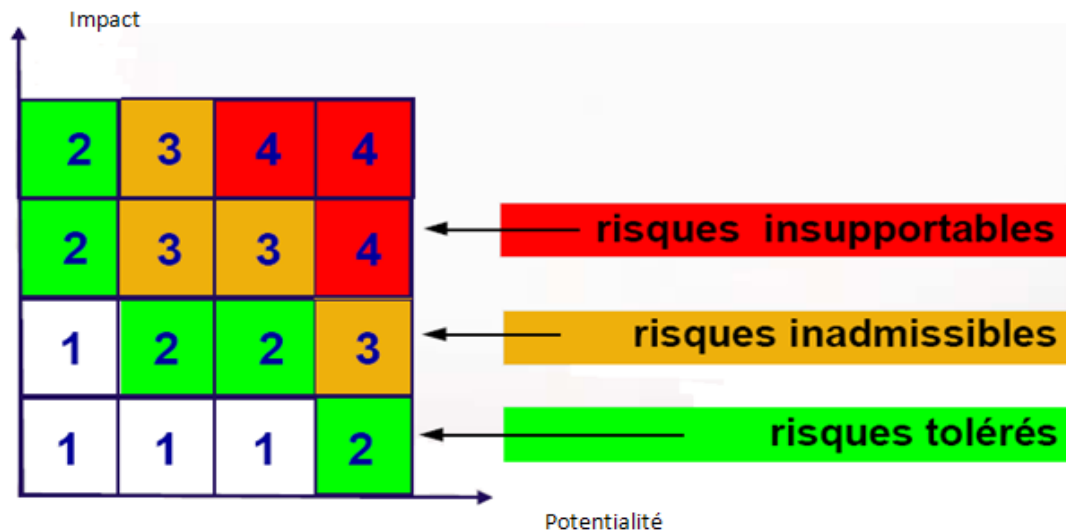


Figure 11-Evaluation globale du risque

En résumé

- Une situation de risque peut être caractérisée par une potentialité et un impact intrinsèques, en l'absence de toute mesure de sécurité.
- Potentialité intrinsèque et Impact intrinsèque peuvent être évalués.
- Des mesures de sécurité peuvent venir réduire ce risque intrinsèque par le biais de facteurs significatifs de réduction de risque.
- Ces facteurs d'atténuation de risque peuvent être évalués.
- Sur la base de ces éléments, il est possible d'évaluer une potentialité et un impact résiduels, caractéristiques du risque, et d'en déduire un indicateur de gravité de risque.
- MEHARI propose des outils d'assistance tout au long de ce processus d'analyse et d'évaluation.

3.3 OUTIL

RISICARE est une approche associée à un outillage, s'appuyant sur la méthode MEHARI et qui permet d'améliorer la productivité et la justesse d'une démarche de gestion des risques. Cet outil est payant et disponible sur le marché.

RISICARE s'appuie sur les caractéristiques suivantes :

- L'utilisation de la méthode MEHARI développée au sein du CLUSIF (CLUB de la Sécurité des systèmes d'Information Français) comme modèle d'analyse des risques

CITI

- La possibilité de personnaliser les bases de connaissances, voire de construire ses propres bases de connaissances (RISIBASE)
- Une relation entre un audit de l'existant et la quantification de scénarios
- L'élaboration de plans d'actions cohérents optimisant la réduction de l'ensemble des risques
- Une aide en ligne très développée avec l'accès à un ensemble de rubriques méthodologiques et techniques
- Un outil performant et simple à utiliser

Avantages :

- Automatisation
- Rapidité
- Complétude de l'analyse
- Conçu pour permettre une approche de diagnostic qui s'adapte à la taille et à la complexité de l'organisme

Inconvénient :

- Il est essentiel de bien assimiler MEHARI pour utiliser cet outil, notamment en PME ou son utilisation nécessite de savoir définir un périmètre des processus clefs afin d'optimiser la démarche et les ressources.

OCTAVE / OCTAVE-S

4.1 OBJECTIFS

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) est une méthode d'évaluation des vulnérabilités et des menaces sur les actifs opérationnels. Ce sont ces actifs opérationnels et les pratiques de sécurité qui ont dirigé l'orientation de la méthode. Elle a également été conçue pour être menée par des membres internes à une organisation, sans faire appel à des spécialistes externes. Cette technique permet, par la même occasion, d'améliorer la connaissance de l'entreprise sur ses propres pratiques de sécurité. Pour être menée à bien elle suppose donc la composition d'une équipe d'analyse multidisciplinaire.

4.2 PROCESSUS

L'approche OCTAVE est avant tout basée sur les actifs de l'entreprise. L'équipe d'analyse devra donc :

- Identifier les actifs de l'entreprise
- Centrer son analyse des risques sur les actifs les plus critiques
- Considérer les relations entre ces actifs ainsi que les menaces et les vulnérabilités pesant sur eux
- Evaluer les risques d'un point de vue opérationnel
- Créer une stratégie de protection basée sur des pratiques

Pour y parvenir, OCTAVE définit donc trois phases comme le montre la figure ci dessous.

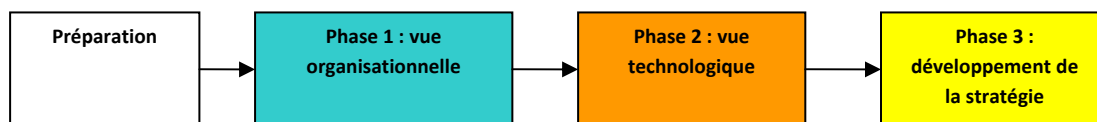


Figure 12-Les phases principales d'OCTAVE

Phase 1 : Vue organisationnelle : Constitution des profils de menaces basés sur les actifs de l'entreprise

C'est une évaluation avant tout organisationnelle. Il s'agit de l'identification des ressources informatiques importantes, de leurs menaces et des exigences de sécurité associées. On évalue les

CITI

pratiques actuelles de l'organisation pour protéger ces ressources critiques (si elles existent) et on identifie les vulnérabilités sur ces ressources. On étudie ensuite les menaces qui pourraient les exploiter pour dégager ensuite un profil de menace.

Phase 2 : Vue technique : Identification des vulnérabilités de l'infrastructure

C'est une évaluation de l'infrastructure informatique. L'équipe d'analyse identifie les moyens d'accès aux actifs, dégage des classes de composants qui leur sont reliés, pour finalement déterminer les classes qui sont déjà résistantes aux attaques et celles qui doivent être améliorées.

Phase 3 : Développement de la stratégie de sécurité et planification

L'équipe d'analyse procède à une analyse des risques sur les actifs opérationnels et décide du traitement possible.

OCTAVE

La méthode OCTAVE se décompose en 8 processus répartis dans les 3 phases majeures de la méthode.

Phase 1 : Vue organisationnelle***Processus 1 : Identification des connaissances par les cadres supérieurs***

Le but est d'identifier la vue que les dirigeants ont des actifs de l'entreprise, les menaces qui s'y rattachent, les impératifs de sécurité et ce qui est actuellement fait pour remplir ces impératifs.

Processus 2 : Identification des connaissances par les cadres de l'opérationnel

Le but est d'identifier la vue que les cadres ont des actifs opérationnels de l'entreprise, les menaces qui s'y rattachent, les impératifs de sécurité et ce qui est actuellement fait pour remplir ces impératifs.

Processus 3 : Identification des connaissances par les équipes de production

Le but est d'identifier la vue qu'ont les équipes de production et l'équipe IT des actifs de l'entreprise, les menaces qui s'y rattachent, les impératifs de sécurité et ce qui est actuellement fait pour remplir ces impératifs.

CITI

Processus 4 : Création des profils de menace

Le but est de consolider les données recueillies lors des trois processus précédents et de déterminer les ressources critiques de l'entreprise, d'identifier les impératifs de sécurité et les menaces qui pèsent sur les actifs.

Pour créer ces profils de menace, il existe un guide complet de l'ensemble des profils. Il est certes loin d'être exhaustif mais il propose une vue intéressante en arborescence et une classification par impact.

Phase 2 : Vue technique

Processus 5 : Identification des composants clefs

Le but est ici d'identifier les composants clefs pour chaque actif critique de l'entreprise. On sélectionnera ensuite la méthode et les outils pour procéder à l'audit des vulnérabilités.

Processus 6 : Evaluation des composants sélectionnés

Le but est ici de procéder à un audit des vulnérabilités des composants sélectionnés dans le processus précédent.

Phase 3 : Développement de la stratégie

Processus 7 : Analyse des risques

Le but est d'identifier les risques, de définir une métrique pour évaluer ces risques et de procéder à cette évaluation en utilisant les profils de menace définis au cours du processus 4.

Processus 8 : Développements

Ce processus se divise en deux parties :

- **Partie A : Développement de la stratégie de protection**
Le but est de définir une stratégie de protection, un plan de gestion des risques et une liste d'actions à mener à court terme.
- **Partie B : Sélection de la stratégie de protection**
Le but est ici d'impliquer les dirigeants dans la stratégie de protection et de décider de l'implémentation des contre-mesures retenues.

CITI

OCTAVE-S

OCTAVE-S (Small) est une version réduite d'OCTAVE à destination des entreprises de moins de 100 salariés. On retrouve les 3 phases présentées ci-avant. Les processus sont allégés et la méthode est ainsi plus accessible à une organisation disposant de moins de ressources. Comme pour OCTAVE, la méthode est bien documentée avec des guides de travail, des conseils et un exemple complet.

Phase 1 : Vue organisationnelle

Processus 1 : Dégager des informations sur l'organisation

Le but est d'établir un critère d'évaluation d'impact, d'identifier les actifs de l'organisation et d'évaluer les pratiques de sécurité actuelles de l'organisation.

Processus 2 : Créer les profils de menace

Le but est de sélectionner des actifs critiques, d'identifier les impératifs de sécurité pour les actifs ainsi que les menaces qui pèsent sur ces derniers.

Phase 2 : Vue technique

Processus 3 : Examiner l'infrastructure informatique en relation avec les actifs critiques

Le but est ici d'examiner les voies d'accès aux actifs critiques de l'entreprise. On analysera ensuite les processus en rapport avec la technologie.

Phase 3 : Développement de la stratégie

Processus 4 : Identifier et analyser les risques

Le but est d'évaluer l'impact des menaces, d'établir un critère de probabilité et enfin d'évaluer la probabilité d'occurrence des menaces.

Processus 5 : Développer la stratégie de protection et les plans de réduction des risques

Le but est de décrire la stratégie actuelle, de sélectionner l'approche pour la gestion, d'identifier les changements et les actions à mener.

CITI

4.3 OUTILS

OCTAVE

La documentation offre des conseils sur la préparation à la méthode, comment sélectionner son équipe d'analyse, choisir le périmètre de l'étude, identifier les participants clefs. Elle fournit également un modèle de planning et des références pour l'adaptation de la méthode.

Chaque processus fait ensuite l'objet d'un volume séparé (il en existe une vingtaine en tout). On retrouvera pour chaque processus un résumé des objectifs à atteindre, des feuilles de travail, et un descriptif des objectifs à remplir. La méthode va jusqu'à définir les concepts qu'elle aborde afin que des non-spécialistes puissent l'utiliser. De plus, chaque processus est également présenté sous forme de présentation électronique à diffuser à l'équipe.

Par ailleurs, un exemple complet accompagne le lecteur tout au long de la méthode. Il concerne la sécurisation d'une clinique.

OCTAVE-S

De la même façon, OCTAVE-S offre une documentation exhaustive. A la différence d'OCTAVE qui fournit plutôt un parcours, OCTAVE-S propose un ensemble de check-lists adaptées aux besoins de plus petites organisations. C'est une approche plus pragmatique.

Le même exemple que pour OCTAVE est proposé, à savoir une clinique, mais avec les check-lists d'OCTAVE-S.

5. IT-Grundschatz

5.1 OBJECTIFS

L'IT-Grundschatz présente une liste de mesures standards pour des SI génériques. Le but de ces recommandations est d'atteindre un niveau de sécurité adéquate pour les SI ayant un besoin de sécurité normal ou élevé.

Le manuel de L'IT-Grundschatz comprend:

- Une description d'une situation potentiellement dangereuse
- Des descriptions détaillées de mesures à prendre afin de faciliter la mise en œuvre
- Une description du processus d'établissement et de maintien d'un niveau de sécurité adéquat
- Une procédure simple pour déterminer le niveau de sécurité de l'information obtenu sous la forme d'une comparaison des résultats cibles

Ce manuel est gratuit, disponible à tous et qui plus est actualisé par l'insertion tous les 6 mois de nouveaux modules. Il est également possible de s'enregistrer gratuitement pour recevoir des informations complémentaires sur la méthode. Cela permet un échange entre utilisateurs et le BSI pour faire évoluer le manuel en fonction des remarques et besoins. De plus, des outils logiciels et des guides supplémentaires sont disponibles et il est possible d'être certifié.

CITI

5.2 PROCESSUS

Pour l'IT-Grundschutz nous allons nous focaliser sur le standard 100-2 méthodologie :

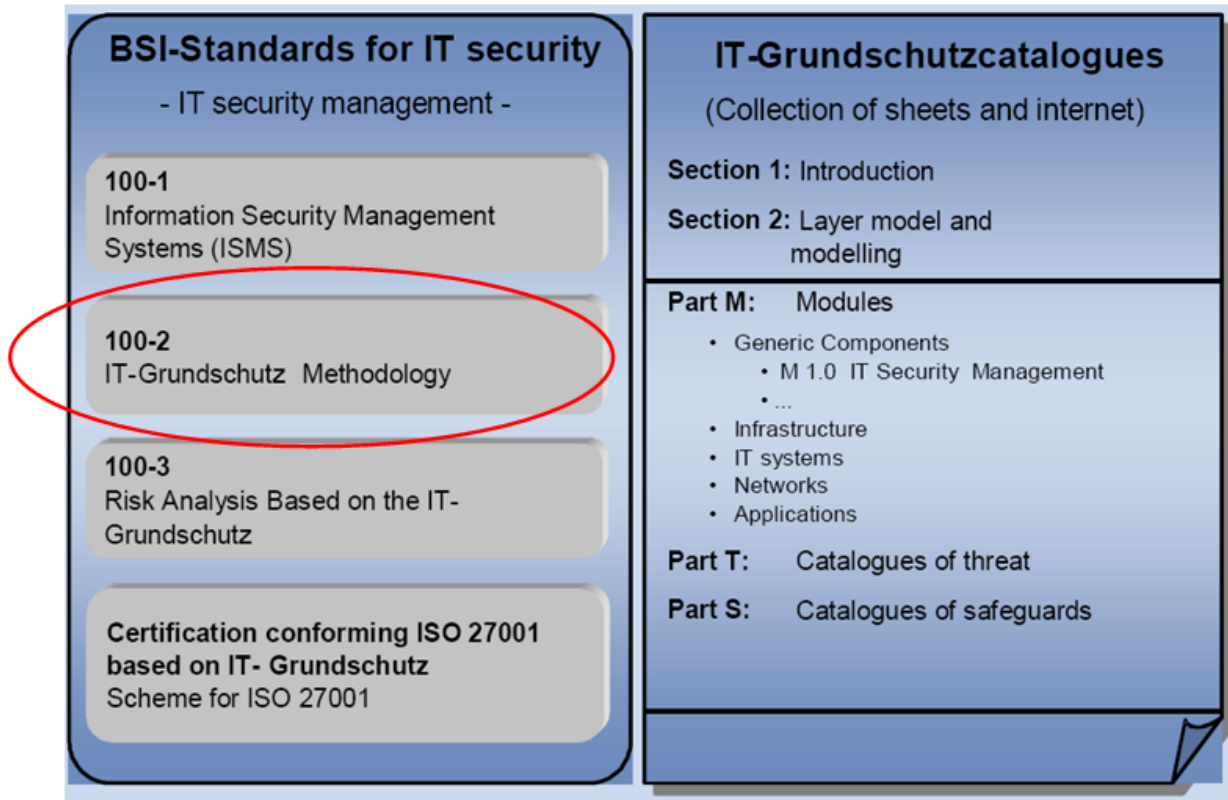


Figure 13-BSI standards

Le standard 100-2 : la méthodologie de l'IT-Grundschutz

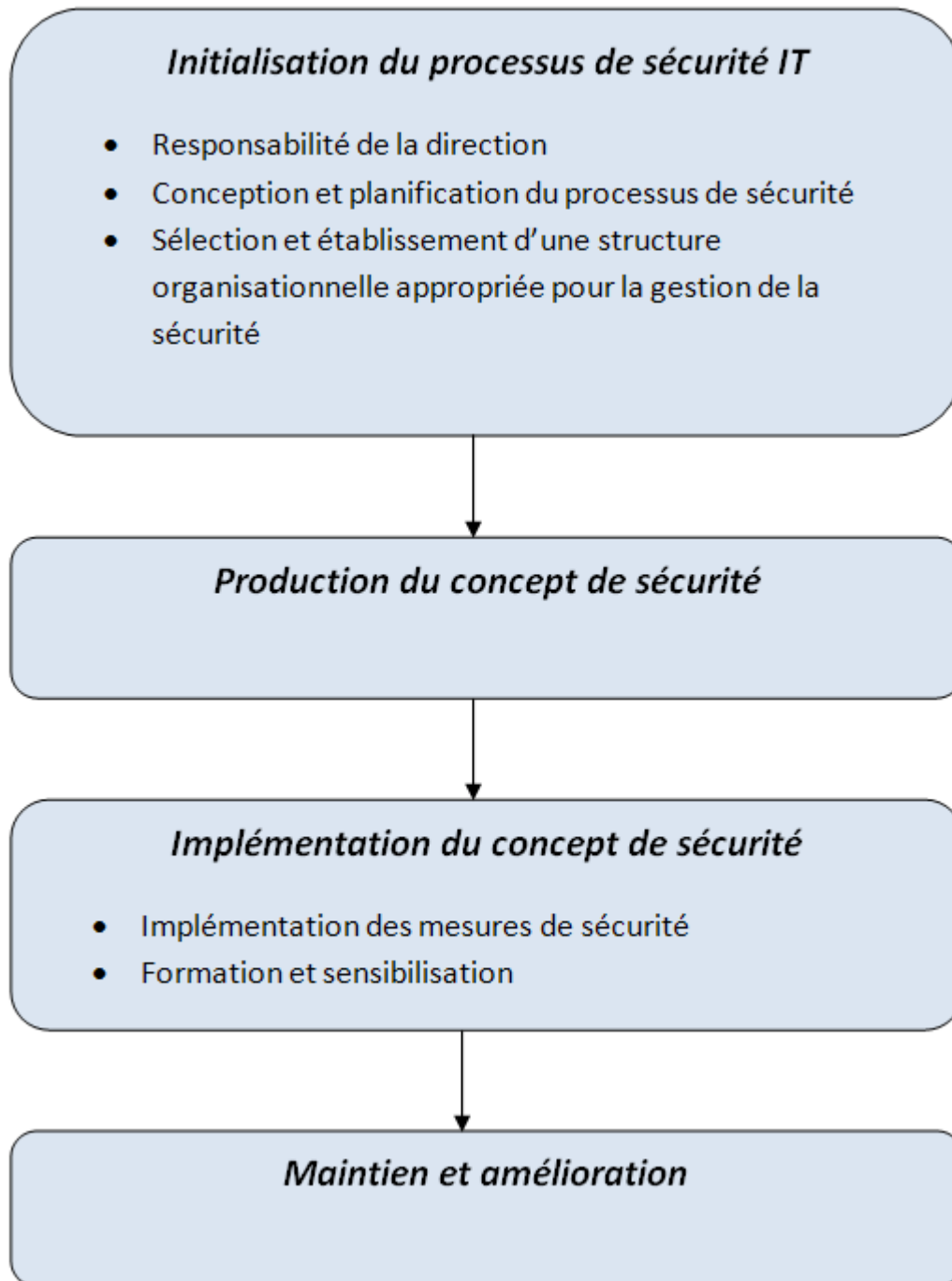


Figure 14-Processus de la méthodologie IT-Grundschutz

CITI

Etape 1 : Initialisation du processus de sécurité IT

Pour réaliser ou maintenir un niveau approprié de sécurité IT, il est nécessaire d'exiger une approche planifiée et organisée mais aussi une structure organisationnelle adéquate. Il est important de définir des objectifs de sécurité ainsi qu'une stratégie pour les réaliser, qui doit être fondée sur un processus continu.

Etape 2 : Production du concept de sécurité

Un des objectifs de l'IT-Grundschutz est de proposer une approche pragmatique et efficace à la réalisation d'un niveau de sécurité IT normal et qui peut aussi fournir la base pour un niveau de sécurité plus élevé. Pour produire un concept de sécurité IT, il faut tout d'abord initialiser le processus de sécurité puis définir l'organisation et la politique de sécurité à mettre en place.

De nombreuses références sont faites aux catalogues de l'IT-Grundschutz et apportent à l'utilisateur la base de connaissances nécessaire à la méthodologie.

Le module 1 du catalogue de l'IT-Grundschutz explique et détaille les étapes d'implémentation du concept de sécurité, les étapes sont :

- Analyse de la structure IT
- Définition d'exigences de protection
- Choix de mesure de sécurité
- Contrôle de sécurité basic
- Analyse de sécurité supplémentaire

Etape 3 : Implémentation du concept de sécurité

Cette section présente les aspects que l'on doit considérer pour implémenter le concept de sécurité. On retrouve ici comment mettre en œuvre les mesures de sécurité, les planifier, les exécuter, les surveiller et les contrôler. Depuis 2003, l'office fédéral de la sécurité de l'information propose un système de certification suivant le régime prévu par l'IT-Grundschutz, grâce auquel il est possible de vérifier le niveau de sécurité de l'information réellement atteint.

Etape 4 : Maintien et amélioration

Cette étape permet de garantir une amélioration continue du niveau de sécurité, grâce à :

- Des rapports de détection d'incidents

CITI

- Des tests de simulation d'incidents
- Des audits internes et externes
- Une certification de conformité à des critères de sécurité

5.3 OUTILS

Pour faciliter la sélection des contre-mesures à mettre en place, le BSI (Bundesamt für Sicherheit in der Informationstechnik) propose un outil shareware « GSTOOL », qui fournit cette sélection en spécifiant son infrastructure IT.

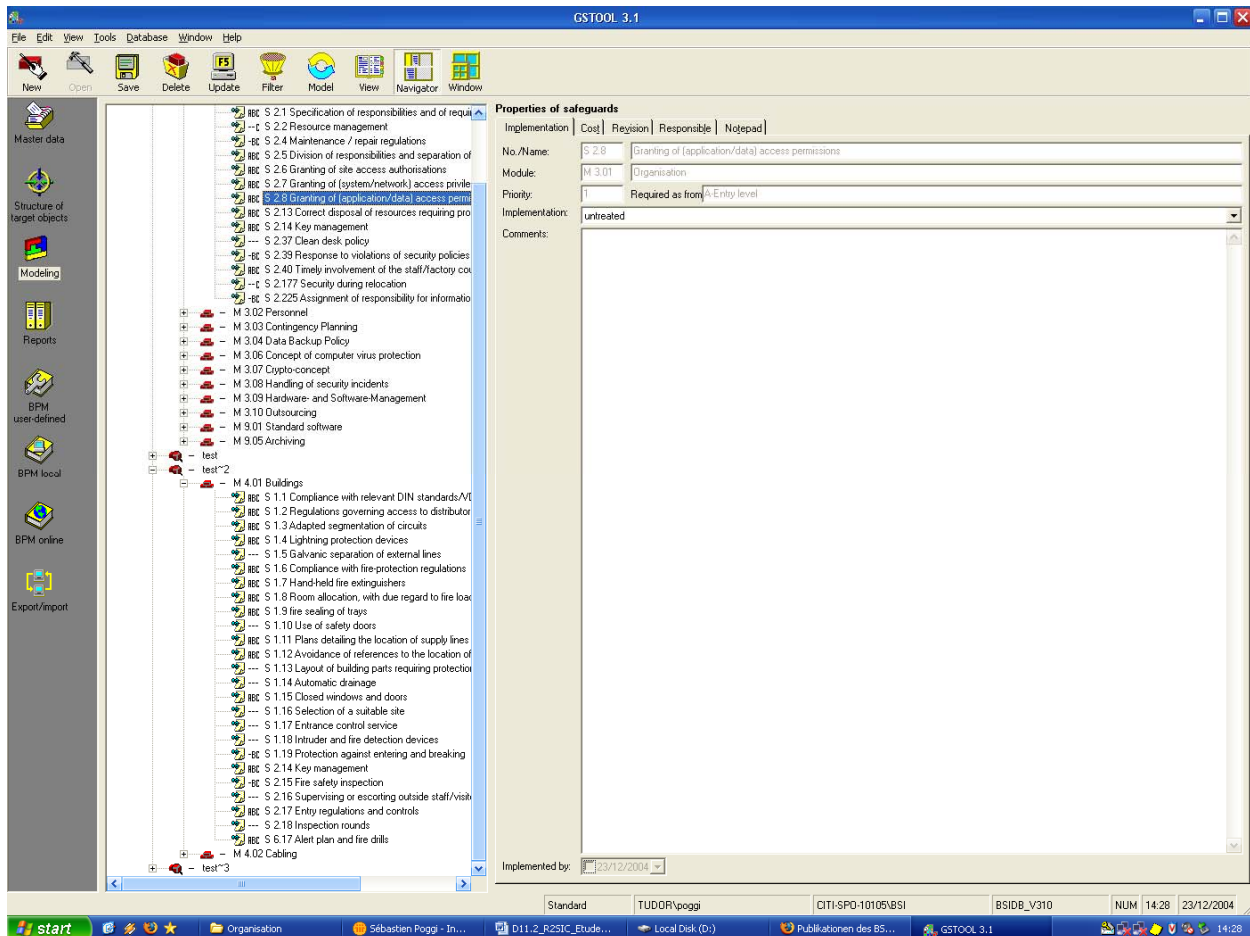


Figure 15-Copie d'écran du logiciel GSTOOL

CITI

Synthèse

Pour conclure, le tableau suivant met en évidence les avantages et inconvénients de chaque méthode.

	Avantages	Inconvénients
ISO/CEI 27005	<ul style="list-style-type: none"> • Démarche flexible 	<ul style="list-style-type: none"> • Ne constitue pas un guide
EBIOS	<ul style="list-style-type: none"> • Démarche très logique • Traitement des exigences • Logiciel • Bases de connaissances • Soutenue par la DCSSI • Très reconnue 	<ul style="list-style-type: none"> • Distingue peu l'opérationnel du reste de l'organisation • Difficile d'utilisation pour un novice de la sécurité
MEHARI	<ul style="list-style-type: none"> • Logiciel • Conçu par le CLUSIF • Reconnue 	<ul style="list-style-type: none"> • Méthode potentiellement lourde
OCTAVE / OCTAVE-S	<ul style="list-style-type: none"> • Orientée métier • Accessible à tous • Documentation très complète • Catalogue de pratiques • Variante –S pour les PME • Soutenue par le CERT /CC (Computer Emergency Response Team/ Coordination Center) 	<ul style="list-style-type: none"> • Ne traite pas les exigences
IT-Grundschutz	<ul style="list-style-type: none"> • Démarche simple, innovante • Rapidité de mise en œuvre • Très accessible 	<ul style="list-style-type: none"> • Non exhaustive • Ne traite pas les exigences • Peu formelle

CITI

	<ul style="list-style-type: none">• Mise à jour fréquente• Soutenue par l'Union Européenne• En pleine expansion• Certification possible	
--	--	--

Figure 16-Tableau de synthèse

Table des figures

Figure 1-Processus ISO/IEC 27005	9
Figure 2-La démarche EBIOS.....	12
Figure 3-Exemple d'identification de risque pour une entité.....	16
Figure 4-Exemple de traitement des risques pour une entité.....	17
Figure 5-Copie d'écran du logiciel d'assistance à la méthode EBIOS.....	19
Figure 6-Copie d'écran du logiciel d'assistance à la méthode EBIOS.....	20
Figure 7-Processus MEHARI	21
Figure 8-Processus d'analyse des risques	22
Figure 9-Tableau d'impact intrinsèque	24
Figure 10-Grille de réduction d'impact	25
Figure 11-Evaluation globale du risque	26
Figure 12-Les phases principales d'OCTAVE	28
Figure 13-BSI standards	34
Figure 14-Processus de la méthodologie IT-Grundschatz	35
Figure 15-Copie d'écran du logiciel GSTOOL.....	37
Figure 16-Tableau de synthèse	40