Centre Africain d'Etudes Supérieures en Gestion

CESAG BF – CCA
BANQUE, FINANCE, COMPTABILITE, CONTROLE & AUDIT

Master Professionnel
en Audit et Contrôle de Gestion
(MPACG)

Promotion 7
(2012-2014)

Mémoire de fin d'étude

THEME

LA MISE EN PLACE DU PROCESSUS DE GESTION DES RISQUES DU SYSTEME D'INFORMATION DU GIE GAINDE 2000 AVEC L'OUTIL EBIOS

Présenté par :
Malick SARR

Dirigé par :
Samba NDIAYE
Enseignant-Chercheur

FEVRIER 2016

DEDICACES

Je dédie ce mémoire à :

- **ALLAH LE TOUT PUISSANT** pour m'avoir donné la force et le courage d'arriver là ;
- ma mère, celle qui est toujours présente dans mon esprit pour faire mon bonheur. Merci pour t'être sacrifiée pour que tes enfants grandissent et prospèrent ;
- mon père, qui m'a envoyé à l'école, qui m'a toujours conseillé.
- à mes frères et sœurs.

REMERCIEMENTS

Mes remerciements vont à l'endroit de tous ceux qui ont contribué à ce travail, en particulier à :

- Mon directeur de mémoire, Monsieur Samba NDIAYE, enseignant-chercheur et maitre de conférences**,** je tiens à lui exprimer toute ma reconnaissance pour ses conseils avisés, sa disponibilité à m'accompagner tout au long de ce travail ;
- mon maitre de stage, Monsieur Mohamed DIOUF et l'ensemble du personnel de GAINDE 2000 pour les travaux pratiques mené au sein du GIE.

Je tiens également à remercier l'ensemble du corps enseignants du CESAG pour leur accompagnement tout au long de l'année.

Je n'oublie pas toutes les personnes que je n'ai pas pu citer nommément. Je voudrais que chacun de vous trouve dans ce document l'expression manifeste de ma profonde gratitude.

Listes des Sigles et Abréviations

AFAI : Association française pour l'audit et le conseil en informatique

AFNOR : Association française de normalisation

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

CCTA: Central Computing and Telecommunications Agency

CGR : Comité de Gestion du Risque

CI : Contrôle Interne

CIGREF : Club Informatique des Grandes Entreprises Françaises

CLUSIF : Club de la Sécurité des Systèmes d'Information Français

COSO: Committee of Sponsoring Organizations of the Treadway Commission

CRAMM: (CCTA Risk Analysis and Management Method)

CRM : Customer Relationship Management

DCSSI : Direction Centrale de la Sécurité des Systèmes d'Information

DDA : Déclaration D'Applicabilité

DIC : Disponibilité-Intégrité-Confidentialité

DO : Direction des Opérations

EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité

ERP : Enterprise Resource Planning

FEROS : fiche d'expression rationnelle des objectifs de sécurité

GIE: Groupement d'Intérêt Economique

HRM : Human Resource Management

IDS : Intrusion Detection System ou (système de détection d'intrusion)

ISACA: Information System Audit and Control Association

ISO: International Organization for Standardization

MEHARI : Méthode Harmonisée d'Analyse de Risques

OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation

PP : Profil de Protection

RSSI : Responsables de la sécurité de l'information

SMQ : système de management de la qualité

SMQSI : système de management de la qualité et la Sécurité de l'Information

SMSI : Système de Management de la Sécurité de l'Information

SSI : Sécurité des Systèmes d'Information

SI : Système d'Information

SIC : Science de l'Information et de la Communication

TIC : Technologies de l'Information et de la Communication

Liste des figures

Liste des tableaux

Liste des annexes

Table des matières

INTRODUCTION GENERALE

Quelles seraient les conséquences d'une faille du système d'information dans une entreprise ? Dans toute organisation, les ressources internes (la direction, le personnel…) et les ressources externes (les fournisseurs, les clients, l'Etat…) ont besoin de disposer d'informations afin de leur permettre de prendre des décisions en connaissance de cause, d'en contrôler l'exécution, de s'assurer de la qualité des résultats obtenus et, de coordonner l'action des différents membres de l'organisation.

Cette information peut prendre différentes formes (images, textes, etc.) et peut être obtenue de différentes manières. Souvent à l'aide des technologies de l'information et de la communication (TICs), d'une discussion entre deux individus, ou au cours d'une réunion, par la lecture d'un livre. Pour exploiter rationnellement cette matière première qu'est l'information pertinente en temps opportun, il est apparu nécessaire de disposer d'un véritable système d'information.

Tout changement de fonctionnement de l'entreprise impacte sur son système d'information (SI) que ce soit sous forme de modification de procédures de traitement, de stockage ou de communication de l'information ; dès lors on parlera du système d'information informatisé.

La société moderne devient de plus en plus, une société informatisée : l'informatique est devenue incontournable. Le manque de connaissance en informatique et le défaut de maîtrise de l'ordinateur (c'est-à-dire les logiciels de base) entrainent un handicap dans la compétitivité sur le marché et le risque de ne pas atteindre les objectifs dans des secteurs clefs de développement. L'informatique est devenue un privilégié de traitement de l'information dans les organisations, on parlera après de système d'information électronique ou système informatique.

En Afrique francophone, cette tendance se confirme au sein des entreprises qui sont, pour la plupart, en pleine restructuration ou modernisation. Ces entreprises perçoivent l'intérêt de maîtriser les systèmes d'information et leur valeur ajoutée, c'est le cas du GIE GAINDE 2000 qui évolue dans un milieu totalement informatisé et qui souhaiterait obtenir la certification ISO 9001 : 2008 relative aux exigences du système de management de la qualité et ISO 27001 : 2013 relative aux exigences du système de management de la sécurité de l'information.

La sensibilité aux risques liés aux systèmes d'information est donc devenue une des préoccupations majeures du GIE, notamment sur les aspects de confidentialité et d'accès aux

données, de conservation et d'archivage, de sécurité physique et de cohérence globale du système. Ces derniers points interpellent le GIE GAINDE 2000 qui manie deux (2) types d'informations : celles venant du client, et celles émanant de l'organisation.

Aujourd'hui, les documents, dossiers, factures du GIE GAINDE 2000 sont traités avec l'aide de composants informatiques, donc il faudra nécessairement que le système informatique soit en adéquation avec les dernières tendances technologiques, sécurisé on peut ainsi faire appel à une norme internationale 17799 :2005 qui établit des lignes directrices et des principes généraux pour préparer, mettre en œuvre, entretenir et améliorer la gestion de la sécurité de l'information au sein d'un organisme (En 2007, la norme ISO/CEI 17799:2005 étant obsolète, a été remplacée par la norme 27002 qui en reprend l'essentiel.). Mais le SI peut présenter des failles plus ou moins importantes. Naturellement, certaines menaces sont moins dangereuses que d'autres car plus facilement détectées.

Les vulnérabilités qui menace le GIE sont dues à la malveillance de certaines personnes qui ont tout intérêt à ce que l'entreprise ne fonctionne plus, ou qui cherchent à s'infiltrer dans le système afin de nuire à l'entité (vol d'information confidentielle…).

Le système informatique peut être attaqué par des virus qui s'en prennent au fonctionnement des ordinateurs, ou bien par un cheval de Troie ou un ver qui, vont s'infiltrer incognito dans le système, opérer seul sur les programmes et bloquer le système entier en se propageant d'un poste à un autre du réseau.

Mais aussi certaines failles sont à notées comme le non renouvellement du mot de passe Wifi et la non mise à jour des anti-virus et pare-feu.

Et tout ceci a pour conséquences des pertes de données clients et fournisseurs, financières, de confidentialité pour le GIE GAINDE 2000.

Quelle est l'origine des risques qui attaquent le GIE ?

Quelle est l'impact que les risques peuvent avoir sur l'entité ?

Quelle est la nécessité de gérer les risques du système d'information d'une entité ?

Comment évaluer le risque pour un SI ?

Quels risques devrait-on accepter de prendre ?

Au vue des problèmes d'insécurité que peut rencontrer un système d'information, nous avons posé une problématique à laquelle notre travail va tenter d'apporter des solutions qui est la suivante : Comment maitriser les risques du système d'information afin de les traiter ?

L'analyse du risque permet de recenser les risques de façon claire et structurée. Une organisation qui comprend clairement tous les risques auxquels elle est exposée, peut les jauger et les classer en ordre de priorité et, prendre les mesures appropriées pour réduire les pertes. Sa stratégie vise à inscrire la définition d'un plan d'action dans une logique managée. La stratégie de gestion des risques permet d'instruire la décision de traiter, de transférer, de refuser ou d'accepter les risques en fonction du niveau du risque, mais également de la recevabilité opérationnelle, technique, organisationnelle et financière des mesures à mettre en place.

La gestion des risques en sécurité de l'information, recommandée par de nombreux référentiels comme la norme ISO 27001, est en train de devenir une obligation pour les responsables de la sécurité de l'information (RSSI), les directeurs des systèmes d'information (DSI), et bien d'autres acteurs de l'entreprise.

Après les démarches de gestion des risques, comme EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) et MEHARI (Méthode d'Evaluation et de management des Risques liés à l'Information) en France, la norme ISO 27005, première méthode de gestion des risques structurée et normalisée, est appelée à s'imposer à l'échelle planétaire.

Le COSO 2 peut être une solution au problème posé. Il s'agit d'un cadre de référence pour la gestion des risques de l'entreprise (Enterprise Risk Management Framework).

Comme solution retenue, l'utilisation de l'application EBIOS, qui est la traduction sous forme de logiciel de la norme 27005, nous parait adéquate pour mettre en place un processus de gestion des risques du GIE GAINDE 2000.

L'objectif général de notre étude sera de montrer l'importance, pour une entreprise, de la mise en place d'un processus efficace de réponses aux incidents liés au système d'information, afin de les traiter et de minimiser les pertes (financières, économiques…).
Pour être plus précis dans cette étude, nous nous sommes fixé des objectifs spécifiques qui découlent de l'objectif général tels que :

- Définir l'environnement du système d'information et ses composants
- Enumérer les risques associés à cet environnement
- Analyser et évaluer les risques
    - Présentation des normes ISO 2700X
    - Présentation d'une méthode d'analyse des risques : EBIOS
- Mettre en place la cartographie de ces risques
- Donner des recommandations (dans la gestion des risques)

L'introduction massive de l'informatique signifie pour les entreprises l'automatisation possible d'une multitude d'opérations au niveau de la production mais aussi dans les bureaux, au niveau des tâches comptables et administratives. Désormais un système informatique s'installe.

Mais, on connaît depuis trois décennies une augmentation des attaques sur le système informatique portant atteinte sur les systèmes d'informations, entrainant des pertes financières importantes et de données confidentielles au niveau des entreprises. Cela nous a semblé intéressant de mener notre étude sur ces risques afin de proposer un processus de maitrise pour ces derniers. Vue l'étendue du système d'information du GIE GAINDE 2000 que nous ne pouvons pas couvrir : nous allons limiter notre étude au niveau de la direction des opérations où une grande quantité d'informations est recueillie et traitée.
L'intérêt de ce sujet est double :

- **Pour le GIE GAINDE 2000**

Cette étude pourra être bénéfique au **GIE GAINDE 2000** étant donné qu'elle va dégager une représentation structurée d'un ensemble de risques du système d'information identifiés et quantifiés. Enfin, l'étude présente de l'intérêt pour toute entreprise soucieuse d'assurer la pérennité de son SI.

- **Pour l'étudiant**

Nous trouvons intéressant de traiter un sujet du domaine de l'audit informatique ; car nous estimons que les travaux effectués sur le sujet contribueront à améliorer notre expérience dans le cadre professionnel. Ce sujet nous permettra de gérer les risques informatiques avec l'outil EBIOS (un logiciel gratuit de gestion des risques adaptable à tout type d'entreprise avec un système d'information moderne) qui n'est pas utilisé dans le cadre académique, au niveau du

Centre africain d'études supérieures en gestion (CESAG) par exemple. C'est aussi l'occasion d'approfondir l'étude sur les systèmes d'informations et la pratique de la gestion des risques.

Pour mener à bien notre travail, nous avons opté pour un plan composé de deux (2) grandes parties à savoir :

- Le cadre théorique de l'étude qui regroupe trois (3) chapitres :
    - Le premier chapitre porte sur l'environnement du système d'information ;
    - le deuxième chapitre s'intéresse à la méthodologie de gestion des risques ;
    - le troisième chapitre traite de l'approche méthodologique de la recherche qui a été utilisé.
- Le cadre pratique de l'étude c'est-à-dire la présentation, l'interprétation des résultats et la formulation des recommandations destinées à améliorer la bonne marche de l'entreprise est consignée dans les trois (3) premiers chapitres :
    - Le quatrième chapitre est consacré à la présentation globale du GIE GAINDE 2000 ;
    - le cinquième chapitre est consacré à une étude de cas pratique ou nous avons élaboré le processus de gestion des risques du SI du GIE GAINDE 2000 selon la méthode EBIOS ;
    - le dernier chapitre sera le cadre d'exposition des recommandations.

PREMIERE PARTIE :

Cadre théorique

Introduction de la première partie

Nous ne pouvons pas parler de système d'information sans au préalable définir des notions tel que l'information ou la communication qui sont des éléments clef d'une SI. Et au fil du temps, il a su s'adapter à l'environnement de plus en plus moderne et informatisé.

Donc pour mener à bien notre travail de recherche, nous avons eu recours à quelques écrits relatifs à notre sujet. Ces écrits nous permettent de voir comment les personnes qui se sont intéressées au système d'information devenu plus tard informatisé, à la gestion des risques du SI et, quelle importance elles lui accordent.

Dans cette partie, nous aborderons au cours du chapitre 1, l'environnement informatique, le système d'information, et les risques associés.

Concernant le chapitre 2, nous exposerons la mise en place du processus de gestion des risques du système d'information, nous allons présenter différentes méthodes de gestion des risques et en choisir la plus adéquate à notre sujet.

Et pour le troisième chapitre, les techniques de collecte de données ainsi qu'une méthode d'analyse seront dévoilées.

Chapitre 1 : l'environnement du système d'information.

Une entreprise crée de la valeur en traitant de l'information, en particulier dans le cas des sociétés de service. Ainsi, l'information possède une valeur d'autant plus grande qu'elle contribue à l'atteinte des objectifs de l'organisation. L'information existe sous différentes formes et types (son, image, signaux,...), elle représente la matière première du fonctionnement du système d'information.

1.1. Définition de l'information.

L'étymologie du mot information vient du latin « informare » qui désigne un processus de façonnage de l'esprit, c'est également la mise en forme des idées et l'attribution d'un sens. Découlant du verbe latin « formarer », mettre en forme, c'est donc former l'esprit pour qu'il soit à son tour capable de créer une information et de la transmettre : acte d'informer et d'éduquer. Les spécialistes en SIC (Science de l'Information et de la Communication) voient l'information comme la représentation d'une idée accompagnée d'un processus de structuration, c'est-à-dire de création et de transmission, d'où la définition de l'objet de la science de l'information qui est un « système d'échange entre différents acteurs autour d'une recherche d'information dont on veut comprendre le fonctionnement et surtout le rôle qu'y joue chaque acteur pour éventuellement intervenir dessus » (FONDIN,2001 : 116).

Selon REIX (2002 : 20) l'information est ce qui modifie notre vision du monde, qui réduit notre incertitude. L'information « crée une différence » ; c'est un renseignement au sens courant du terme.

On entend aussi parler d'information et d'informateur mais sait-on exactement ce que signifie le mot information. Selon BRETON & al. (2002 : 92), L'information est « une notion caméléonesque ». « Caméléonesque »parce qu'elle touche des domaines aussi différents les uns des autres, l'informatique, les médias, la documentation, l'économie, la société.

Mais nous retiendrons qu'une information est un renseignement qui accroit la connaissance concernant une personne, un objet ou un événement déterminé. Elle peut être :

- objective, quand elle reflète un ensemble de données porteur de sens ;
- subjective, quand elle résulte de l'interprétation d'un ensemble de données.

1.1.1. Typologie des informations.

On assiste depuis quelques années à une multiplication grandissante des différents types d'informations. Leur connaissance permet sans aucun doute de faciliter l'activité de veille dans l'entreprise. Le défrichage de la « jungle informationnelle » s'avère comme une phase préliminaire dans le processus de mise en place du dispositif d'observation et de surveillance de son environnement.

- **L'information formelle et informelle.**

Selon BREILLAT (2007 : 7) Parmi la masse d'informations économiques en circulation, on distingue les informations dites "formelles" des informations dites "informelles". Les sources d'informations formelles sont toujours inscrites sur un support qu'il soit papier, filmographique ou informatique. Entre la presse spécialisée, la télévision, la radio, les banques de données, les brevets, les informations légales et les études publiées.

Selon MARTINET & al. (1995 : 23), Pour collecter l'information informelle, « il faut être « au contact » c'est-à-dire se déplacer, passer du temps, pouvoir entendre, sentir, toucher, de manière à la percevoir ». Cette information est souvent recueillie oralement. Elle est qualitative et exige des recoupements avec d'autres informations et des analyses approfondies pour pouvoir être suffisamment utiles à l'entreprise. Elle comprend :

- l'information de type « floue » ;
- l'information de type expertise ;
- l'information de type foires et salons.

- **Rôle de l'information dans l'entreprise.**

L'information a un rôle essentiel dans le processus de prise de décision tant au niveau des décisions opérationnelles quotidiennes qu'au niveau des grandes décisions stratégiques.

Il existe deux situations devant lesquelles chaque collaborateur peut se retrouver :

- l'excès d'information c'est-à-dire une abondance, difficulté à discerner les degrés d'importance ;
- le déficit d'information pertinente et réellement nécessaire qui peut souvent être masquée par le défaut précédent.

1.2.La communication.

Les relations humaines se situent dans le champ de la communication. Chaque personne, chaque plante, chaque animal et chaque objet émet des signaux qui, lorsqu'ils sont perçus, transmettent un message au récepteur. Ces messages modifient l'information de celui qui les perçoit et peuvent en conséquence modifier son comportement. Le changement de comportement du récepteur, à son tour, peut influencer l'émetteur d'une façon perceptible ou non.

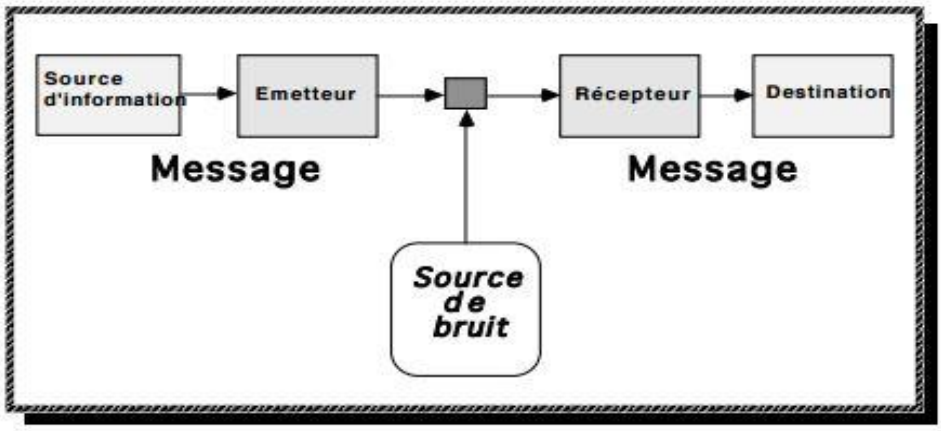
1.2.1. Définition de la communication.

« Le système de communication est un ensemble organisé d'éléments permettant une communication. Il comprend les éléments de base suivants : un émetteur, un récepteur, un message et un canal véhiculant le message jusqu'au récepteur. » (LENDREVIE & al. 2008 : 24).

La communication est la manière dont l'information circule dans l'entreprise. Elle s'effectue à travers un réseau de communication qui comporte au moins un émetteur, un canal de transmission et un destinataire. L'émetteur utilise un langage, c'est à dire un ensemble de symboles (mots, nombres) qui ont une signification commune pour l'ensemble des participants à la communication et désignent la même réalité.

Le canal de transmission nécessite un codage dans un langage particulier utilisé par ce canal. Et à la réception, la compréhension du message exige un décodage c'est à dire une traduction du langage du canal dans le langage du destinataire.

Figure 1: système de communication.



Source : SHANNON & al. (1975 : 69)

1.2.2. Collecte et traitement de l'information.

Selon le Club des contrôleurs de gestion des ministères économiques et financiers (2013 :4) la collecte et le traitement des données s'effectuent en 5 grandes étapes, à adapter au contexte de la demande :

- **Lancement de la collecte.**

Il s'agira de communiquer auprès des contributeurs : objectifs de la collecte, nature des données demandées, circuits de transmission des données et échéance(s) associée(s), aide disponible.

- **Suivi de la collecte et relances.**

Pour le suivi il faudra répondre aux questions des contributeurs, relancer les non-répondants et informer régulièrement le commanditaire de l'état d'avancement.

- **Contrôle de cohérence et corrections éventuelles.**

Il conviendra de vérifier la cohérence et la qualité des données de base, et les corriger si nécessaire (apporter soi-même les corrections en informant au préalable les contributeurs de toute modification intégrée, ou faire corriger les données).

- **Exploitation, mise en forme et analyse.**
    - Exploiter les données (calculs, pondération etc.) ;
    - produire le « livrable » final sous le format attendu par le commanditaire ;
    - rédiger une analyse si nécessaire (selon les besoins préalablement
    - définis).
- **Validation finale.**
    - Transmettre au commanditaire le « livrable » attendu, pour validation ;
    - Apporter les corrections éventuelles.

1.3. Le système information.

Une entreprise crée de la valeur en traitant de l'information, en particulier dans le cas des sociétés de service. Ainsi, l'information possède une valeur d'autant plus grande qu'elle contribue à l'atteinte des objectifs de l'organisation. Nous verrons ci-dessous la définition d'un système d'information ainsi que ses caractéristiques.

1.3.1. Définition et caractéristiques.

Selon MARIE & al (2003 : 5) un système d'information peut se définir comme un ensemble organisé des procédures pour collecter, traiter, stocker et communiquer des informations permettant de prendre des décisions et contrôles.

Ces définitions mettant en avant les aspects prise de décision et communication montrent la place que peut avoir le SI dans le management des organisations. Le SI n'est pas une simple composante technique mais fait partie intégrante de la stratégie de l'organisation.

Certains auteurs citent J.-L. PEAUCELLE pour leur définition du système d'information :

« Le Système d'Information (SI) peut être défini comme un langage servant à représenter de manière fiable et économique des aspects de l'activité de l'organisation. » (MARCINIAK & al. 2000 : 7)

Les auteurs retiennent donc du SI son côté de "mémoire" collective, de mémoire de l'organisation, ne servant qu'à retranscrire la réalité. Ce n'est donc pas à leurs yeux un élément central de l'organisation, un élément sur lequel l'organisation peut s'appuyer ou se construire autour. Toutefois, et c'est une des fonctions du SI, les auteurs retiennent que le SI est la représentation de l'organisation.

REIX& al. (2002 : 11) ont donné la définition suivante : Un système d'information est un ensemble d'acteurs sociaux qui mémorisent et transforment des représentations via des technologies de l'information et des modes opératoires.

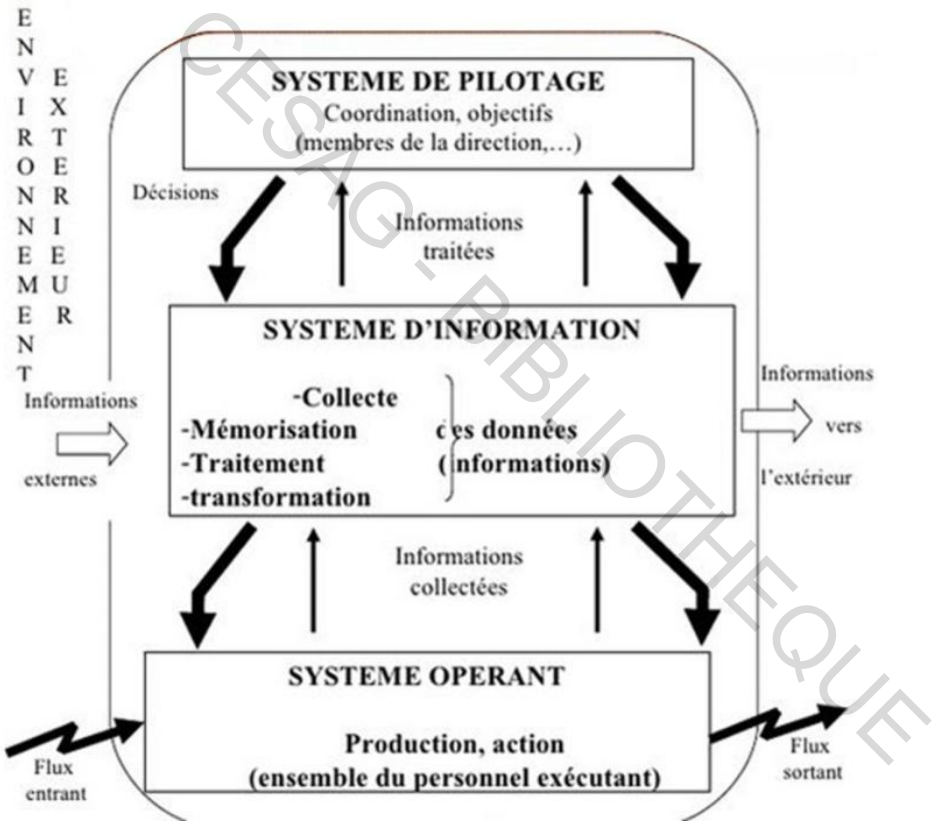
Ici, les auteurs se focalisent sur la partie humaine et de mémorisation collective de l'organisation. Cependant, il est abordé ici le fait que le SI est également un système technique, voire technologique. Nous choisissons de différencier clairement les techniques de traitement de l'information, des technologies de l'information. Le second terme évoquant chez nous un côté matériel, voire de machines, alors que le premier revêt un côté de procédure.

Selon une approche systématique d'une entreprise ou de tout autre organisme, « le système d'information d'une entreprise est un réseau complexe de relations structurées où interviennent des hommes, des machines et des procédures, qui a pour objet d'engendrer des flux ordonnés d'informations pertinentes, provenant de sources internes et externes à l'entreprise et destinées à servir de base aux décisions. »(LAMBIN, 1990 : 26)

Selon cette approche, nous pouvons distinguer trois (3) composantes :

- Le système opérant : chargé de la réalisation des tâches d'exécution répondant à la finalité de l'entreprise (établissement de documents administratifs) ;
- le système de pilotage : prise de décision, fixation des objectifs et des moyens (peut exister à tous les niveaux hiérarchiques de l'entreprise) ;
- le système d'information : intermédiaire entre les deux précédents, il est chargé de véhiculer l'information interne et externe.

Figure 2: le système d'information et ces composantes.



Source : LEMOIGNE (2010 :19)

- Flux physique d'entrée : matières premières, flux financiers ;
- flux physique de sortie : produits finis ;
- les informations entre le système de pilotage et le système opérant sont véhiculées par un troisième système appelé système d'information.

« Un système d'information est un ensemble organisé de ressources : matériel, logiciel, personnel, données, procédures... permettant d'acquérir, de traiter, de stocker des informations (sous forme de données, textes, images, sons, etc...) par des organisations. » (REIX, 2011 : 3).

Cette définition plus complète qu'elle soit, nous paraît être la plus proche du sujet que nous traitons.

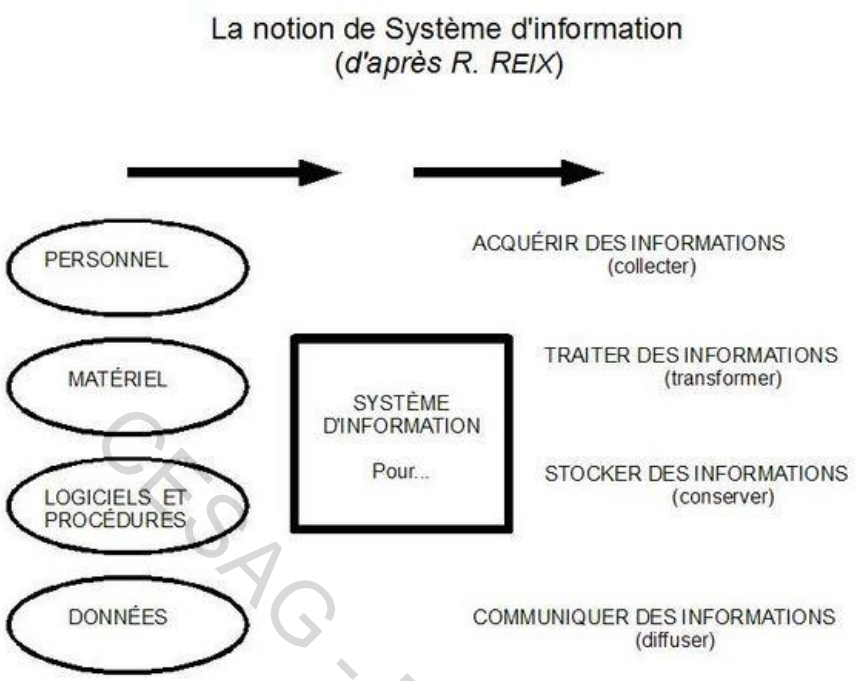
R. REIX propose aussi un schéma du système d'information, nous le reproduisons ici, car il complète efficacement la définition ci-dessus

Il ne doit pas être confondu avec un système informatique qui est un ensemble organisé de ressources (matériel, logiciel, personnel données, procédures…) permettant d'acquérir, de stocker, de communiquer des informations sous forme de données, textes, images, sons dans les organisations.

Mais il existe une relation entre un système d'information et un système informatique.

Selon GERMAK (2013 : 3) il existe bien de nos jours une relation étroite entre système d'information et informatique. Cependant, il ne s'agit pas d'une relation d'identité mais d'une relation de type demande et offre. Il existe dans les organisations des besoins de traiter des informations pour permettre à l'organisation d'être efficace et de se développer. L'informatique peut offrir des outils permettant de satisfaire ces besoins d'une manière adaptée. La relation entre les deux est donc de type maîtrise d'ouvrage et maîtrise d'œuvre ou client à fournisseur. Cela aura des incidences très importantes qui feront l'objet d'une partie conséquente de cet ouvrage.

Figure 3 : schéma du système d'information.



Source : REIX (2011 : 3)

S'agissant des caractéristiques du SI, elles suivront l'idée d'une dématérialisation des procédures : cœur du SI. Et pour venir à cette dématérialisation, il faudra :

- Utiliser des moyens informatiques (progiciels, logiciels, etc.), électroniques (serveurs, ordinateurs, etc.)et des télécommunications ;
- Automatiser et dématérialiser les opérations telles que les procédures d'entreprise;
- Mettre en lieu et place des moyens classiques tels que les formulaires sur papier et le téléphone.

1.3.2. La fonction système d'information.

Selon AUTISSIER et al (2008 :48) le système d'information traite de l'utilisation de la technologie informatique en entreprise. C'est une fonction à part entière qui a en charge trois points :

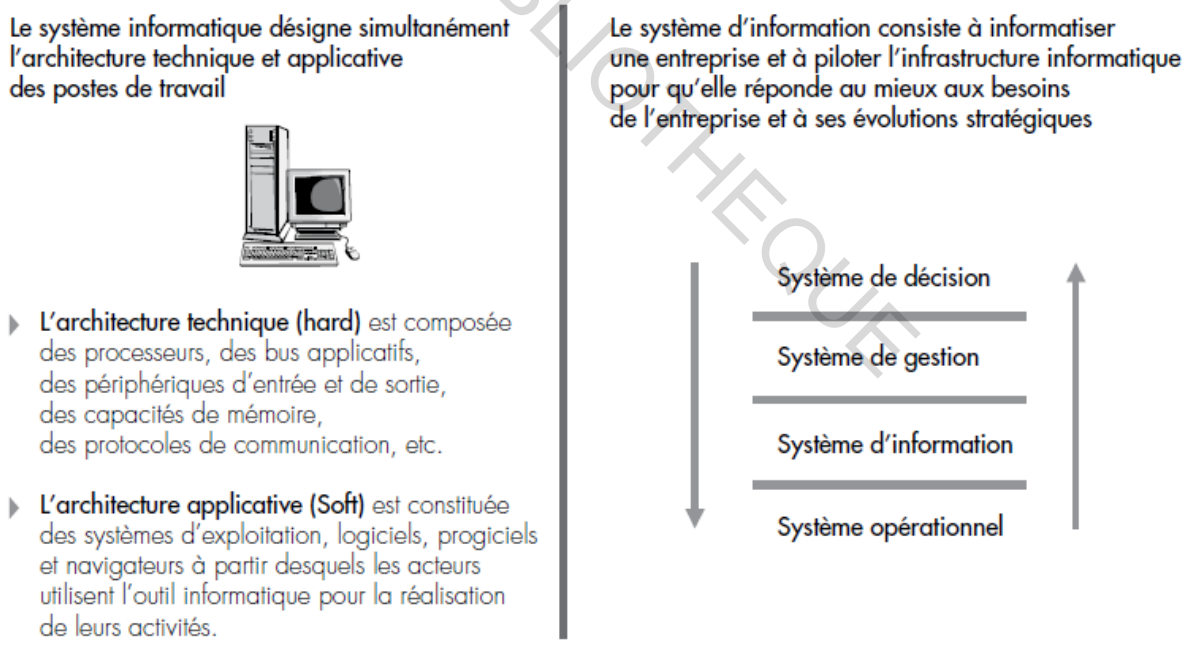
- La stratégie des systèmes d'information: quels sont les besoins de l'organisation en matière d'informatique, en fonction de son activité et de ses stratégies ?

- Le déploiement des systèmes d'information: comment réussir les projets informatiques ?
- L'exploitation du système d'information: comment suivre la disponibilité du parc informatique et télécom, et la performance des applications de l'entreprise ?

Le système d'information traite de l'installation et de l'utilisation de la technologie informatique pour la réalisation des activités d'une organisation. L'informatique est la technologie gérée par le système d'information, mais il existe une différence entre ces deux notions :

- Le système d'information fait le lien entre la technologie informatique et le fonctionnement d'une entreprise ;
- l'informatique, quant à elle, désigne des machines (ordinateurs, réseaux) et des logiciels. La compétence informatique consiste à maîtriser à la fois la technicité des matériels et des langages de programmation et/ou le paramétrage des logiciels.

Figure 4 : informatique et système d'information.



Source : AUTISSIER & al. (2008 :48)

« Que fait une personne qui occupe un poste en système d'information ? Quelles sont ses productions au quotidien dans le cadre de son activité ? Pour répondre à ces questions, nous avons regroupé les principales pratiques de la fonction en trois parties :

- Les pratiques liées aux projets d'informatisation ;
- les pratiques liées au pilotage des TIC ;
- les pratiques liées à la gestion de la technologie informatique. » (AUTISSIER & al. 2008 :48)

- **Les pratiques liées aux projets d'informatisation**

Le déploiement de projets informatiques occupe, en général, une grande partie du temps de travail des personnes en système d'information. Les tâches confiées sont très différentes en fonction des projets, des technologies déployées et des entreprises.

- **Les pratiques liées au pilotage du SI**

Une fois installées, les technologies informatiques, sous forme d'infrastructures matérielles et d'applications, nécessitent d'être pilotées au regard de leurs performances opérationnelles et de leur intégration comme levier de la stratégie générale de l'entreprise.

- **Les pratiques liées à la technologie informatique**

Ces pratiques sont à la frontière entre la compétence SI et la compétence informatique. Celui qui occupe un poste en système d'information n'est pas un technicien de l'informatique, mais il est nécessaire qu'il en maîtrise les principales caractéristiques pour faire en sorte de gérer au mieux les projets d'informatisation.

1.4. Les systèmes d'information électroniques.

«A l'heure du commerce électronique des réseaux, des progiciels de gestion intégré, de la relation client et du décisionnel, aucune entreprise ne peut s'affranchir d'un plan d'évolution de son système d'information et de ses structures» (ROWE, 2002:259)

On appelle système d'information électroniques, l'ensemble des moyens et méthodes se rapportant aux traitements automatisés des données de l'organisation. Il se compose de matériels, logiciels et de réseaux de communication.
L'informatique est l'un des moyens privilégiés qui permet d'apporter au système d'information un accroissement des performances de traitement, de mémorisation, de recherche d'informations et de restitution de celles-ci sous différentes formes (écran, fichier, papier).

On dispose entre autre de moyens techniques permettant de traiter et transmettre de façon automatisée une partie de ces informations et, de méthodes permettant de gérer l'ensemble des informations automatisées.

Nous verrons successivement ces deux moyens qui ont apporté une grande évolution des systèmes d'information des entreprises.

1.5. La méthode MERISE.

« Merise est un acronyme signifiant Méthode d'Étude et de Réalisation Informatique par les Sous-ensembles ou pour les Systèmes d'Entreprise. La méthode Merise a comme objectif d'aider, de guider les Ssii, dans leurs phases d'analyses, de conception et le développement de l'applicatif. Nous devons la création, l'étude et la mise en place de cette méthode à une équipe de chercheurs et d'ingénieurs aixois (JeanLouis le Moigne, Hubert Tardieu, Dominique Nancy, Henry Heckenroth, Daniel Pasco, Bernard Espinasse) qui en posèrent les bases dans le milieu des années 1970.

La méthode Merise présente comme avantage indéniable de permettre une définition claire et précise de l'ensemble du Système d'Information et d'en définir correctement le périmètre. » (BAPTISTE, 2012 :3)

1.5.1. Présentation générale de la méthode Merise.

Selon BAPTISTE (2012 :2) la méthode Merise se caractérise par :

- Une approche systémique en ayant une vue de l'entreprise en terme de systèmes ;
- une séparation des données (le côté statique) et des traitements (le côté dynamique) ;
- une approche par niveaux.

1.5.1.1. La systémique.

La définition du Larousse semble plus explicite : « Combinaison de parties qui se coordonnent pour concourir à un résultat, de manière à former un ensemble ».Tout système fonctionne en transformant des flux d'entrée en flux de sortie selon des processus plus ou moins complexes. » (BAPTISTE ,2012 :6).

1.5.1.1.1. Les caractéristiques d'un système.

Un système est un élément fini dont le périmètre est une frontière qui le sépare de son environnement. Il interagit avec son environnement grâce à des flux d'informations entrantes, qu'il va traiter et restituer à l'environnement sous forme de flux d'informations sortantes.
Le système va générer des informations qui rendent compte de son comportement à la fois au sein de l'environnement, mais aussi pour son propre compte. Un système communique. Un système a besoin, pour prendre des décisions, de stocker et de traiter des informations.

1.5.1.1.2. La représentation schématique des systèmes de l'entreprise.

Selon BAPTISTE (2012 : 5) si nous reprenons l'analogie anatomique, et si nous comparons l'entreprise à un corps humain, nous pouvons réduire l'entreprise à un cerveau qui pilote, un muscle qui opère et des nerfs qui font transiter les informations.

- **Le système de pilotage**

Le système de pilotage définit les missions et les objectifs, organise l'emploi des moyens, contrôle l'exécution des travaux. Il assigne des objectifs à l'organisation, analyse l'environnement et le fonctionnement interne à l'organisation, contrôle le système opérant. Il est relié aux autres systèmes par des flux d'informations internes.

- **Le système d'information**

Le système d'information est l'ensemble des ressources humaines, techniques et financières qui fournissent, utilisent, compilent, traitent et distribuent l'information de l'organisation. Il alimente l'organisation en informations d'origines diverses (internes ou externes). Il est la passerelle obligatoire pour toutes les informations de l'entreprise.

- **Le système opérant**

Le système opérant est l'ensemble des moyens humains, matériels, organisationnels qui exécutent les ordres du système de pilotage. Il assure le fonctionnement du système global, son activité est contrôlée par le système de pilotage.

1.5.1.2. La séparation des données et des traitements.

Elle comporte 2 parties : les données et les traitements.

- **Les données (ou informations)**

Selon BAPTISTE (2012 :7) l'information est l'émission ou la réception de signaux oraux ou écrits, sonores, visuels ou multimédias dont le but est de déclencher les processus alimentant l'échange, base naturelle et indispensable de l'animation de l'organisation.

- **Les traitements**

Ils sont collectés comme les informations via un processus d'interview et d'étude des documents. Ils peuvent être de deux sortes :

- automatiques ;
- manuels.

Ils sont déclenchés par l'arrivée d'évènements. La gestion des traitements sert à identifier les fonctionnalités selon une approche qui va du général au particulier et qui définit leur découpage et leur enchaînement.

1.5.1.3. MERISE, Une approche par niveaux.

Pour BAPTISTE (2012 :9) la conception d'un SI, il est nécessaire de considérer quatre niveaux d'étude :

- Le niveau conceptuel ;
- le niveau organisationnel ;
- le niveau logique ;
- le niveau physique.

- **Le niveau conceptuel**

Le niveau conceptuel consiste à concevoir le SI en faisant abstraction de toutes les contraintes techniques ou organisationnelles et cela tant au niveau des données que des traitements.
Le niveau conceptuel répond à la question Quoi ? (le quoi faire, avec quelles données).
Le formalisme Merise employé sera :

- Le Modèle Conceptuel des Données (MCD) ;
- le Modèle Conceptuel des Traitements (MCT).

- **Le niveau organisationnel**

Le niveau organisationnel a comme mission d'intégrer dans l'analyse les critères liés à l'organisation étudiée. Le niveau organisationnel fera préciser les notions de temporalité, de chronologie des opérations, d'unité de lieu, définira les postes de travail, l'accès aux bases de données…

Les questions posées, au niveau des traitements, sont :

- Qui ?
- Où ?
- Quand ?

Le formalisme Merise employé sera :

- Le Modèle Organisationnel des Données (MOD) ;
- le Modèle Organisationnel des Traitements (MOT).

- **Le niveau logique**

Le niveau logique est indépendant du matériel informatique, des langages de programmation ou de gestion des données. C'est la réponse à la question Avec quoi ?

Le formalisme sera :

- Le Modèle Logique des Données (MLD) ;
- le Modèle Logique des Traitements (MLT).

- **Le niveau physique**

Le niveau physique permet de définir l'organisation réelle (physique) des données. Il apporte les solutions techniques, par exemple sur les méthodes de stockage et d'accès à l'information. C'est la réponse au Comment ?

Le formalisme employé sera :

- Le Modèle Physique des Données (MPD) ;
- le Modèle Opérationnel et physique des Traitements (MOpT).

Ainsi cette modélisation peut se faire dans ce tableau ci-après :

Tableau 1 : récapitulatif de l'approche par niveaux-MERISE.

NIVEAUX	DONNEES	TRAITEMENTS
Conceptuel	Modèle Conceptuel des Données	Modèle Conceptuel des Traitements
Organisationnel	Modèle Organisationnel des Données	Modèle Organisationnel des Traitements
Logique	Modèle Logique des Données	Modèle Logique des traitements
Physique	Modèle Physique des Données	Modèle Opérationnel et Physique des Traitements

Source : BAPTISTE (2012 : 10)

1.6. Les risques liés au système d'information.

Le lieu de travail est devenu un lieu à risques multiples. Le SI est le plus souvent ciblé alors qu'étant une roue motrice dans l'activité de l'entreprise. Les risques se présentent comme tels :

Tableau 2 : les risques liés au SI.

Types	Descriptions
Risques induits par les systèmes construits pour les métiers	Défaut de confidentialité, erreurs, indisponibilité, manque d'audibilité, infractions réglementaires.
Risques induits par les infrastructures informatiques	Indisponibilité
Risques induits par les activités des informaticiens	Erreurs, malveillance
Risques par les bâtiments	Malveillance liée à des défauts de sécurité physique, accidents (incendie)
Risques induits par le niveau de performance économique de l'informatique et la stratégie	Défaut d'agilité des métiers, excédent de charges, mauvais alignement stratégique
Risques découlant de l'exécution des projets	Non-conformité des livraisons, retard

Source : Manuel EBIOS bases de connaissances

1.6.1. L'origine des risques.

Elle peut être de source humaine ou technique.

Les risques humains sont les plus importants, même s'ils sont le plus souvent ignorés ou minimisés. Ils concernent les utilisateurs mais également les informaticiens eux-mêmes.

Les risques techniques sont tout simplement ceux liés aux défauts et pannes inévitables que connaissent tous les systèmes matériels et logiciels.

Ces incidents sont évidemment plus ou moins fréquents selon le soin apporté lors de la fabrication et des tests effectués avant que les ordinateurs et les programmes ne soient mis en service. Cependant, les pannes ont parfois des causes indirectes, voire très indirectes, donc difficiles à prévoir.

Avec la méthode EBIOS, les sources de menaces représentent une typologie des choses ou personnes à l'origine des risques. On distingue les sources par :

- leur origine humaine ou non humaine ;
- leur facilité d'accès au sujet de l'étude (interne ou externe) ;
- dans le cas de sources humaines :
    - leur caractère intentionnel ou accidentel ;
    - leurs capacités (force intrinsèque, selon leurs ressources, expertise, dangerosité…) ;
- dans le cas de sources non humaines :
    - Leur type (naturelle, animale, contingence…).

Chaque type de source de menace fait l'objet d'exemples, qui figurent en italique.

Tableau 3 : les différentes sources de menaces du système d'information.

Type de source	description
Sources humaines agissant de manière délibérée	Personnes ou groupes de personnes mal intentionnées, qu'elles soient physiques ou morales, et qui peuvent être à l'origine de risques. Elles peuvent être internes ou externes au sujet de l'étude. Leurs capacités (force intrinsèque) dépendent principalement de leurs ressources, de leur expertise et du

	temps qu'elles peuvent accorder. Leur motivation peut être le jeu, la cupidité, la vengeance, une idéologie, le chantage, l'égo, la recherche d'un avantage concurrentiel, le terrorisme…
Source humaine interne, malveillante, avec de faibles capacités	*Collaborateur malveillant avec des possibilités d'action limitées sur le système d'information (personnel en fin de contrat ou voulant se venger de son employeur ou de ses collègues…), stagiaire* *agissant de manière ludique, client désirant obtenir des avantages, personnel d'entretien.*
Source humaine interne, malveillante, avec des capacités importantes	*Collaborateur malveillant avec d'importantes connaissances et possibilités d'action sur le système d'information (manager ambitieux en fin de contrat ou voulant se venger de son employeur ou de ses collègues, développeur agissant par égo ou de manière ludique, fraudeur, actionnaires…), sous-traitant ou prestataire, personnel de maintenance ou d'assistance à distance.*
Source humaine interne, malveillante, avec des capacités illimitées	*Collaborateur malveillant avec des connaissances et possibilités d'action illimitées sur le système d'information (administrateur système ou réseau agissant par vengeance, dirigeant…).*
Source humaine externe, malveillante, avec de faibles capacités	*Script-kiddies, vandale.*
Source humaine externe, malveillante, avec des capacités importantes	*Militant agissant de manière idéologique ou politique, pirate passionné, casseur ou fraudeur, ancien employé désirant se venger d'un licenciement, concurrent, groupement professionnel, organisation de lobbying, syndicat, journaliste, organisation non gouvernementale.*
Source humaine externe, malveillante, avec des capacités illimitées	Organisation criminelle, agence gouvernementale ou organisation sous le contrôle d'un État étranger, espions, organisation terroriste.
Sources humaines agissant de manière accidentelle	Personnes ou groupes de personnes sans intention de nuire, qu'elles soient physiques ou morales, et qui peuvent être à l'origine de risques. Ceci comprend tout type d'activités humaines. Elles peuvent être internes ou externes au sujet de l'étude. Leurs capacités

	(force intrinsèque) dépendent principalement de leurs ressources, de leur expertise et du temps qu'elles peuvent accorder. Leur action involontaire peut être due à une faute d'attention, à une erreur de manipulation, à un manque d'investissement, à la malchance…
Source humaine interne, sans intention de nuire, avec de faibles capacités	Collaborateur maladroit ou inconscient avec des possibilités d'action limitées sur le système d'information, personnel à faible conscience d'engagement, peu sensibilisé ou peu motivé dans sa relation contractuelle avec l'organisme, personnel d'entretien maladroit, stagiaire, thésard, intérimaire, utilisateur, fournisseur, prestataire, sous-traitant, client, actionnaires.
Source humaine interne, sans intention de nuire, avec des capacités importantes	*Collaborateur maladroit ou inconscient avec d'importantes connaissances et possibilités d'action sur le système d'information (manager, développeur…).*
Source humaine interne, sans intention de nuire, avec des capacités illimitées	*Collaborateur maladroit ou inconscient avec des connaissances et possibilités d'action illimitées sur le système d'information (administrateur système ou réseau, dirigeant…).*
Source humaine externe, sans intention de nuire, avec de faibles capacités	*Entourage du personnel, personne réalisant des travaux dans le voisinage, manifestants, visiteur maladroit, forte ambiance sonore.*
Source humaine externe, sans intention de nuire, avec des capacités	*Matériels émettant des ondes, des vibrations, activités industrielles dégageant des substances chimiques toxiques ou susceptibles de provoquer des sinistres mineurs, trafic routier ou aérien pouvant générer des accidents.*
Source humaine externe, sans intention de nuire, avec des capacités illimitées	*Matériels émettant des radiations ou des impulsions électromagnétiques, activités industrielles susceptibles de provoquer des sinistres majeurs, explosion dans le voisinage.*

Source : Manuel EBIOS bases de connaissances version 25 janvier 2010. Pages15-16

1.6.2. Les conséquences des risques.

Vis-à-vis des entreprises et des projets, l'impact des risques du système d'information a des répercussions sur deux (2) grands domaines.

- **Le domaine opérationnel**

Le dysfonctionnement du système d'information de par la dégradation des supports électroniques qui lui sont affecté généralement pour conséquence un arrêt ou un ralentissement de la production de l'entreprise, même si son activité n'est pas directement ou uniquement basée sur un processus informatique.

- **Le domaine financier**

« En avril 2011, le piratage du Playstation Network de Sony a eu un impact énorme sur l'image de la société avec une perte de données pour plus de 77 millions d'utilisateurs (informations bancaires et personnelles). Celle-ci a engendré plusieurs milliards de dollars de pertes et un grand nombre d'actions en justice a été engagé contre Sony. La firme japonaise a du dédommager de nombreux utilisateurs, ce qui a encore accru la perte financière suite à cette attaque » (TIRATAY, 2013)

Cet article illustre le vol de données pouvant engendrer des pertes financières importantes.

Tout au long de ce chapitre nous a pu présenter les différentes définitions des notions qui tournent autour du système d'information et des risques liés à ce dernier. Au terme de ce chapitre, nous pouvons dire qu'un système d'information est un ensemble organisé de ressources par l'entreprise. Le chapitre suivant sera consacré à la mise en place d'un processus de gestion des risques du système d'information.

Chapitre 2 : Mise en place d'un processus de gestion des risques du système d'information.

La survenance d'un événement d'origine interne ou externe peut avoir des répercussions sur l'atteinte des objectifs. Les événements peuvent avoir un impact négatif, positif ou les deux à la fois. Les événements ayant un impact négatif constituent des risques. Toute activité économique est porteuse de risques qui peuvent mettre en péril l'entreprise, son fonctionnement, sa rentabilité, son développement ou sa pérennité. Devant cette présence continue de risques, le rôle du chef d'entreprise est d'identifier les risques encourus par son entreprise, d'évaluer leurs conséquences ainsi que leur gravité et, de mettre en œuvre des actions visant à les maitriser du mieux possible

Ainsi, au cours de ce chapitre, nous allons définir la notion de risques, puis donner ses caractéristiques et ensuite présenter la mise en place du processus de gestion des risques.

2.1. Définition d'un risque.

«Etymologiquement, le mot risque vient du latin *risicare,* qui signifie doubler un promontoire. Cette origine, qui montre la prise de conscience dès l'antiquité des difficultés de la navigation Commerciale, est donc souvent attribuée à l'assurance maritime. » (LAFITTE 2003 :96)

Mais aussi selon l'IFACI (2007 : 23) le risque représente la possibilité qu'un événement survienne et nuise à l'atteinte des objectifs. Exemple : panne, incendies, perte de crédit.

Selon la norme ISO 17799 le risque est défini comme suit :

$$\text{Risque} = \frac{\text{Menace} \times \text{vulnérabilité}}{\text{Contre mesure}}$$

La menace (en anglais « threat ») représente le type d'action susceptible de nuire dans l'absolu, tandis que la vulnérabilité (en anglais « vulnerability », appelée parfois faille ou brèche) représente le niveau d'exposition face à la menace dans un contexte particulier. Enfin la contre-mesure est l'ensemble des actions mises en œuvre en prévention de la menace.

Les contre-mesures à mettre en œuvre ne sont pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un ensemble de règles clairement définies.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'ennemi.

2.1.1. Mesure du risque.

Selon BARTHELEMY & al. (2004 :11) nos activités génèrent directement certains risques. On les qualifiera d'endogènes. D'autres naissent dans notre environnement et nous affectent par contrecoup. On les appellera exogènes. Un risque se caractérise donc par deux grandeurs :

- Sa probabilité d'occurrence, ou fréquence **f** ;
- ses effets, ou gravité **G**.

Un risque se mesure par le produit de ces deux grandeurs, sa criticité **C** :

$$C = f \times G$$

2.2. Mise en place d'un processus de gestion des risques.

« Gérer les risques, c'est répondre à nos préoccupations par rapport au futur, ce qui revient à prendre en comptes la totalité du spectre des risques auxquels une entreprise est et sera confronté. Le dilemme est donc clair : la gestion des risques implique des éléments importants d'incertitudes précisément parce qu'elle requiert que nous anticipions l'avenir et regardions vers l'avant, bien au-delà de ce que nous savons du passé et du présent. » (CLEARY & al. 2006 : 63)

Un constat : à peine la moitié des entreprises évaluent l'ensemble de leurs risques tous les ans. Or certains experts sont formels : seule une stratégie globale des risques, bien maîtrisée et régulièrement actualisée, permet de gérer le développement de l'entreprise et d'assurer sa pérennité. C'est dire que les nouveaux risques, tout comme les anciens, doivent être préalablement identifiés et gérés, sous peine de mettre en danger l'entreprise. En effet, les risques peuvent altérer gravement sa performance. Il faut donc comprendre et prévenir ces risques avant les autres afin de ne pas perdre un avantage concurrentiel. Plus que jamais, la prévention doit être le maître-mot. « Car le temps et l'argent consacrés à entrevoir l'occurrence de risques seront toujours infiniment moindres que le temps et l'argent dépensés pour en réparer les dégâts » (DUCRET, 2012).

Donc il est très important de mettre en avant la nécessité de mettre en œuvre des procédures internes afin de faire face à des risques potentiels ou avérés de non-continuité des activités :

Quelle que soit la typologie des risques, il est essentiel de mettre en place des solutions pour que l'entreprise ne soit pas fragilisée.

2.2.1. Définition du processus de gestion du risque.

« La gestion est la mise en œuvre de moyens humains et matériels d'une organisation pour atteindre des objectifs préalablement fixés. La croissance des bureaucraties professionnelles dans nos sociétés a transformé l'appareil administratif d'organisations en une puissante machine de gestion des organisations dont les opérations visent l'efficacité et la prévisibilité dans l'atteinte de ses objectifs. » (ANDRE-LEGER, 2013 : 31).

Selon ROWE (2002 : 281) la gestion du risque consiste soit à réduire la probabilité d'occurrence d'évènement indésirables soit à en réduire l'impact s'ils devaient survenir.

La gestion des risques a pour but de créer un cadre de référence aux entreprises afin d'affronter efficacement le risque et l'incertitude. Le processus d'identification, d'évaluation et de gestion des risques fait partie du développement stratégique de l'entreprise et doit être conçu et planifié au plus haut niveau, soit au conseil d'administration. Une approche intégrée de la gestion des risques doit évaluer, contrôler et faire le suivi de tous les risques auxquels l'entreprise est exposée.

Elle est définie par l'ISO comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. On dégage en général trois finalités à la gestion des risques pour les SI :

- Améliorer la sécurisation des systèmes d'information ;
- justifier le budget alloué à la sécurisation du système d'information ;
- prouver la crédibilité du système d'information à l'aide des analyses effectuées.

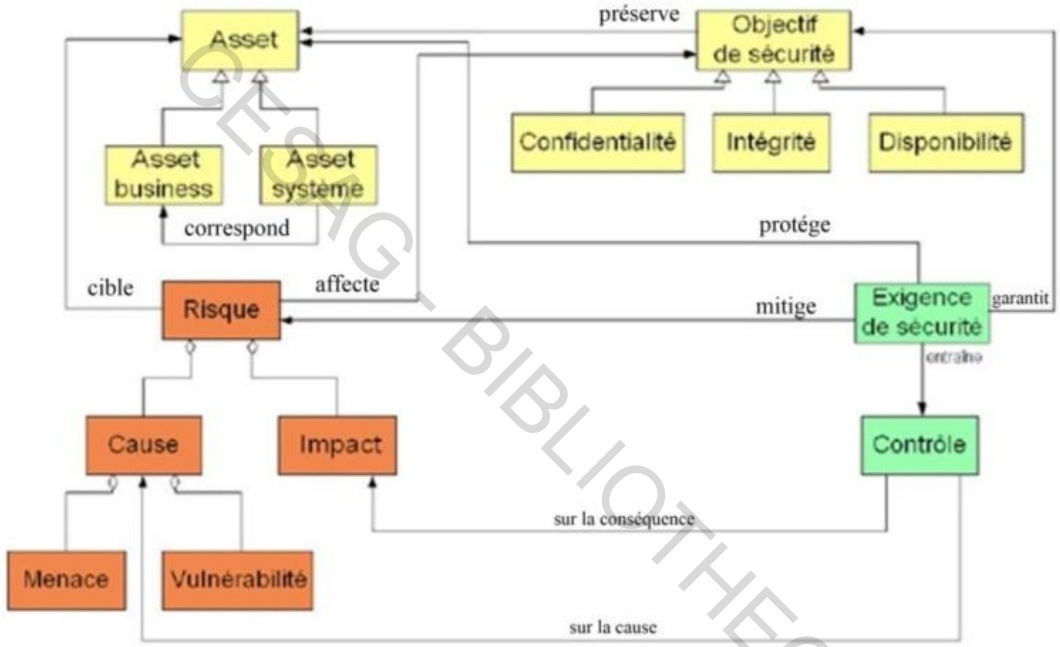
2.2.2. Fondements.

Pour bien appréhender la gestion des risques, ses objectifs et ses limites, il est nécessaire de comprendre en premier lieu les concepts sous-jacents et le processus employé.

2.2.2.1. Concepts des gestions des risques.

La gestion des risques, « dans son plus simple appareil », se compose de trois blocs interdépendants. Nous distinguons l'organisation cible de l'étude, définie par ses Assets « Asset désigne tout élément représentant de la valeur pour l'organisme » (ISO/IEC 13335-1:2004) et ses besoins de sécurité, puis les risques pesant sur ces assets et enfin les mesures prises ayant pour but de traiter les risques et donc d'assurer un certain niveau de sécurité.

Figure 5 : les concepts de la gestion des risques.



Source : MAYER & al. (2006 : 2)

Les assets sont définis comme étant l'ensemble des biens, actifs, ressources ayant de la valeur pour l'organisme et nécessaires à son bon fonctionnement. On distingue ici les assets du niveau business des assets liés au SI. Du côté des assets business, on retrouve principalement des informations (par exemple des numéros de carte bancaire) et des processus (comme la gestion des transactions ou l'administration des comptes). Les assets business de l'organisme sont bien souvent entièrement (ou presque) gérés au travers du SI, ce qui entraîne une dépendance de ces assets vis-à-vis de ce dernier. Qu'on appelle aussi les "assets système ".

On retrouve dans les assets système les éléments techniques, tels les matériels, les logiciels et les réseaux, mais aussi l'environnement du système informatique, comme les utilisateurs ou

les bâtiments. C'est cet ensemble qui forme le SI. Le but de la gestion des risques est donc d'assurer la sécurité des assets, sécurité exprimée la plupart du temps en termes de confidentialité, intégrité et disponibilité, constituant les objectifs de sécurité.

Pour bien comprendre la notion de risque, il est important de se pencher sur chacune de ses composantes. Tout d'abord la menace, la source du risque, est l'attaque possible d'un élément dangereux pour les assets. C'est l'agent responsable du risque. Ensuite, la vulnérabilité est la caractéristique d'un asset constituant une faiblesse ou une faille au regard de la sécurité. Enfin l'impact représente la conséquence du risque sur l'organisme et ses objectifs. La menace et la vulnérabilité, représentant la cause du risque, peuvent être qualifiées en termes de potentialité. L'impact peut, quant à lui, être qualifié en termes de niveau de sévérité.

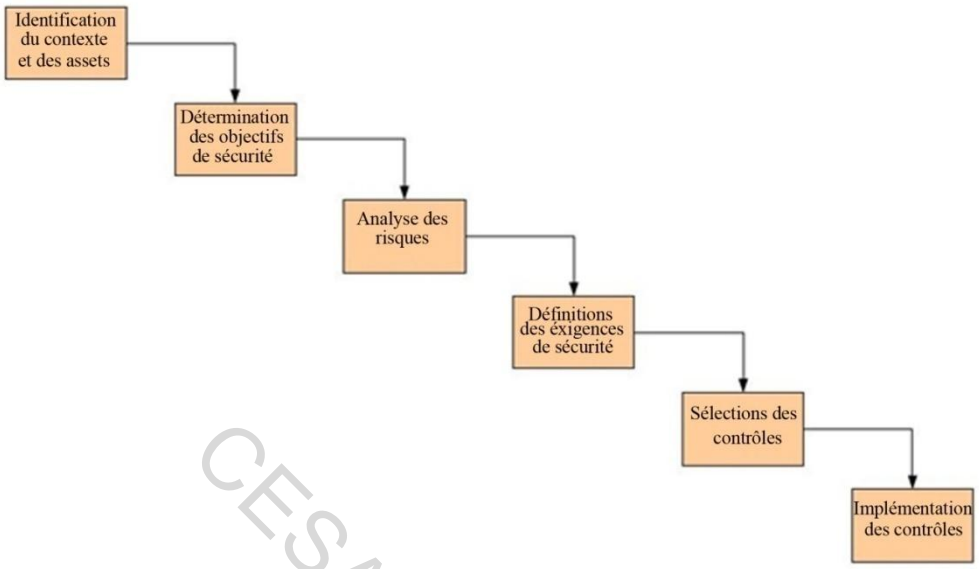
Afin de mitiger ces risques et de protéger les assets, une politique de traitement des risques est mise en place. Elle sera constituée d'exigences de sécurité permettant de répondre aux risques. Ces exigences de sécurité vont ensuite entraîner la mise en place de contrôles (ou contre-mesures) de sécurité à implémenter, afin de satisfaire aux exigences. Les contrôles sont de deux types :

- sur la menace ou la vulnérabilité, afin de limiter la cause du risque ;
- sur l'impact, afin de limiter la conséquence du risque.

2.2.2.2. Description d'un processus de gestion des risques.

Après avoir mis en évidence les concepts intervenant dans la gestion des risques, on peut identifier un processus de haut niveau couvrant ses activités. Ce processus est presque toujours appliqué dans les méthodes pratiques de gestion des risques, comme nous le verrons par la suite.

Figure 6 : le processus de gestion des risques.



Source : MAYER & al. (2006 :4)

La première étape d'une démarche de gestion des risques consiste en l'identification du domaine et des assets. Dans cette partie, il est question de prendre connaissance avec l'organisation, son environnement, son SI et de déterminer précisément les limites du système sur lequel va porter l'étude de gestion des risques. Une fois notre système borné, on procède en premier lieu à l'identification des assets business constituant la valeur de l'organisation. Ensuite, le lien sera fait entre ces assets business et les assets système, sur lesquels on identifiera et corrigera les risques d'un point de vue technique et organisationnel.

La détermination des objectifs de sécurité vise à spécifier les besoins en termes de confidentialité, intégrité et disponibilité des assets, en particulier au niveau business. Le lien entre les assets business et les assets système étant faits en amont, on retrouve donc les besoins en sécurité au niveau du système.

L'analyse des risques constitue le cœur de la démarche de gestion des risques.

Elle a pour finalité l'identification et l'estimation de chaque composante du risque (menace/vulnérabilité/impact), afin d'évaluer le risque et d'apprécier son niveau, dans le but de prendre des mesures adéquates (parfois, cette étape est également appelée « appréciation du risque » (ISO/IEC Guide 73:2009). Il y a deux grandes écoles pour l'identification des risques : soit en réalisant un audit du système et de ses différents acteurs (OCTAVE : 2008),

soit à partir de bases de connaissances prédéfinies (EBIOS : 2013) (MEHARI : 2013). Pour l'estimation des risques, il est possible en théorie de les quantifier à l'aide de distributions de probabilités sur les menaces et les vulnérabilités, ainsi qu'en estimant les coûts occasionnés par les impacts. En pratique, il se révèle difficile de donner des valeurs absolues et on se contente bien souvent d'une échelle de valeurs relatives, par exemple, allant de 1 à 4. Cette estimation permet de faire un choix, dans le traitement du risque, avant de passer à la détermination des exigences de sécurité.

D'une manière générale, on considère que :

- les risques ayant une occurrence et un impact faible sont négligeables ;
- les risques ayant une forte occurrence et un impact important ne doivent pas exister, autrement une remise en cause des activités de l'entreprise est nécessaire (on évite le risque, avoidance en anglais) ;
- les risques ayant une occurrence forte et un impact faible sont acceptés, leur coût est généralement inclus dans les coûts opérationnels de l'organisation (acceptation du risque) ;
- les risques ayant une occurrence faible et un impact lourd sont à transférer. Ils peuvent être couverts par une assurance ou un tiers (transfert du risque) ;
- enfin, les autres risques, en général majoritaires, sont traités au cas par cas et sont au centre du processus de gestion des risques ; l'objectif, étant de diminuer les risques en les rapprochant au maximum de l'origine de l'axe (atténuation du risque à l'aide de contrôles).

Une fois l'analyse des risques effectuée, la définition des exigences de sécurité permettra de réduire les risques identifiés. Comme précédemment, en fonction des méthodes, cette étape pourra être effectuée avec l'assistance de référentiels (ISO 15408) (ISO/27002) ou aiguillée par la connaissance d'experts système/sécurité. La définition des exigences de sécurité, de par son importance et sa complexité, est souvent effectuée de manière incrémentale. En effet, on conseille bien souvent de débuter par des exigences générales, qui définiront l'intention de contrer les risques identifiés (de niveau stratégique), pour les transformer ensuite en des exigences plus précises (vers le niveau opérationnel). Toutefois les exigences sont censées être génériques et applicables à tout SI. Il faut également rappeler que ces exigences de mitigation des risques porteront à la fois sur le système informatique (comme le besoin de

cryptage des mots de passe), mais aussi sur son environnement (par exemple, « l'utilisateur du système ne doit pas dévoiler son mot de passe à un tiers »).

Le dernier niveau est constitué par la sélection des contrôles (ou contre-mesures) de sécurité. Ici sont définis les choix techniques des solutions de sécurité, influencés par le système déjà en place, les compétences disponibles, les coûts de mise en œuvre.

Une fois les contrôles sélectionnés, il reste alors à les implémenter dans le SI et à éventuellement les tester et les évaluer. Il subsiste alors indéniablement une part de risques traités partiellement ou non, qui constitue ce que l'on appelle le risque résiduel.

Ce processus est communément admis par les différentes méthodes de gestion des risques. Par contre, la terminologie est souvent très différente, d'une méthode ou norme à une autre. La comparaison du processus de plusieurs méthodes nécessite alors une bonne analyse, mais dans l'ensemble, le schéma présenté précédemment est suivi. Toutefois, quelques méthodes se distinguent en présentant une trame quelque peu différente ou étendue (tout en gardant bien souvent comme base l'inamovible processus générique présenté).

2.3. La gestion des risques en pratique.

Tel que décrit précédemment, plus de 200 méthodes de gestion/analyse des risques sont déclinées actuellement à travers le monde. Ces dernières sont plus ou moins bien finalisées, plus ou moins faciles d'accès ou tout simplement inconnues. A ce titre, le CIGREF a récemment rappelé, en regard du domaine de la sécurité des SI, que « l'abondance de normes et de méthodes est souvent source de confusion ». Il ne faut, en effet, pas se perdre dans le dédale des méthodes et tenter d'aller à l'essentiel sur cette thématique.

Mais comment faire son choix au milieu de la jungle des référentiels d'analyse des risques ? Une première aide précieuse est fournie via la présentation, en amont, des fondements caractérisant les concepts et processus de la gestion des risques pour les SI. Ces concepts transcrivent le cadre de compréhension nécessaire pour appréhender sereinement la matière. En effet, à partir de ces informations, le choix peut alors se faire, de manière progressive et en fonction du contexte.

Pour réduire le champ du choix au cœur des méthodes formelles, certaines sont actuellement très populaires, faisant référence dans leur domaine. A ce titre, nous avons choisi de détailler

EBIOS, MEHARI, OCTAVE et CRAMM qui remplissent efficacement leur rôle dans la conduite d'une démarche de gestion des risques.

2.4. Présentation du référentiel COSO.

Selon MOISAND & al, (2009:12) le COSO (Committee of Sponsoring Organizations of the Treadway Commission) a publié en 1992 un cadre de référence pour le contrôle interne afin d'aiderles entreprises à évaluer et à améliorer leur système de contrôle interne. Le contrôle interne y est décrit comme un processus étant sous la responsabilité d'une instance constituée dans le but d'assurer la réalisation d'objectifs regroupés dans les domaines suivants :

- efficacité et efficience des opérations ;
- fiabilité des rapports financiers ;
- conformité aux lois et règlements.

Selon RENARD (2010:136) le COSO1 a réuni les compétences d'un certain nombre de professionnels représentant l'IIA, de quelques cabinets d'audit externe et de grande entreprise américaine. Il a édité l'ensemble de ses travaux dans un ouvrage The Internal Control Framework traduit en Français sous le titre La pratique du contrôle interne1. Cet ouvrage définit ce qu'il faut entendre par « contrôle interne », vocable dont on ne dira jamais assez que c'est une mauvaise traduction, la plus mauvaise que l'on ait pu trouver pour le terme anglo-saxon « internal control », oubliant que pour les Anglo-Saxons « to control » veut dire en majeur « maîtriser » et en mineur « vérifier », alors que c'est l'inverse pour les pays de langue française.

Le contrôle interne, et la Commission Treadway le confirme, n'a donc aucun rapport direct avec un quelconque système d'inspection ou de vérification ; c'est la réponse à la question « comment faire pour maîtriser au mieux ses activités ? ». Et on perçoit bien que cette question s'adresse à tous. Pour y répondre le COSO1 retient cinq éléments essentiels jugés nécessaires pour une bonne maîtrise des activités : ils réunissent donc les conditions indispensables pour un bon contrôle interne. Ces éléments, présentés sous la forme d'une pyramide, comportent de la base au sommet :

- l'environnement de contrôle traduisant la culture de l'organisation et qui doit être favorable pour que la mise en place d'un contrôle interne satisfaisant ne rencontre pas d'obstacles ;

- une évaluation des risques afin de bien les connaître pour être en mesure de les maîtriser ;
- des activités de contrôle lesquelles regroupent les dispositifs spécifiques jugés nécessaires pour faire échec aux risques. ;
- une information et une communication satisfaisantes ;
- un pilotage de l'ensemble par chaque responsable à son niveau.

En 2004, le COSO 2 a publié le document Management des risques dans l'entreprise (Enterprise Risk Management ou ERM) qui élargit le périmètre du contrôle interne. Il fait suite au COSO 1, en le complétant par l'approche du management des risques. Le COSO 2 parle d'événement dans la vie d'une entreprise qui devient un risque s'il l'impacte négativement ou au contraire une opportunité si l'événement s'avère bénéfique. COSO 2 parle également d'appétence au risque, soit le niveau de risque auquel l'entreprise est prête à faire face. Cette appétence est englobée d'un seuil de tolérance, soit une variation acceptable du niveau de risque par rapport à l'appétence, qui est l'objectif défini. Par rapport au référentiel COSO 1, qui traite du contrôle interne, COSO 2 prend également en compte les objectifs stratégiques en plus des objectifs opérationnels, de reporting et de conformité.

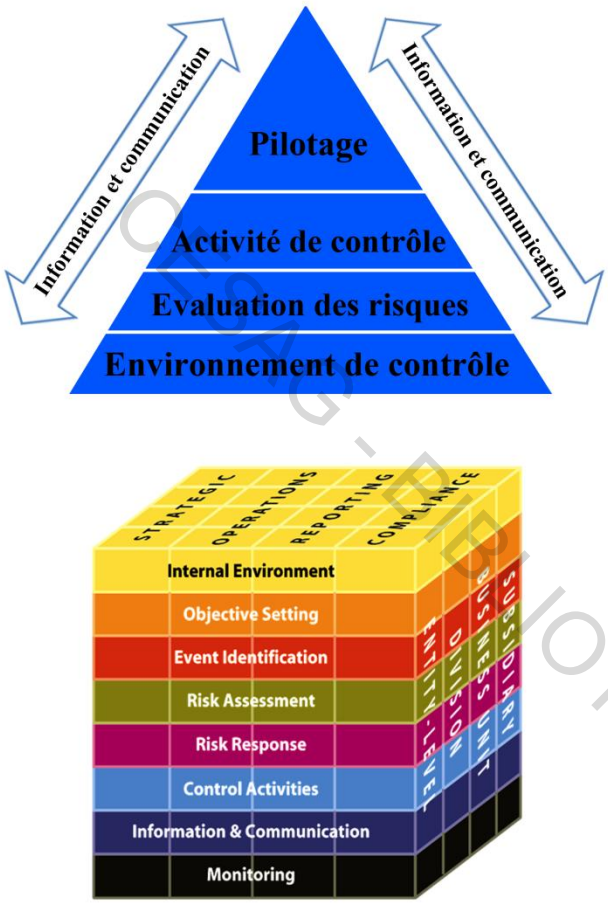
De même, trois éléments sont rajoutés par rapport au dispositif de contrôle interne : la fixation des objectifs (afin d'identifier à partir de ces derniers quels événements pourraient nuire à leur atteinte), l'identification des événements (à la fois risques et opportunités) et le traitement des risques (ici les opportunités sont mises de côté, comme pour l'évaluation des risques). Enfin, COSO 2 donne une dimension d'analyse supplémentaire car les risques doivent être maîtrisés et analysés dans toute l'entreprise.

L'ERM englobe :

- la notion de portefeuille de risques ;
- une structuration en quatre catégories d'objectifs (opérations, reporting, conformité et objectifs stratégiques) ;
- le niveau de prise de risque décidé de façon stratégique par l'entreprise ;
- les événements qui impactent les risques ;
- les quatre catégories de réponse aux risques (éviter, réduire, partager et accepter) ;
- le périmètre de l'information et de la communication ;

- les rôles et les responsabilités des acteurs en charge de la sécurité mais aussi des directeurs (board).

Figure 7 : comparaison COSO 1 à COSO 2 : de la pyramide au cube.



Source **:** BOURROUILH & al. (2010 :19)

- **Le COSO 2 face à la méthode EBIOS**

La méthode EBIOS s'intéresse aux besoins de sécurité du système d'information. Elle met à disposition de ses utilisateurs une base de connaissances qui décrit les types d'entités, les méthodes d'attaques, les vulnérabilités, les objectifs et les exigences de sécurité. Cette méthode comprend également un recueil des meilleures pratiques concernant l'élaboration de schémas directeurs du système d'information.

Tandis que le COSO 2 propose un processus efficace pour lutter contre les risques et les incertitudes d'une organisation.

Ils ont la même finalité de gérer les risques mais leur démarche est différente.

Dans notre cas le COSO 2 peut nous être utile notamment par la notion d'appétence au risque qui s'avère être le niveau de prise de risque accepté par une organisation dans le but d'accroître sa valeur, mais la méthode EBIOS semble plus adéquate pour gérer les risques spécifiques au système d'information.

2.5. Présentation du référentiel COBIT.

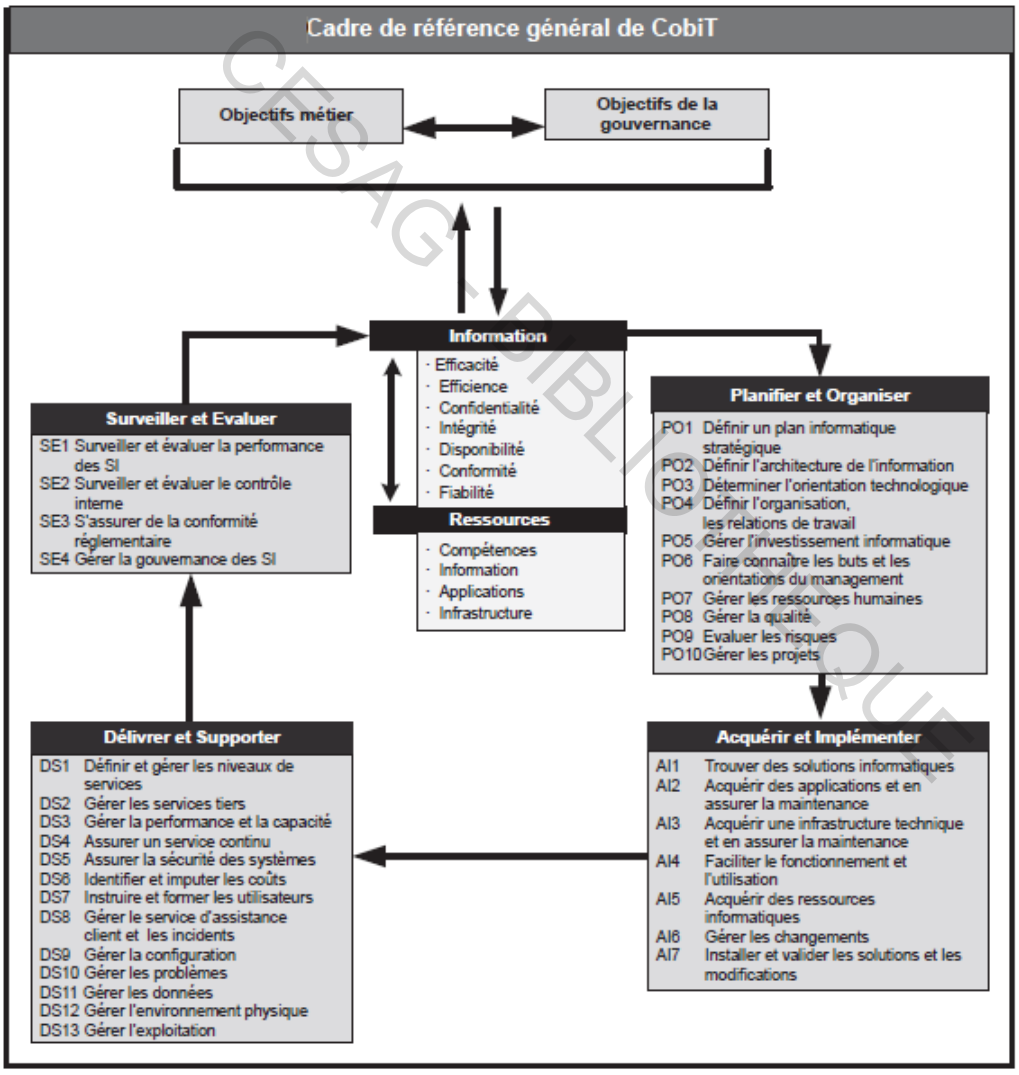
Selon MOISAND & al. (2009:3) CobiT est le résultat des travaux collectifs réalisés par les principaux acteurs de la profession, auditeurs internes ou externes, fédérés au sein de l'ISACA (Information System Audit and Control Association). Cette association mondiale basée aux États-Unis est déployée dans les plus grandes villes du monde. Elle est représentée en France par l'AFAI (Association française pour l'audit et le conseil en informatique). Dans ses premières versions, publiées à partir de 1996, CobiT (Control OBjectives for Information and relatedTechnology) se positionne comme un référentiel de contrôle. Il décline sur le domaine IT les principes du référentiel COSO (Committee of Sponsoring Organizations of the Treadway Commission), publiés pour la première fois en 1992 et dont l'objectif est d'aider les entreprises à évaluer et à améliorer leur système de contrôle interne.

« Dans certains secteurs, l'activité cœur de métier de l'entreprise peut être mise en péril en cas d'arrêt ou de dysfonctionnement de ses systèmes informatiques, car la dépendance des processus métier envers l'informatique est totale. Dans notre exemple de distribution par le Web, si ce canal est le seul prévu pour le produit en question, l'indisponibilité pour cause de panne ou de retard dans l'ouverture du service de commande en ligne se solde par une perte nette de revenus qui ne sera jamais récupérée. La gestion des risques informatiques ou des systèmes d'information correspond à un référentiel qui comprend une analyse de risque et un plan de traitement des risques associé. Ce plan de traitement des risques doit être établi selon des critères de tolérance par rapport au préjudice financier lié à la réalisation des risques. Cela veut dire en d'autres termes que les moyens engagés pour couvrir les risques ne doivent pas coûter plus cher que le préjudice lui-même »MOISAND & al, (2009:9).

CobiT a été et reste le référentiel d'audit de la gouvernance des SI. Il offre un cadre de référence de contrôle structuré des activités informatiques selon 34 processus répartis en quatre domaines :

- planifier et organiser ;
- acquérir et implémenter ;
- délivrer et supporter ;
- surveiller et évaluer.

Figure 8 : organisation du référentiel COBIT.



Source : MOISAND & al. (2009:30).

2.5.1. L'apport de CobiT pour l'audit.

La structure de CobiT offre à l'auditeur une classification très solide :

- domaines, processus, objectifs de contrôle ;
- critères d'information (efficacité, efficience, confidentialité, intégrité, disponibilité, conformité et fiabilité) ;
- ressources (applications, infrastructure, information et personnes).

À cette structure se rattache un détail « générique » pour chaque objectif de contrôle, présenté comme suit dans le document *IT Assurance Guide: Using CobiT*:

Objectif de contrôle	Inducteurs de valeur	Inducteurs de valeur

Source : MOISAND & al. (2009:199).

Cette notion de valeur liée à un objectif de contrôle est tout à fait intéressante puisqu'elle étend le périmètre du contrôle, en incluant non seulement la maîtrise des risques, mais aussi la création de valeur. On trouve ensuite un plan de contrôle pour cet objectif, puis des tests détaillés. Enfin, ce référentiel peut être enrichi pour prendre en compte des aspects techniques pointus.

2.5.2. CobiT et l'ISO/IEC 27001.

Selon MOISAND & al (2009 :215) la norme ISO/IEC 27001, qui s'appuie sur l'ISO/IEC 27002, décrit les exigences de mise en place d'un système de management de la sécurité de l'information (SMSI). Les principes utilisés sont identiques à ceux exprimés dans la norme ISO 9001. CobiT, à travers le processus PO8, préconise la mise en place d'un système de management de la qualité (SMQ) qui reprend les finalités de l'ISO 9001.

Quant aux exigences de l'ISO/IEC 27001, elles se retrouvent également dans les processus PO6, PO9, DS4 et DS5. En ce sens, CobiT est parfaitement compatible avec la mise en place d'un SMSI. La mise en place d'un SMSI relève de la même logique que celle d'un SMQ ; c'est une question de stratégie et d'affichage. En effet, la mise en place d'un système de management ISO 9001 ou ISO/IEC 27001 est souvent motivée par un besoin de reconnaissance, lequel est matérialisé par la certification. Il est cependant important de noter que la manière de définir les périmètres est différente selon que l'on traite de l'ISO 9001 ou de l'ISO/IEC 27001. Pour le management de la sécurité de l'information, le périmètre est déterminé par l'identification des actifs devant être protégés.

2.6. Les différentes méthodes d'évaluation des risques.

Le tableau suivant liste les principales normes utilisées provenant des organismes de normalisation internationaux ainsi que celles soutenues par le secteur privé ou associatif :

Tableau 4 : les différentes méthodes d'évaluation des risques.

Méthode	Création	Popularité	Auteur	Soutenue par	Pays	Outils disponibles
EBIOS	1995	***	DCSSI	Gouvernement	France	Logiciel gratuit
MEHARI	1995	***	CLUSIF	Association	France	Logiciel Risicare
OCTAVE	1999	**	Université de Carnegie Mellon	Universitaire	Etats-Unis	Logiciel payant
CRAMM	1986	**	Siemens	Gouvernement	Angleterre	Logiciel payant
SPRINT	1995	*	ISF	Association	Angleterre	Logiciel payant
BS 7799		***		Gouvernement	Angleterre	
ISO 17799		***		International		
ISO 13335				International		
ISO 15408				International		
SCORE	2004		Ageris consulting	Secteur privé	France	Logiciel payant
CALLIO	2001		CALLIO TECHNOLOGIES	Secteur privé	Canada	Logiciel payant
COBRA	2001		C&A systems security limited	Secteur privé	Angleterre	Logiciel payant
ISAMM	2002		Evosec	Secteur privé	Belgique	
RA2	2000		aexis	Secteur privé	Allemagne	Logiciel payant

Légende : *** très populaire, **peu populaire,* pas populaire

Source: Etude comparative pour la sélection de la méthode d'analyse du risque, GIE GAINDE 2000.

2.7. La famille des normes ISO/IEC 27000.

Les normes de la famille ISO/IEC 27000 constituent un ensemble de méthodes, mesures et bonnes pratiques reconnues au niveau international dans le domaine de la sécurité de l'information. Ces normes ont pour but de décrire les objectifs à atteindre en matière de sécurité informatique, et non la manière concrète d'y arriver. Celle-ci dépend généralement du contexte propre à toute organisation.

Au niveau international, c'est le sous-comité 27 du comité joint entre l'ISO et l'IEC numéro 1, en abrégé: ISO/IEC JTC 1/SC 27, qui s'occupe de la gestion et de la publication de ses normes phares du domaine de la sécurité de l'information.

2.7.1. Présentation de la famille ISO 2700x.

Cette famille se décline en 8 volumes :

- ISO 27000 présente les principes et le vocabulaire ;
- ISO 27001 décrit les processus permettant le management de la sécurité de l'information (SMSI) ;
- ISO 27002(anciennement appelé ISO/CEI 17799 : 2005) présente un catalogue de bonnes pratiques de sécurité,
- ISO 27003 décrit les différentes phases initiales à accomplir afin d'aboutir à un système de Management tel que décrit dans la norme ISO 27001 ;
- ISO 27004 permet de définir les contrôles de fonctionnement du SMSI ;
- ISO 27005 décrit les processus de la gestion des risques ;
- ISO 27006 décrit les exigences relatives aux organismes qui auditent et certifient les SMSI des sociétés ;
- ISO 27007 constitue le guide pour l'audit de Systèmes de Management de la Sécurité de l'Information (SMSI).

Nous allons nous intéresser à la norme ISO 27005 dans le cadre de notre étude.

2.7.2. La norme ISO 27005 : Gestion du risque pour le SMSI.

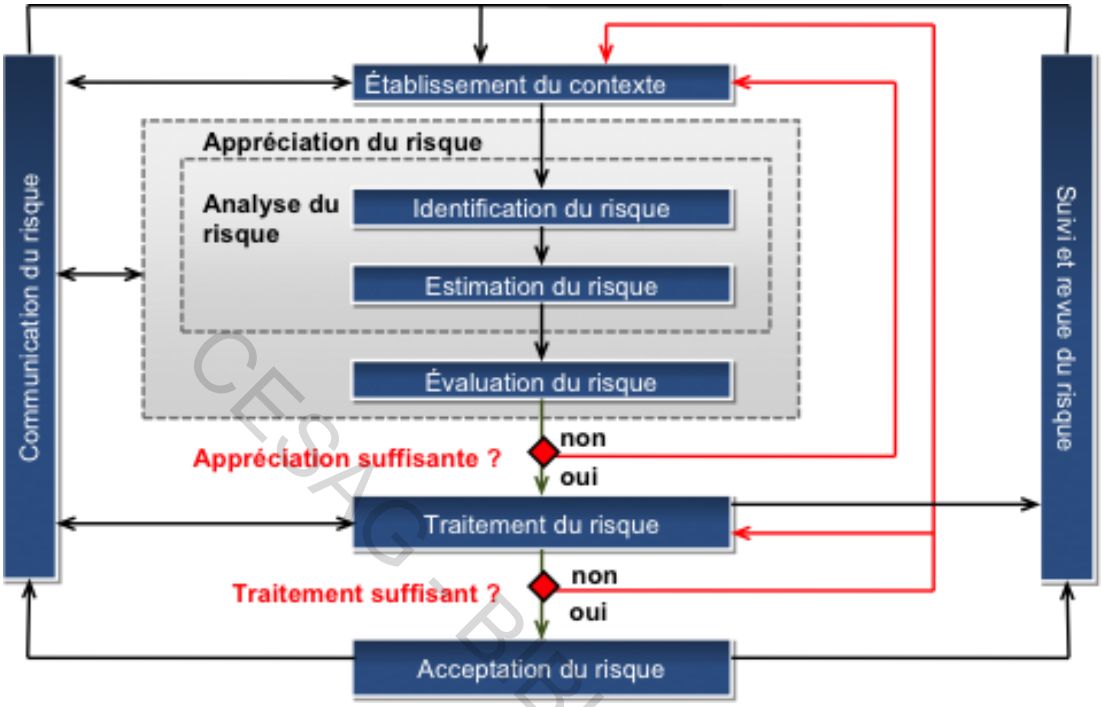
La norme ISO27005 (ISO/CEI 27005:2008) a été publiée le 4 juin 2008 en langue anglaise, puis en octobre 2009 en version française. Cette norme adresse la gestion des risques en Sécurité des Systèmes d'Information.

«Il est important de bien comprendre que la norme ISO 27005 n'est pas une méthodologie de gestion de risque. Elle donne un cadre normatif qui pourra être utilisé pour l'élaboration ou la validation de méthodologies de gestion de risque informationnel, comme c'est le cas avec l'approche présentée dans ce livre, qui se conforme à ISO 27005. La norme ISO 27005 a pour but d'aider à mettre en œuvre un système de management (ou de gestion) de la sécurité de l'information (SMSI) selon la norme ISO 27001, qui est fondée sur une approche de gestion du risque.» (LEGER 2013:139)

La norme ISO 27005 propose une démarche de gestion des risques itérative, alignée sur les quatre phases Plan - Do - Check - Act. La tâche la plus importante reste cependant dans la

phase de mise en place initiale, avec l'appréciation du risque. Les activités décrites dans le standard et le processus générique de gestion des risques sont représentés dans le schéma.

Figure 9 : démarche de gestion des risques selon la norme ISO 27005.



Source : BOURASSA (2015)

La norme ISO 27005 définit une démarche, mais ne constitue pas une méthode, et n'en recommande à proprement parler aucune. Chaque activité de la démarche peut donc être menée selon une méthodologie propre à l'organisme, ou plus spécialement adaptée à un contexte donné. Ainsi, la norme ne fournit pas directement de métriques, ni de formule de calcul du niveau de risque. Cependant, il existe une méthode d'évaluation des risques en informatique, développée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), une traduction numérique de la norme ISO 27005 : la méthode EBIOS.

2.8. Les méthodes de gestion des risques.

Dans le cadre de notre étude nous avons tout juste retenu quatre (4) méthodes de gestion des risques du système d'information qui sont : EBIOS, MEHARI, OCTAVE et CRAMM.

- **EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)**

« Créée en 1995 par l'ANSSI et régulièrement mise à jour, la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) bénéficie de ses 20 ans d'expérience dans le domaine de la gestion du risque. Elle permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information (SSI). Elle permet aussi de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires, constituant ainsi un outil complet de gestion des risques SSI.

L'ANSSI et le Club EBIOS ont élaboré la version 2010 de la méthode EBIOS pour prendre en compte les retours d'expérience et les évolutions normatives et réglementaires.

Cette approche plus simple, plus claire, contient des exemples et des conseils. Elle offre la possibilité d'élaborer et d'assurer le suivi d'un plan d'actions relevant de la sécurité des systèmes d'information. Elle est assortie d'une base de connaissances cohérente avec le référentiel général de sécurité, enrichie d'exemples concrets permettant d'élaborer des scénarios de risque pertinents pour votre organisme.

Elle comprend enfin une étude de cas type, permettant d'appréhender la méthode.

Modulaire et conforme aux normes internationales ISO/IEC 31000, ISO/IEC 27005, ISO/IEC 27001, la méthode EBIOS reste la boîte à outils indispensable pour toute réflexion de sécurité de l'information :

- pour construire son référentiel SSI ;
    - gestion des risques d'un organisme ;
    - mise en place d'un système de management de la sécurité de l'information ;
    - élaboration d'une doctrine, d'une stratégie, d'une politique, d'un plan d'actions, ou d'un tableau de bord SSI.

Pour intégrer la SSI dans les projets ou les systèmes existants, quel que soit leur niveau d'avancement :

- dossier de sécurité ;
- cahier des charges ;
- fiche d'expression rationnelle des objectifs de sécurité (FEROS) ;
- profil de protection (PP) ;

- cible de sécurit. » ANSSI (2015).

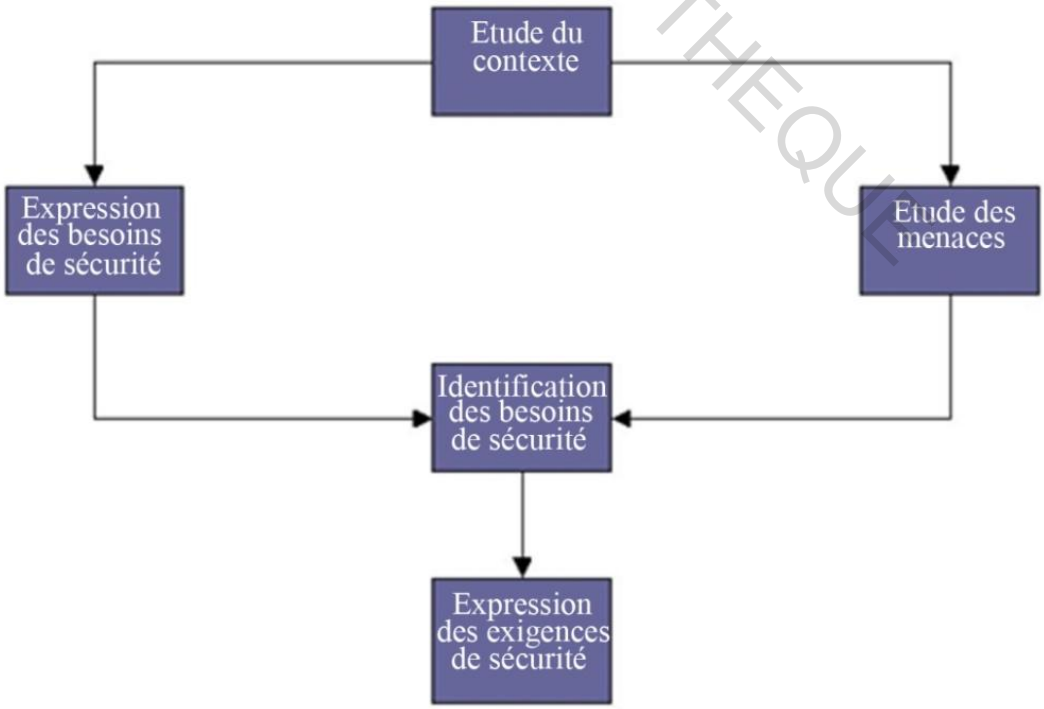
Selon ETIEVANT (2006), le logiciel libre et gratuit permet de simplifier l'application de la méthode et d'automatiser la création des documents de synthèse. La DCSSI possède un centre de formation où sont organisés des stages à destination des organismes publics français. Un club d'utilisateurs EBIOS a été créé en 2003 et constitue une communauté experte permettant le partage des expériences. Une base de connaissances à laquelle se connecte le logiciel EBIOS permet d'avoir à accès à la description d'un ensemble de vulnérabilités spécifiques, de contraintes de sécurité, de méthodes d'attaques. Elle peut être enrichie via le logiciel.

La méthode EBIOS est découpée en 5 étapes :

- étude du contexte
- expression des besoins de sécurité
- étude des menaces
- identification des objectifs de sécurité
- détermination des exigences de sécurité

Le schéma ci-après illustre les 5 étapes de la méthode.

Figure 10 : démarche EBIOS globale.



Source : ETIEVANT (2006)

L'étude du contexte

Selon LEGER (2013 :185) Un contexte bien défini permet de gérer les risques de manière parfaitement appropriée, et ainsi de réduire les coûts à ce qui est nécessaire et suffisant au regard de la réalité du sujet étudié. Pour ce faire, il est essentiel d'appréhender les éléments à prendre en comptes dans la réflexion :

- le cadre mis en place pour gérer les risques ;
- les critères à prendre en considération (comment estimer, évaluer et valider le traitement des risques) ;
- la description du périmètre de l'étude et de son environnement (contexte externe et interne, contraintes, recensement des biens et de leurs interactions…).

La méthode EBIOS permet d'aborder tous ces points selon le degré de connaissance que l'on a du sujet étudié. Il sera ensuite possible de l'enrichir, de l'affiner et de l'améliorer à mesure que la connaissance du sujet s'améliore.

L'expression des besoins de sécurité permet d'estimer les risques et de définir les critères de risque. Les utilisateurs du SI expriment durant cette étape leurs besoins de sécurité en fonction des impacts qu'ils jugent inacceptables.

L'étude des menaces permet d'identifier les risques en fonction non plus des besoins des utilisateurs mais en fonction de l'architecture technique du système d'information. Ainsi la liste des vulnérabilités et des types d'attaques est dressée en fonction des matériels, de l'architecture réseau et des logiciels employés. Et ci, quelles que soient leur origine (humaine, matérielle, environnementale) et leur cause (accidentelle, délibérée).

L'identification des objectifs de sécurité confronte les besoins de sécurité exprimés et les menaces identifiées afin de mettre en évidence les risques contre lesquels le SI doit être protégé. Ces objectifs vont former un cahier des charges de sécurité qui traduira le choix fait sur le niveau de résistance aux menaces en fonction des exigences de sécurité.

La détermination des exigences de sécurité permet de déterminer jusqu'où on devra aller dans les exigences de sécurité. Il est évident qu'une entreprise ne peut faire face à tout type de risques, certains doivent être acceptés afin que le coût de la protection ne soit pas exorbitant. C'est notamment la stratégie de gestion du risque telle que cela est défini dans un plan de risque qui sera déterminé ici : accepter, réduire ou refuser un risque. Cette stratégie est

décidée en fonction du coût des conséquences du risque et de sa probabilité de survenue. La justification argumentée de ces exigences donne l'assurance d'une juste évaluation. EBIOS fournit donc la méthode permettant de construire une politique de sécurité en fonction d'une analyse des risques qui repose sur le contexte de l'entreprise et des vulnérabilités liées à son SI.

- **OCTAVE**

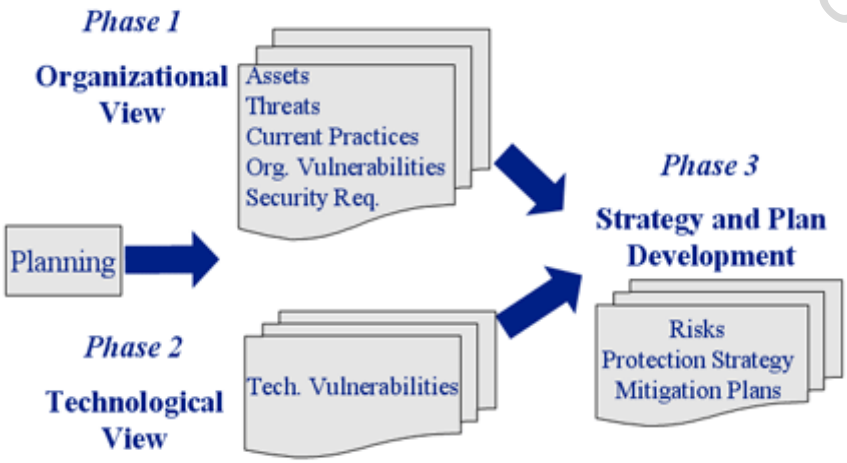
«L'acronyme OCTAVE signifie Operationally Critical Threat, Asset, and Vulnerability Evaluation. Il s'agit d'une suite d'outils, de techniques et méthodes créés pour l'évaluation des risques basée sur la sécurité de l'information stratégique et la planification» (LEGER 2013,176)

Elle a pour but de permettre à une entreprise de réaliser par elle-même l'analyse des risques de leur SI, sans aide extérieure (consultants). Pour cela, un catalogue de bonnes pratiques de sécurité est fourni avec la méthode.

Octave est constitué de 3 phases :

- vue organisationnelle
- vue technique
- stratégie de sécurité

Figure 11 : les phases de la méthode d'OCTAVE.



Source : ETIEVANT (2006)

La vue organisationnelle permet d'identifier les actifs de l'entreprise, les menaces qui pèsent sur son fonctionnement, les vulnérabilités de son organisation, les objectifs de sécurité imposés par la direction et les mesures actuelles de sécurité. Ce sont trois processus de collecte de l'information qui sont réalisés durant cette phase, chacun par une population particulière : les cadres supérieurs, les cadres opérationnels et les équipes de production. La consolidation des informations nées de ces processus amène à créer des profils de menaces.

La vue technique identifie les éléments essentiels de chaque actif identifié plus haut et les audite afin d'en connaître les vulnérabilités.

Le développement de la stratégie de sécurité consiste à évaluer les risques identifiés (impact, probabilité) plus haut et à proposer les mesures permettant de les réduire. Un plan de réduction des risques est alors planifié.

La méthode OCTAVE est centrée sur la protection des actifs de l'entreprise et le management du personnel. Elle couvre l'ensemble des processus métiers de l'entreprise à tous les niveaux (organisationnel et technique).

Cette méthode suppose la constitution d'une équipe pluridisciplinaire comprenant des membres de tous les services de l'entreprise.

- **MEHARI (Méthode Harmonisée d'Analyse de Risques)**

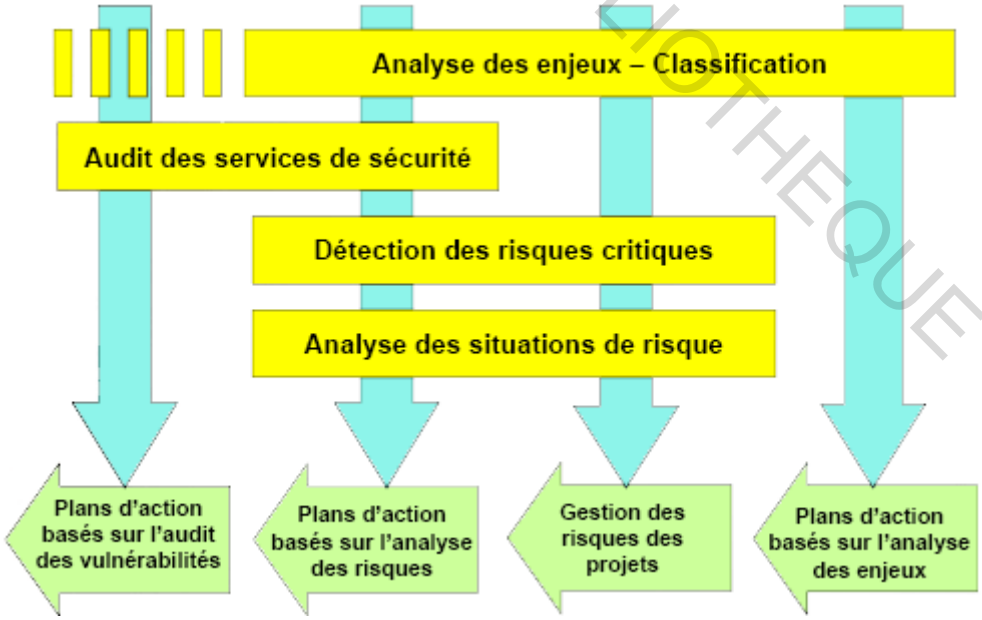
« MÉHARI, la MÉthode Harmonisée d'Analyse du Risque Informatique, est issue des travaux de Jean-Philippe Jouas et de Albert Harari, lorsqu'ils étaient en fonction chez Bull. À l'époque, Jean-Phillipe Jouas était Directeur de la sécurité du Groupe Bull et Albert Harari était responsable des méthodes au sein de cette Direction. Leurs travaux initiaux furent consolidés par la commission Méthodes du Clusif, le Club de la Sécurité des Systèmes d'Information Français. Albert Harari avait développé Melisa pour la DCN, la Direction des Constructions Navales de la Délégation Générale pour l'Armement de la République Française. La méthode Melisa proposait une certaine vision des risques, avec des paramètres d'évaluation relativement simples et adaptés à la cible visée. Son utilisation dans un contexte industriel et dans une société multinationale a conduit Jouas et Harari à faire évoluer cette base pour définir un modèle du risque complet et une métrique associée. Les résultats de ces travaux furent publiés en 1992. C'est en incorporant les bases de connaissances de la méthode Marion, développés depuis 1984, aux travaux de Jouas et Harari que s'est construit

progressivement un ensemble d'outils de management de la sécurité qui sont devenus MÉHARI. » (LEGER 2013 :180)

Elle se présente comme une véritable boîte à outils de la sécurité des SI, permettant d'appréhender le risque de différentes manières au sein d'une organisation, et composée de plusieurs modules. Ces derniers, indépendamment de la démarche sécurité choisie, permettent notamment :

- D'analyser les enjeux de la sécurité (en décrivant les types de dysfonctionnements redoutés) et, corrélativement, de classifier les ressources et informations selon les trois critères sécurité de base (Confidentialité, Intégrité, Disponibilité) ;
- d'auditer les services de sécurité, de manière à prendre en comptes l'efficacité de chacun, son contrôle, et de synthétiser les vulnérabilités ;
- d'analyser les situations de risques, permettant d'évaluer les potentialités et les impacts intrinsèques, ainsi que les facteurs d'atténuation de risque, et, enfin, de déduire un indicateur de gravité de risque.

Figure 12 : démarche MEHARI globale.



Source : ETIEVANT (2006)

MEHARI présente une grande diversité dans l'utilisation de ses modules. Trois approches se détachent plus particulièrement :

- En se basant sur une analyse détaillée des risques, il est possible de mettre en œuvre des plans de sécurité. Cette démarche se décline au niveau stratégique, mais aussi opérationnel. Le premier niveau permet la cohérence des besoins et du contexte de l'ensemble de l'organisation. Le second niveau définit les unités business autonomes au cœur de l'organisation et en charge des décisions nécessaires en matière de sécurité ;
- en se basant sur l'audit de sécurité, ou plus précisément après un diagnostic de l'état de sécurité, la réalisation de plans d'actions est facilitée. En effet, des faiblesses relevées découlent alors, directement, les actions à entreprendre ;
- dans le cadre de la gestion d'un projet particulier, tenir comptes de la sécurité, en se basant, de nouveau, sur l'analyse des risques, et ainsi faciliter l'élaboration de plans d'action. Les besoins de sécurité sont alors directement intégrés aux spécifications du projet, et à intégrer dans le plan de sécurité global de l'entité concernée.

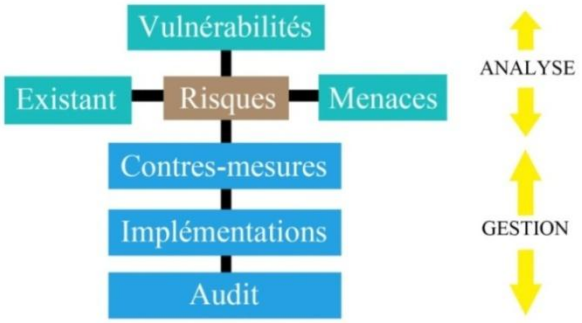
Cette méthode s'aligne avec les deux premières en termes de couverture du processus de gestion des risques.

- **CRAMM (CCTA Risk Analysis and Management Method)**

Cramm a été inventée par Siemens en Angleterre et est soutenue par l'état. Cramm est une méthode exhaustive assez lourde, réservée aux grandes entreprises puisqu'elle recourt à près de 3 000 points de contrôle. Elle possède deux variantes : Cramm Express et Cramm Expert et est compatible avec la norme BS77.

Des logiciels sont fournis avec la méthode à des fins de simulation, de reporting et de suivi des mesures de sécurité.

Figure 13 : démarche général de la méthode Cramm.



Source : ETIEVANT (2006)

La méthode Cramm est composée de 3 phases :

- Identification de l'existant ;
- évaluation des menaces et des vulnérabilités ;
- choix des remèdes.

L'identification de l'existant permet de dresser l'inventaire des équipements, des applications, et des données qui constituent l'infrastructure informatique sur laquelle repose le Sl de l'entreprise. Chacun des éléments de cet inventaire est évalué en termes de coût et d'impact en cas de compromission (indisponibilité, altération, destruction...).

L'évaluation des menaces et des vulnérabilités met en évidence les problèmes possibles. Pour cela, la base de connaissances de Cramm fournit une liste importante des risques possibles dont il faut évaluer le niveau de criticité.

Le choix des remèdes consiste à sélectionner parmi une base de 3 000 contre-mesures possibles classées en 70 thèmes les remèdes aux risques identifiés plus haut. Le logiciel fourni avec Cramm détermine les remèdes à adopter en fonction des risques, de leur criticité identifiés précédemment et du niveau de sécurité désiré.

Ce second chapitre nous a permis de connaître le processus de gestion des risques, la famille des normes ISO/IEC 27000, ainsi que les différentes méthodes utilisées.

Au nombre des différentes méthodologies d'étude, nous présentons à présent celle qui nous parait le plus adéquat pour la gestion des risques de la direction des opérations.

- **Choix de l'outil d'analyse des données**

Une méthode est définie selon GRAWITZ (1979 : 345) comme étant un ensemble ordonné des principes, des règles et des opérations intellectuelles permettant de faire l'analyse en vue d'atteindre un résultat. Dans le cadre de notre travail, nous avons fait recours à la méthode EBIOS.

- **Pourquoi la méthode EBIOS ?**

Critère de sélection d'une méthode :

- La langue de la méthode, il est essentiel de maîtriser le vocabulaire employé ;
- l'existence d'outils logiciels en facilitant l'utilisation ;
- l'existence d'un club d'utilisateurs afin d'avoir un retour d'expériences ;
- la qualité de la documentation ;
- le coût de la mise en œuvre ;
- la conformité avec la norme ISO 27005.

Tableau 5 : présentation des méthodes.

Pondération

Critères	Pondération
ISO 27001	15
langue	8
Cout	7
Outils	5
Doc	2
Popularité	2

Attribution de notes

Méthode	Popularité	langue	Doc	Outils	ISO 27001	Cout
EBIOS	4	5	2	4	4	5
Mehari	4	5	2	5	4	3
Octave	3	3	5	4	5	2
Cramm	3	3	4	4	5	2

Tableau comparatif

Méthode	Popularité	langue	Doc	Outils	ISO 27001	Cout	Note finale
EBIOS	8	40	4	20	60	35	167
Mehari	8	40	4	25	60	21	158
Octave	6	24	10	20	75	14	149
Cramm	6	24	8	20	75	14	147

Source: Etude comparative pour la sélection de la méthode d'analyse du risque, GIE GAINDE 2000.

La norme internationale ISO 27005 définit un cadre commun pour gérer les risques de sécurité de l'information.. De ce fait, il ne s'agit évidemment pas d'une méthode directement applicable. Elle décrit le processus de gestion du risque en sécurité de l'information et pour chacune des activités de ce processus, les productions à réaliser mais pour appliquer ces principes et produire les livrables attendus, l'emploi d'une méthode est indispensable. L'évolution d'EBIOS permet aujourd'hui de gérer les risques conformément à l'ISO 27005, tout en bénéficiant des nombreux avantages d'EBlOS. Cette méthode s'est révélée être la plus appropriée si on base notre sélection sur des critères tels que la langue, le coût, la facilité d'usage et l'accès à des outils.

Tout au long de ces chapitres, nous pouvons retenir que le processus de gestion des risques du système d'information a pour principal but de réduire la gravité des risques jusqu'à un seuil qui soit compatible avec les objectifs de l'entrepris.

En effet, ce chapitre nous a permis de connaitre les outils et méthodes permettant gérer les risques. Les connaissances théoriques que nous avons eu à acquérir tout au long de ces chapitres nous permettrons de bien structurer notre recherche afin d'aborder la deuxième et dernière partie de notre mémoire.

Notre étude porte sur comment montrer l'importance pour une entreprise, de la mise en place d'un processus efficace de réponses aux incidents liés au système d'information, afin de les traiter et de minimiser les pertes. Pour ce faire, il nous faut une méthode à suivre afin de mener à bien ce travail. Le chapitre qui suit traitera sur la méthodologie de notre étude.

Chapitre 3 : Approche méthodologique de la recherche.

La revue de littérature nous a permis de dégager les différentes étapes pour mettre en place un processus de gestion des risques d'un système d'information.

Ce chapitre se déroulera en trois parties. La première étape consistera à présenter une méthode d'analyse ensuite, les différentes techniques de travail qui nous permis de collecter les données nécessaires. Et enfin une méthodologie d'analyse sera proposée pour expliquer comment les données recueillies seront traitées.

3.1. Méthode d'analyse.

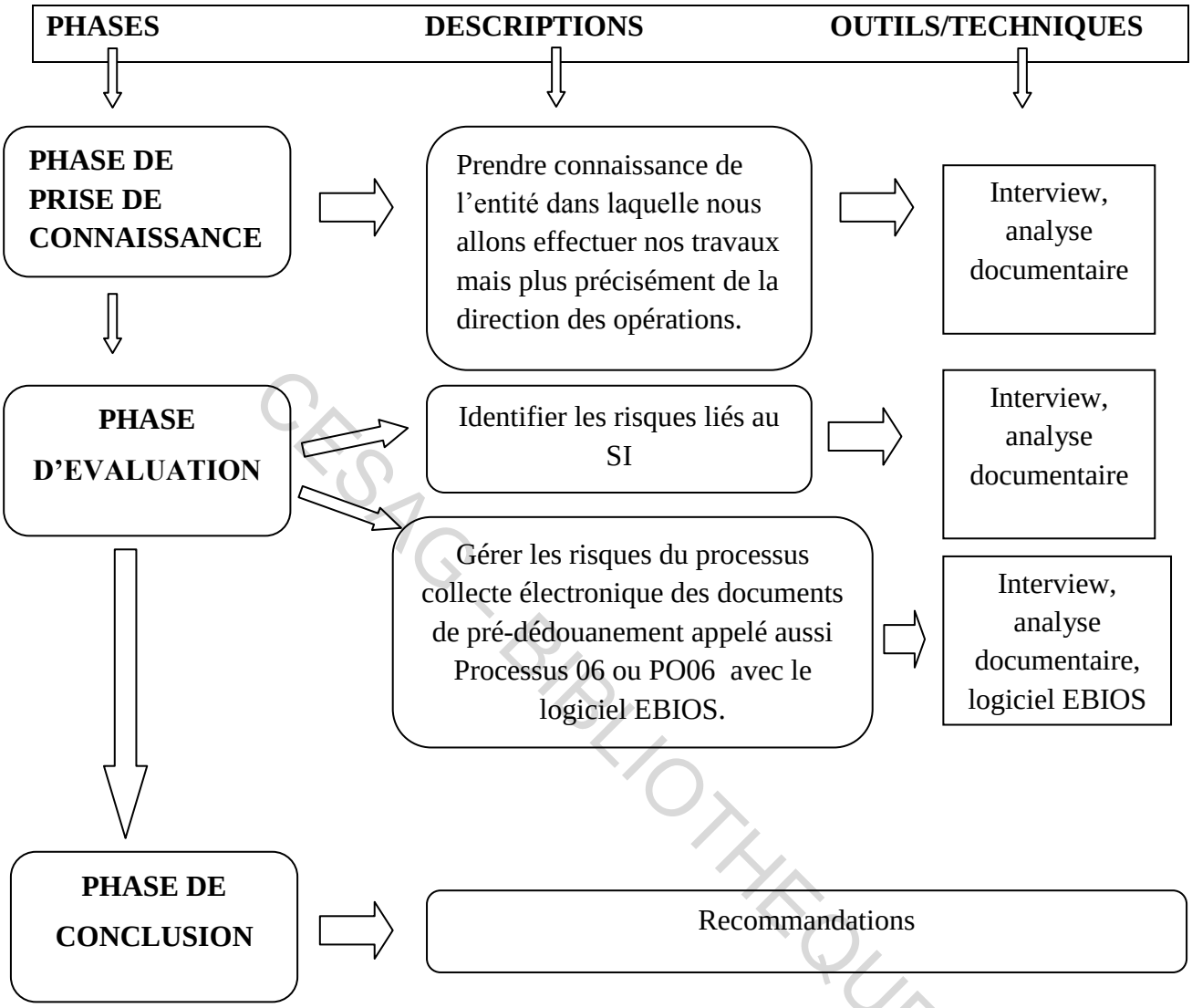
Suite à la revue théorique réalisée sur notre thème qui porte sur la mise en place d'un processus de gestion des risques du SI, nous avons conçu un modèle d'analyse qui décrit notre démarche à suivre en 3 phases successives.

Dans un premier temps, une prise de connaissance de direction est nécessaire. Elle nous permettra de recueillir des informations par rapport à leur méthodologie de travail ainsi que les risques auxquels elle est exposée.

Dans la suite, nous aurons à identifier les risques liés au SI mais plus précisément ceux affectant la direction des opérations a travers leurs travaux, cette direction maie le plus d'information interne comme externe. Et enfin, nous ferons une analyse et proposerons des recommandations.

La figure ci-dessous présente notre modèle d'analyse comme suit :

Figure 14: Modèle d'analyse.



Source : nous-mêmes

3.2. Les techniques de collecte de donnée.

Une technique est définie comme étant l'ensemble des moyens et procédés qui permettent au chercheur de rassembler des données et des informations sur son sujet de recherche. Au cours de notre recherche, nous avons fait recours principalement à la technique documentaire et la technique d'interview.

3.2.1. La phase de prise de connaissance.

Dans cette phase, nous présenteront l'entité dans son ensemble ainsi qu'une description du SI actuel et des problématiques rencontrés par la DO. Pour procéder à cela, nous utiliseront

différents technique de collecte de donnée. Selon GRAWITZ (1979 :571) la technique documentaire consiste en une fouille systématique de tout ce qui est écrit ayant une liaison avec le domaine de recherche. Il s'agit de voir le manuel de procédures du GIE gainde 2000, l'instruction de classifications des documents, la politique de sécurité de l'information.

La documentation à elle seule ne suffit pas pour donner des informations recherchées. Pour cette raison, nous avons organisé l'interview au personnel du GIE pour récolter des informations sur le fonctionnement du système d'information.

3.2.2. La phase d'évaluation.

Après avoir collecté les informations nécessaires à notre étude, présenter les risques rencontrés par la DO, nous mettrons en place un processus de gestion des risques avec l'outil EBIOS.

Nous suivrons les étapes proposés par le logiciel que nous allons adapter à l'environnement du GIE et plus précisément de la DO afin d'identifier, d'hiérarchiser, de cartographier et de gérer les risques du SI.

3.2.3. La phase de conclusion.

Dans cette phase, nous formulerons des recommandations a la suite de la présentation et de l'analyse des résultats. Il s'agira de voir quelles recommandations proposées à l'entité et principalement au service concerné par l'étude. Dans la suite, ces recommandations, si toutefois elles sont mises en œuvre, devraient leur permettre une certaine amélioration.

3.3. Méthodologie d'analyse.

Le traitement des données va nécessiter l'utilisation de logiciels comme Excel mais surtout d'EBIOS. Ceci pour permettre au mieux de gérer les risques du SI.

Nous avons effectué l'étude au moment d'un stage pratique et d'imprégnation professionnelle sur une durée de deux mois au sein de la Direction des opérations. Ce n'était pas suffisant vu tous les éléments qu'on avait à rassembler pour mener à bien notre étude.

Les techniques ont été mises en place suivant la disponibilité du personnel concerné (entre autres, le RSSI, le responsable informatique) par cette étude.

Conclusion de la première partie

La première partie de notre étude nous a permis de faire une revue littérature de notre étude en présentant successivement trois (3) chapitres. Le premier était porté sur l'environnement du système d'information. Dans ce chapitre, nous avons vu les caractéristiques de l'information, le rôle, les fonctions et les composants du SI ainsi que le SI électronique. Ces notions nous ont apportées des éclaircissements pour une meilleure compréhension de notre thème. Le second et le troisième chapitre nous ont permis de présenter la gestion des risques et la méthodologie de l'étude.

Cette partie nous permet ainsi de passer au cadre pratique de notre étude à travers le modèle de la gestion des risques choisis. Nous allons dans le chapitre suivant présenter l'entité dans laquelle nous avons fait notre étude, le GIE GAINDE 2000.

DEUXIEMEPARTIE :

Cas Pratique GIE GAINDE 2000

Introduction de la deuxième partie

Cette deuxième partie est consacrée à la gestion des risques du système d'information du GIE GAINDE 2000. Elle nous permettra de prendre connaissance du contexte pratique de notre thème. Afin de bien exercer notre travail, nous nous sommes basés essentiellement sur les travaux de la Direction des opérations en vue de nous imprégner des éléments nécessaires à la réalisation de notre étude.

Ainsi, tout au long du reste du travail, nous allons procéder à la présentation globale du GIE GAINDE 2000. Ensuite, mettre en place un processus de gestion des risques du système d'information à l'aide du logiciel EBIOS. Et enfin des recommandations seront présentées. Ceci nous amènera à décliner un plan d'action et de mise en œuvre de ces recommandations.

Chapitre 4 : Présentation globale du GIE GAINDE 2000.

Dans ce chapitre, nous allons présenter l'entité dans laquelle nous avons effectué le stage. Nous verrons donc le GIE GAINDE 2000 en tant que tel, son historique, sa structure organisationnelle, ses objectifs et missions, ses réalisations, le secteur d'activité où il évolue ainsi qu'une description de l'existant en précisant les problématiques rencontrées.

4.1. Historique.

Le GIE GAINDE 2000 est une jeune entreprise, créée en 2002 et dont l'expertise repose en partie sur l'expérience du Sénégal qui, depuis la fin des années 80, a développé et mis en service un ensemble d'outils en matière de douane. Il est le fruit d'un partenariat entre le secteur public et le secteur privé en vue de faciliter les formalités de pré dédouanement.

Initialement conçu pour assurer une logique d'assistance à la douane sénégalaise, le GIE GAINDE 2000 a, après seulement six années d'existence, consolidé un vrai savoir-faire grâce à des outils et méthodes développés et éprouvés au fil de ses missions.

Le champ de couverture des solutions GAINDE 2000 dépasse aujourd'hui le cadre du Sénégal. Les solutions informatiques proposées par GAINDE 2000 tiennent compte de la complexité des processus de dédouanement et des besoins locaux des administrations.

Le métier de GAINDE 2000 consiste à développer des solutions informatiques pour accroître l'efficacité du commerce et du transport. Au niveau international, GAINDE 2000 est reconnue comme un pionnier en matière d'intégration de solutions de la facilitation des échanges.
Engagés dans la modernisation des Douanes sénégalaises et la facilitation des opérations du commerce depuis 1995, nos experts ont su développer des compétences dans les domaines suivants :

- informatique douanière ;
- développement de systèmes d'information ;
- mise en place de guichets uniques ;
- mise en place de systèmes de paiement électronique ;
- mise en œuvre de projets informatiques ;
- support et assistance (help desk) ;
- formation ;

- etc.

Dans un souci d'amélioration de la plate-forme ORBUS, le GIE GAINDE 2000 s'est lancé dans la dématérialisation des procédures du commerce extérieur visant à alléger les démarches administratives des entreprises, favoriser leur compétitivité et améliorer l'environnement des affaires au Sénégal.

Par définition, la dématérialisation est « le fait de transformer un flux de documents, ainsi que les processus qui lui sont appliquées, en flux et traitements numériques » tout en respectant les principes de base sécuritaire et le parallélisme des formes.

Un document numérique est la résultante :

- d'une numérisation de documents physiques ou ;
- de la création dès le départ (à la source) de documents sous format numérique ou ;
- de l'archivage des données numériques ou ;
- de la transmission électronique des documents dématérialisés.

Au Sénégal, la loi sur les transactions électroniques N°2008-8 du 25 janvier 2008 consacre l'équivalence entre dossiers électroniques et documents papier.

4.2. Objectifs.

Aujourd'hui, le GIE GAINDE 2000 est entourée d'un réseau de partenaires qui accroît son champ de compétences, augmente sa capacité d'intervention et consolide son développement.
Les objectifs de la dématérialisation sont :

- l'amélioration du système de commerce électronique à l'échelle nationale ;
- l'interopérabilité entre ORBUS/GAINDE et des plates-formes internationales ;
- la dissémination en Afrique de l'Ouest.

Dans le cadre de la mise en œuvre du projet, trois organes chargés de la supervision, du contrôle et de l'exécution du projet ont été érigés :

- **le Comité de Pilotage** : instance de validation des décisions relatives au projet et de suivi des jalons ;
- **le Comité de Projet** : organe d'exécution du projet. Il propose au Comité de Pilotage un plan d'actions et en assure l'exécution une fois celui-ci validé ;

- **la Commission Administrative** : supervise tous les processus de recrutement de consultants et d'attribution des marchés.

Les résultats attendus de la dématérialisation sont :

- **Au niveau du gouvernement :**
  - une amélioration de l'environnement du commerce extérieur ;
  - une contribution à la création d'un environnement des affaires de classe internationale pour doper la compétitivité de l'économie nationale ;
  - la promotion des exportations et l'attraction des investisseurs nationaux et étrangers.
- **Au niveau des administrations publiques et privées :**
  - une meilleure planification des interventions grâce à la mise à disposition anticipée d'information d'aide à la décision ;
  - le partage des données logistiques ;
  - l'optimisation des délais ;
  - la réduction des coûts des prestations et l'amélioration de la qualité des services rendus à la clientèle.
- **Au niveau des importateurs et exportateurs :** principaux bénéficiaires de la dématérialisation des formalités du commerce extérieur, les importateurs et exportateurs pourront mener des transactions commerciales internationales prévisibles, transparentes et bénéficier des meilleures conditions de coût et de délai, gages de compétitivité et de gains de parts de marché.
- **Au niveau régional :** l'expérience sénégalaise fera l'objet d'une dissémination dans la sous-région Ouest africaine, afin de stimuler l'appropriation du concept de dématérialisation par les pays ouest africains et leur engagement à développer le commerce électronique au travers de Guichets Uniques ; assurer l'interopérabilité des systèmes avec les plates-formes existant au niveau régional et international et accroître l'efficacité du commerce régional et international.

4.3. Structure organisationnelle.

Le GIE GAINDE 2000 est composé actuellement de six(6) directions (ANNEXE N°1 : 103) :

- **Le Centre de Développement et de Recherche**

Toutes les solutions conçues et développées par le GIE GAINDE 2000 sortent de cette unité composée d'experts en TIC et management. Le département regroupe des développeurs de base de données chevronnés qui ont capitalisé plusieurs années d'expérience d'environnement Microsoft, .Net et J2EE. L'équipe technique a une expérience solide dans le développement et le déploiement de systèmes informatiques douaniers et de Guichets Uniques. Sa capacité à travailler avec différents langages positionne le GIE GAINDE 2000 parmi les structures phares intervenant sur la scène internationale dans le domaine de la facilitation commerciale.

- **Direction des opérations**

Entre autres les missions assignées au GIE GAINDE 2000, il y a la gestion du Guichet unique communément appelé ORBUS, opérationnel depuis 2004. A cet effet, le département des opérations a mis sur pied un centre de facilitation dont le rôle est de servir de relais aux utilisateurs finaux. Ce département est composé d'agents et d'opérateurs versés dans l'assistance des clients et rompus à l'utilisation d'outils informatisés de gestion et de suivi. Une unité de saisie a été ouverte au niveau de ce centre pour prendre en charge les besoins des opérateurs économiques qui ne sont pas connectés directement au système. Ainsi, les dossiers ORBUS sont imprimés sur du papier sécurisé et utilisé dans les bureaux de douane éloignés et non encore intégrés au système.

- **Direction Administrative et Financière**

Ce département s'occupe de toutes les questions administratives et financières. Elle a récemment été dotée d'un portail d'entreprise qui lui permet de prendre en charge, dans un environnement automatisé, tous les aspects liés à la gestion des ressources humaines.

- **Direction Technique et Exploitation**

Cette unité s'occupe des aspects techniques infrastructures, acquisitions d'équipement et mise en place de réseaux liés à l'implémentation des solutions du logiciel GAINDE 2000. Pour rappel le logiciel GAINDE 2000 utilise une plateforme centralisée pour le Guichet Unique. Tous les acteurs impliqués dans le processus sont dotés d'installations nécessaires aux échanges électroniques de données et d'information. Le département technique fournit

également une assistance aux utilisateurs des solutions de GAINDE 2000 ainsi qu'aux autres démembrements de la structure.

- **Direction du Développement International**

Le Directeur du Développement International du GIE GAINDE 2000 gère la négociation de tous les projets et veille à la satisfaction des exigences des clients dans le cadre des contrats déjà signés. Il est responsable de l'engagement client. Il a en charge la prospection et la promotion internationale Du logiciel GAINDE 2000. Il pilote et assure le monitoring des projets. Il a en charge la veille sur le plan applicatif. Il peut déléguer certaines activités d'exécution des projets aux autres entités de l'entreprise.

- **Direction Commercial et du Marketing**

Le Directeur Commercial et du Marketing a pour mission de créer des services à valeur ajoutée. Il assure la commercialisation et le développement des produits et services de l'entreprise. Il est chargé des offres commerciales et nationales. Dans l'exécution de sa mission, il peut demander des études au niveau de la Direction du Développement International en vue de créer de nouveaux produits ou services.

4.4. Le secteur d'activité.

Pour une meilleure performance, le GIE GAINDE 2000 a conçu des solutions qui fonctionnent au sein de l'entreprise :

- **ORBUS**

ORBUS est conçu pour faciliter les formalités du commerce extérieur par des échanges électroniques entre les différents intervenants. La plateforme relie toutes les instances administratives impliquées dans le traitement des formalités d'importation/exportation et permet aux déclarants de déposer leurs demandes par l'intermédiaire d'un formulaire électronique unique. Tous les processus sont automatisés et les résultats sont disponibles en format souple, avec la possibilité d'imprimer des copies papier. La solution, souple et modulaire est très susceptible de se conformer aux différentes techniques, aux contraintes organisationnelles et géographiques.

- **Trade X**

L'application Trade X est la solution informatique destinée à des fins douanières. Avec ses différentes composantes, Trade X couvre toutes les procédures de dédouanement, de la transmission électronique du manifeste (Edifact) pour le dédouanement des marchandises, y compris la gestion des entrepôts, la déclaration, le transit et les processus de paiement. Trade X est un outil complet adaptable aux exigences d'une administration douanière moderne. Il est facile à déployer et a offert aux douanes la possibilité d'échanger des données avec d'autres entités.

- **CORUS**

La plateforme de CORUS est le composant de paiement électronique de l'ensemble GAINDE. Il offre au déclarant la possibilité de s'acquitter du paiement des droits de douane par voie électronique avec des garanties de sécurité dans les transactions. L'application est liée au système douanier et communique avec les systèmes Banks 'in-house de commerce.

4.5. Missions.

Le Groupement d'intérêt Economique a pour objet l'exploitation technique et commerciale des produits Du GIE GAINDE 2000. Les objectifs spécifiques suivants lui sont assignés dans ses statuts :

- assurer le déploiement des produits du GIEGAINDE 2000 ;
- doter les produits d'un label normalisé qui en garantit la fiabilité et la crédibilité sur le plan international ;
- conduire les actions de « standardisation » des produits du GIE GAINDE 2000 afin de les rendre opérationnels sous toutes plates-formes pertinentes ;
- engager l'expérimentation, en matière de réseau, du mode de communication par radio-transmission (Wireless) ;
- définir et exécuter une bonne politique de prospection et de promotion des produits du GIE GAINDE 2000 pour son implantation au niveau international ;
- concevoir et développer des modules additionnels pour optimiser les fonctionnalités existantes des produits de GAINDE 2000 et en enrichir le champ d'exploitation ;
- assurer la création, l'acquisition, l'exploitation de toute activité se rattachant aux objets précités.

4.6. Partenariat.

Le GIE GAINDE 2000 entretiens plusieurs partenariats tant au niveau national qu'au niveau international.

4.7. Services offerts.

Le GIE GAINDE 2000 fournit aux utilisateurs une assistance ponctuelle par téléphone, fax, mail ou sur site à travers :

4.7.1. Le centre de facilitation.

Le centre de facilitation est créé d'une part, pour assurer le back office du système ORBUS et d'autre part, pour prendre en charge les besoins de tous les utilisateurs qui n'ont pas de moyens d'accès au système. Des opérateurs de saisie prennent en charge leurs requêtes et assurent le suivi de leurs dossiers. Pour répondre aux demandes des utilisateurs, le centre de facilitation tient à la disposition des utilisateurs :

- Un call center ouvert du lundi au vendredi de 8h30 à 17h30.
- Un espace web utilisateur

4.7.2. Help Desk.

Tous les utilisateurs qui ont des dossiers en cours de traitement, peuvent bénéficier des services du Help Desk :

- informations générales sur les procédures d'ORBUS ;
- Assistance dans la saisie des dossiers ;
- Assistance technique ;
- Résolution on-line des difficultés rencontrées ;
- Suivi de l'état de traitement des dossiers ;
- Signalisation incident ou retard traitement.

La formation est destinée aux utilisateurs du système ORBUS et permet une parfaite maîtrise de l'application, de l'initialisation (création) d'un dossier à la collecte des documents.

Des formations ponctuelles sont dispensées à la demande des utilisateurs.

4.8.Description de l'existant étudié.

- **Objectif de la description**

Cette description sur l'existant informatique au niveau du centre de recherche a pour but de faire une analyse de l'existant en termes de ressources matérielles et logicielles. Elle nous a permis de mener à bien les objectifs suivants :

- évaluer la situation actuelle en faisant ressortir les ressources existantes au sein du GIE GAINDE 2000;
- avoir les éléments concernant l'environnement d'exploitation général des ressources de l'entreprise ;
- identifier les risques rencontrés par la DO.

En d'autres termes, ces travaux d'analyse nous ont permis de décrire la situation actuelle du centre et de dégager les ressources susceptibles d'être prises en comptes dans les besoins qui seront nécessaires pour la mise en œuvre d'un processus de gestion des risques du SI.

- **Démarche suivi pour l'analyse de l'existant**

Lors de nos travaux, l'étude de l'existant nous a conduit à interviewer certaines personnes à l'instar de :

- le responsable informatique, rencontré pour les informations concernant les ressources matérielles et logicielles dont disposent l'institution ;
- le RSSI : pour les informations concernant le système d'information et sa sécurité.

- **Les ressources techniques**

Le tableau suivant montre les équipements que la direction déploie en son sein en nombre approximatifs : (ANNEXE N°2 : 104).

- **Description du SI actuel**

Dans cette rubrique, nous présentons l'ensemble des personnes ainsi que les matériels mise à disposition au niveau de la direction des opérations et les différentes étapes dans la procédure actuelle de collecte de données électroniques.

Pour traiter les informations qui lui parviennent, la direction utilise différentes types d'équipements.

Il existe au niveau du processus collecte de données informatiques, des sous processus regroupant un ensemble d'étapes pour la bonne marche du travail au niveau de la direction. Ils sont au nombre de quatre (4) activités :

- **Collecter, transmettre et traiter documents de pré dédouanements :**
  - documents de Pré-dédouanement ;
  - données du Document.
- **Réception et Initialisation des Dossiers :**
  - facture Règlement ;
  - données du Document ;
  - obtention Numéro ORBUS Facture Provisoire ;
  - besoin en Formation Besoin en Installation.
- **Gérer la souscription et l'accueil des clients :**
  - demande de Souscription ;
  - formulaire Initialisation-Facture Commerciale-Souscription ;
  - référence Souscription Code d'accès Remise « Token » ;
  - besoin en Formation Besoin en Installation.
- **Suivre les dossiers et assister les clients :**
  - requête état des dossiers ;
  - information état des dossiers ;
  - demande Amendement -dossiers ORBUS Autorisation.

4.9. Problématique.

La DO manie des informations confidentielles venant de sa clientèle dans le cadre de la facilitation et la transmission électronique des données nécessaire pour la délivrance des documents de pré dédouanement, mais nous avons constaté certains risques liés à la bonne marche du travail effectué au niveau de la DO:

- diffusion d'informations confidentielles des clients ;
- incident non résolu dans les délais ;
- perte de documents déposés

- erreur lors de l'initialisation des dossiers ;
- indisponibilité du système ;
- niveau de recevabilité ;
- amendement ;
- non-respect des délais de délivrance ;
- intrusion frauduleuse au niveau du système.

Ce chapitre nous a permis d'avoir une idée de la configuration de la structure dans laquelle s'est déroulé notre stage. Nous avons spécifiquement, à travers ce chapitre fait la connaissance de la Direction des opérations en présentant ses objectifs et missions.

Chapitre 5: Processus de gestion des risques du système d'information du GIE GAINDE 2000.

Nous avons tenté ici de collecter les éléments nécessaires à la gestion des risques, afin qu'elle puisse être mise en œuvre dans de bonnes conditions, qu'elle soit adaptée à la réalité du contexte d'étude et que ses résultats soient pertinents et utilisables par les parties prenantes.

Dans ce chapitre, nous présenterons le processus de gestion des risques du SI selon GAINDE 2000 puis nous appliquerons la méthode EBIOS par le biais du logiciel, au sous système « collecte électronique des documents de pré-dédouanement » appelé aussi processus 06 ou PO06.

Cette section sera consacrée à la présentation de l'évaluation des risques que nous avons eu à voir lors de notre étude au sein du GIE GAINDE 2000.

5.1. Contexte de gestion des risques du SI.

La gestion du risque protège le patrimoine du GIE GAINDE 2000 et crée de la valeur pour celle-ci et ses parties prenantes :

- confiance de la part des clients et partenaires,
- confiance des actionnaires,
- fiabilité de l'image de marque,
- disponibilité du système d'information et donc fiabilité de la production,
- protection des données en Confidentialité et en Intégrité,
- continuité d'activité en cas d'incident ou de sinistre majeur,
- conformité règlementaire (transparence, conformité juridique, respect des obligations légales.

C'est dans ce cadre que le processus de maitrise des risques liés à la sécurité de l'information contribue à la politique de sécurité de l'information en identifiant et maitrisant les risques inhérents aux informations manipulées, traitées et stockées au sein de notre système d'information.

5.2. Objectifs de sécurité de l'information.

L'objectif de sécurité de l'information est de mettre en place des mesures permettant de restreindre les risques identifiés afin de garantir les critères de sécurité ci-dessous :

- **Intégrité des données** : permettre à nos partenaires de retrouver leurs données à la suite d'une défaillance technique.
- **Confidentialité des données** : offrir à nos partenaires un cadre sécurisé d'échange de données en réduisant les accès non autorisés
- **Disponibilité des données** : permettre à nos partenaires d'accéder aux données au moment voulu s'ils sont autorisés.

5.3. Présentation de la gestion des risques au sein du GIE GAINDE 2000.

Nous allons voir l'identification des actifs.

5.3.1. Les Actifs.

La première étape consiste à l'identification de tous les actifs dans le cadre du SMQSI par le RSSI, c'est à dire de tous les actifs susceptibles d'affecter la confidentialité, l'intégrité et la disponibilité de l'information dans l'organisation. Les actifs peuvent inclure des documents sur support papier ou électronique, applications et bases de données, des personnes, du matériel informatique, des infrastructures et des services externes / processus externalisés.

5.3.2. L'Inventaire des Actifs.

Les actifs du périmètre de certification sont les actifs primaires et tous les autres actifs aidant à la réalisation des activités sont les actifs supports (Matériel, logiciel, réseau, personne, site et organisation).

5.3.3 Détermination des propriétaires d'actifs à risque.

Lors de l'identification des actifs, il est également nécessaire d'identifier leurs propriétaires afin d'assumer la responsabilité et la traçabilité de l'actif. Il s'agit de la personne ou unité organisationnelle responsable de chaque actif. Le RSSI a mis en place des démarches, ou on peut faire appel au propriétaire de l'actif (ressource ou organisation) pour évaluer ou traiter les risques identifiés sur l'actif.

5.3.4. Valeur de l'actif en termes de Disponibilité-Intégrité-Confidentialité (DIC).

La valeur de l'actif doit intégrer la confidentialité, l'intégrité et la disponibilité ou différentes propriétés importantes de l'actif qui pourraient être affectées explique le RSSI. La DIC se calcule par (D+I+C)/5. La valeur de l'actif en termes de protection est ainsi définie. Les actifs avec une valeur supérieure ou égale à 4 seront ainsi traités.

5.3.5. Analyse des risques.

Selon le RSSI, il s'agira de :

- l'identification des risques ;
- Faire la relation entre les risques et les actifs
- Faire l'estimation des risques

5.3.6. Identification des risques.

L'étape suivante consiste à identifier toutes les menaces et les vulnérabilités associées à chaque actif. Les menaces et les vulnérabilités sont identifiées à l'aide des catalogues figurant dans le tableau d'évaluation des risques. Chaque actif peut être associé à plusieurs menaces. Chaque menace identifiée est associée à une liste de mesures.

5.3.7. Estimation des risques.

L'impact mesure l'importance des conséquences, l'importance des impacts envisagés en cas de survenance du risque.

Pour chaque impact, il est convenu que les niveaux suivront l'échelle présentée au tableau ci-dessous :

Tableau 6 : L'échelle de l'impact.

NIVEAU D'IMPACT	VALEUR ASSOCIEE
Mineur	**1**
Significatif	**2**

Important	**4**
Majeur	**8**

Source : DIENG (2015 : 5)

L'assistante du RSSI nous explique qu'au moment de la détermination des seuils d'impact, il peut être utile de considérer que :

- l'estimation des conséquences peut être exprimée en termes qualitatifs ou quantitatifs ;
- la valeur d'une conséquence dépend généralement de la valeur et de la criticité de l'actif affecté
- cette estimation est obtenue suite à l'analyse de l'impact sur les activités.

L'impact peut avoir des conséquences tels que :

- incapacité de l'entreprise à remplir sa mission ;
- infraction ou manquement aux lois, aux règlements ou à d'autres normes applicables ;
- perte d'image ou dommage à la réputation ;
- perturbation des activités de l'entreprise ;
- impossibilité de remplir ses obligations contractuelles ;
- pertes financières, augmentation des coûts ;
- atteinte à la sécurité de la clientèle, du personnel, des partenaires ;
- dommages moraux ou matériels.

La vraisemblance exprime la possibilité de survenance du risque, autrement dit la potentialité que l'accident se produise. Le GIE définie l'échelle de vraisemblance comme suit :

Tableau 7 : l'échelle de la vraisemblance.

	Niveau de vraisemblance	Valeur associée
1	Très faible	**1**
2	Faible	**2**
3	Forte	**4**
4	Très forte	**8**

Source : DIENG (2015 : 6)

5.3.8. Evaluation des risques.

L'évaluation des risques est mise en œuvre à travers le tableau d'évaluation des risques. Elle consiste à comparer le niveau de risque estimé aux critères d'évaluation et d'acceptation du risque, puis à les prioriser. Le processus d'évaluation des risques est coordonné par le RSSI, l'identification des menaces et des vulnérabilités est réalisée par les propriétaires d'actifs et l'évaluation des conséquences et de la probabilité est effectuée par les propriétaires d'actifs à risque.

5.3.9. Traitement des risques.

Le RSSI propose 4 traitements possibles de chacun des risques identifiés :

- l'acceptation ou conservation,
- l'évitement,
- le transfert,
- la réduction.

Lorsque la décision de traitement du risque est prise, le RSSI et son assistante identifient les risques c'est-à-dire ceux qui persistent après la mise en place des mesures de sécurité. S'ils sont jugés inacceptables, le RSSI défini des mesures de sécurité supplémentaires. C'est dans cette optique que le Comité de Gestion du Risque (CGR) a décidé, suite à des rencontres, de traiter seulement les risques qui sont élevés et moyens.

- **Pour les risques élevés (Fortes) :** ces risques doivent absolument être évités ou réduits par l'application de mesures de sécurité diminuant leur impact et leur vraisemblance. Dans l'idéal, il conviendrait même de s'assurer qu'ils sont traités à la fois par des mesures indépendantes de prévention (actions avant le sinistre), de protection (actions pendant le sinistre) et de récupération (actions après le sinistre) ;
- **Pour les risques Moyens (Moyennes) :** ces risques doivent être réduits par l'application de mesures de sécurité diminuant leur vraisemblance. Les mesures de récupération devront être privilégiées ;
- **Pour les risques faibles (Basses) :** ces risques peuvent être pris, d'autant plus que le traitement des autres risques devrait également contribuer à leur traitement.

Le RSSI procède ensuite à l'identification des propriétaires des risques au niveau de chaque direction métier. Chaque risque est attribué à un propriétaire du risque. Ce dernier a une responsabilité sur le traitement du risque et son suivi dans le temps.

5.3.10. Traitement des risques résiduels répétitifs.

Il s'agit de l'ensemble des risques qui subsistent même après le traitement du risque. Dans ce cas, les risques résiduels ayant une forte occurrence et un faible impact doivent être considérés comme des incidents de sécurité ; ils sont gérés conformément à la procédure de gestion des non conformités, incidents et anomalies.

Les risques résiduels à faible occurrence et fort impact sont considérés comme des sinistres et doivent faire l'objet d'un traitement particulier qui sera défini par le comité de gestion de la continuité des activités.

5.3.11. Déclaration d'application et plan de traitement du risque.

Le but principal de l'appréciation des risques consiste à intégrer et produire la déclaration d'applicabilité (DDA) du SMQSI à partir des menaces.

La DDA représente la portée des contrôles de l'annexe A, que l'organisation veut mettre en œuvre. La norme ISO 27001 dispose d'une annexe A qui propose 114 mesures de sécurité classées en 14 catégories (politique de sécurité, sécurité du personnel, contrôle des accès). Cette annexe normative n'est qu'une liste qui ne donne aucun conseil de mise en œuvre au sein de l'entreprise. C'est pourquoi la gestion des risques est essentielle dans la norme ISO 27001, il est l'instrument que le pilote du processus PP03 (Maitrise des risques de la sécurité de l'information) met en place pour définir la DDA et c'est-à-dire les contrôles.

Une fois les risques à mitiger identifiés, le RSSI et son assistante isole les mesures à appliquer en comparant avec les mesures de l'annexe A. Ce plan peut être mis à jour au besoin en fonction des incidents et nouvelles contraintes.

5.3.12. Communication, surveillance et revue.

La communication relative aux risques SSI représente l'échange ou le partage d'informations concernant les risques. Une fois le risque résiduel validé avec le propriétaire des risques, le risque est communiqué :

- **à la direction** : à travers le comité de gestion des risques afin qu'ils participent à l'identification et au choix des mesures de sécurité appropriées
- **aux propriétaires des actifs et des risques** afin qu'ils soient informer de la responsabilité qui leur incombent sur la bonne gestion de l'actif et du risque tout au long de son cycle de vie.
- **à l'ensemble des utilisateurs et aux propriétaires des risques** afin que les actifs soient correctement classes et protégés.

La gestion des risques est revue, la périodicité est annelle ou en cas de modification de l'un des ses fondements (critères d'appréciations, révision de l'inventaire et de sa méthodologie). Cette révision est effectuée par le comité de gestion du risque.

Chapitre 6 : Analyse du processus de gestion des risques du SI avec EBIOS.

Dans ce chapitre, nous appliquerons la méthode EBIOS par le biais du logiciel, au sous système « collecte électronique des documents de pré-dédouanement » appelé aussi processus 06 ou PO06 afin de gérer les risques rencontrés.

6.1 Etude du contexte.

Nous allons d'identifier globalement le système cible et de le situer dans son environnement pour déterminer précisément la cible de l'étude.

6.1.1. La définition du cadre de la gestion des risques.

L'objectif de l'étude est de gérer les risques SI sur le long terme. Nous avons souhaité que les risques liés à l'information qui pourraient empêcher l'organisme d'atteindre ses objectifs soient gérés, et ce, de manière continue, afin d'être au plus proche d'une réalité en mouvement.

Par ailleurs, nous n'avons pas exclu l'idée d'une certification à terme des principales activités de l'entreprise selon l'ISO 27001. Il nous a paru également nécessaire de souligner l'intérêt d'exploiter les meilleures pratiques reconnues internationalement (ISO 27005). .

6.1.2. La description du contexte général.

L'organisme étudié ici est le GIE GAINDE 2000, avec un capital de 100.000.000 CFA. La politique de gestion des risques est déclinée en axes stratégiques que voici :

- Une gestion des risques intégrée

Le risque est défini comme un « scénario, avec un niveau donné, combinant un événement redouté sur son activité, et un ou plusieurs scénarios de menaces » d'après GAINDE 2000. Son niveau correspond à l'estimation de sa vraisemblance et de sa gravité.

En matière de gestion des risques, les rôles et responsabilités sont les suivants :

- L'administrateur général est pleinement responsable des risques pesant sur sa société ;

- le directeur adjoint a été mandaté pour animer la gestion des risques de sécurité de l'information ; il est ainsi responsable de la réalisation des études de risques ;
- un comité de suivi, composé d'un membre de chaque service, réalisera la première étude de risques et se réunira ensuite tous les six mois afin de faire le point sur les évolutions à apporter à la gestion des risques de sécurité de l'information.

Les interfaces de la gestion des risques sont les suivantes :

- La gestion des risques de sécurité de l'information fait partie intégrante de la gestion de GAINDE 2000 ; à ce titre, ses résultats sont pris en compte dans la stratégie de la société;
- l'ensemble de la société est concerné par la gestion des risques de sécurité de l'information, tant pour apprécier les risques que pour appliquer et faire appliquer des mesures de sécurité.

6.1.3. Délimitation du périmètre d'étude.

Le sujet de l'étude porte sur le cœur de métier de GIE GAINDE 2000. Nous nous intéressons maintenant à la gestion des risques d'un système cible. Le système-cible correspond donc en un sous-ensemble du SI qui concerne l'un des métiers de la société. Il est donc représenté par :

- La collecte électronique des documents de pré-dédouanement appelé aussi processus 06 ou PO06.

Et ma mission est de mettre en place un processus de gestion des risques pour le Processus 06 avec la méthode EBIOS.

6.1.4. Identification des paramètres à prendre en comptes.

L'identification des contraintes nous a permis de recenser celles qui ont un impact sur le système-cible et de déterminer celles sur lesquelles il est toutefois possible d'agir. Elles complètent et amendent les contraintes de l'organisme déterminées précédemment.

Dans notre cas, nous avons relevé quelques contraintes qui étaient liées à l'activité :

- **Relatives au personnel** :
    - le personnel de nettoyage intervient de 7h à 15h ;

- la réception des clients se fait dans les bureaux des commerciaux, mais des visites ont parfois lieu au bureau d'études.

- **d'ordre calendaire**
  - la période de pointe se situant à des dates précises.
- **d'environnement**
  - location à l'aéroport ;
  - location à Fahd centre-ville ;
  - voisinage avec une banque et autres commerces.
- **d'ordre technique**
  - code source disponible 24h/24 ;
  - base de données disponible 24h/24 ;
  - antivirus à jour ;
  - licence de logiciels.

(ANNEXE N°3 : 107)

6.1.5. Identification des sources de menaces.

Au cours de notre étude, nous avons relevé à travers des interviews avec les responsables de la direction ainsi que des documents fournis, une liste des sources de menaces pouvant affecter la bonne marche de la direction. Vous avez ainsi :

Tableau 8 : identification des sources de menaces.

Types de sources de menaces	Retenu ou non	exemple
Source humaine interne, malveillante, avec de faibles capacités	Non, la direction des opérations n'estime pas y être exposée	
Source humaine interne, malveillante, avec des capacités importantes	oui	Employé peu sérieux
Source humaine interne, malveillante, avec des capacités illimitées	oui	Employé peu sérieux
Source humaine externe, malveillante, avec de faibles capacités	Non, la direction des opérations n'estime pas y être exposée	
Source humaine externe, malveillante, avec des capacités importantes	oui	Concurrent (éventuellement en visite incognito) Maintenance informatique

Source humaine externe, malveillante, avec des capacités illimitées	oui	Personnel de nettoyage soudoyé
Source humaine interne, sans intention de nuire, avec de faibles capacités	Non, la direction des opérations n'estime pas y être exposée	
Source humaine interne, sans intention de nuire, avec des capacités importantes	Non, la direction des opérations n'estime pas y être exposée	
Source humaine interne, sans intention de nuire, avec des capacités illimitées	oui	Employé peu sérieux
Source humaine externe, sans intention de nuire, avec de faibles capacités	oui	Client Employé peu sérieux partenaire
Source humaine externe, sans intention de nuire, avec des capacités importantes	oui	Fournisseur d'accès internet Hébergeur
Source humaine externe, sans intention de nuire, avec des capacités illimitées	Non, la direction des opérations n'estime pas y être exposée	
Code malveillant d'origine inconnue	oui	Virus non ciblé
Phénomène naturel	oui	Foudre, usure
Catastrophe naturelle ou sanitaire	oui	maladie
Activité animale	Non, la direction des opérations n'estime pas y être exposée	
Evènement interne	oui	Incendie des locaux

Source : nous-mêmes.

(ANNEXE N°4 : 108).

6.1.6. Préparation des métriques : Définition des critères de sécurité et élaboration des échelles de besoins.

Afin d'exprimer les besoins de sécurité, nous avons retenu des critères de sécurité en nous basant sur la sécurité des systèmes d'informations qui prévoit trois (3) critères. Et pour chaque critère de sécurité, nous lui avons affecté un niveau d'échelle. Au niveau de la DO, les critères de sécurité sont aux nombre de quatre (4) : la confidentialité, la disponibilité, l'intégrité et la preuve. (ANNEXE N°5 : 109).

Nous allons vous présentez un tableau comportant les critères de sécurités les niveaux d'échelle.

Tableau 9 : définition des critères de sécurité et élaboration des échelles de besoins

Critère de sécurité	Niveau d'échelle
Confidentialité	1. public 2. usage interne 3. privé 4. confidentiel
Disponibilité	1. moins de 4h 2. entre 4h et 24h 3. entre 24h et 72h 4. plus de 72h
Intégrité	1. intègre 2. maitrisé 3. détectable
Preuve	1. négligeable 2. faible 3. forte 4. grave

Source : nous-mêmes.

Le niveau d'échelle varie de 1 à 4 pour la disponibilité, la confidentialité et la preuve tandis que l'intégrité varie de 1 à 3.

Concernant la confidentialité, le niveau d'échelle est déterminé sous la base d'une procédure de classification de documents instauré au niveau du GIE GAINDE 2000. Les documents peuvent être à usage public avec un niveau d'échelle faible donc il n'ya aucun impact négatif sur les activités de la DO, à usage interne c'est-à-dire que les documents ne doivent pas quitter le GIE GAINDE 2000, privé et enfin confidentiel pour dire qu'un groupe d'individu ciblé ont accès à l'information.

Le niveau d'échelle de la disponibilité de l'information suit une politique de plans de reprise d'activité (PRA) et de plans de continuité d'activité (PCA). Quand elle est disponible en moins de 4h de temps, le niveau d'échelle correspond à 1 ce qui est acceptable. Et quand elle

atteint 4 cela montre une indisponibilité de l'accès à l'information qui peut impacter négativement sur les opérations de la DO.

Pour ce qui concerne l'intégrité et la preuve, le GIE a suivi le niveau d'échelle par défaut se trouvant dans l'application EBIOS qui est généré automatiquement et qui convient à ce dernier.

6.1.7. L'élaboration d'une échelle de niveaux de gravité.

L'échelle suivante a été utilisée pour estimer les niveaux de gravité des scénarios de menaces et des risques.

Tableau 10 : l'élaboration d'une échelle de niveaux de gravité

Niveaux de l'échelle	Description détaillée de l'échelle
négligeable	la direction des opérations surmontera les impacts sans aucune difficulté.
significative	la direction des opérations surmontera les impacts malgré quelques difficultés.
importante	la direction des opérations surmontera les impacts avec de sérieuses difficultés.
critique	la direction des opérations ne surmontera pas les impacts
catastrophique	Sa survie est menacée

Source : nous-mêmes.

(ANNEXE N°6 : 110).

6.1.8. L'élaboration d'une échelle de niveaux vraisemblable.

L'échelle suivante été utilisée pour estimer la vraisemblance des scénarios de menaces et des risques.

Tableau 11 : l'échelle de niveau vraisemblable

Niveaux de l'échelle	Description détaillée de l'échelle
1. Très peu probable	(< 1 fois / an)
2. Peu probable	(2 à 3 fois/an)
3. probable	(tous les mois)

4. très probable	Permanent

Source : nous-mêmes (ANNEXE N°7 : 111)

6.1.9. Définition des critères de gestion des risques.

Nous avons tenté ici de formaliser les règles choisies pour faire des choix tout au long de notre étude. Toute action de l'étude qui nécessite une décision peut faire l'objet d'un critère de gestion de risques.

Les critères nous permettre d'estimer et d'évaluer les risques, afin de prendre des décisions concernant leur appréciation et leur traitement.

Ils vont porter sur : l'analyse de tous les événements redoutés, de l'évaluation de chaque événement redouté, l'analyse de tous les scénarios de menaces, l'évaluation de chaque scénarios de menace, l'analyse des risques, l'évaluation des risques et enfin le choix des options de traitement des risques. (ANNEXE N°8 : 112).

6.1.10. L'identification des biens.

Nous allons passer à l'identification des biens au sein du périmètre de l'étude qui est la direction des opérations portant comme processus la collecte électronique des documents de pré-dédouanement.

- Les biens essentiels

Dans le cadre du sujet d'étude, la DO a retenu un processus suivant en tant que biens essentiels :

Tableau 12 : identification des biens essentiels

Processus métier	Activité au sein du processus
Collecte électronique des documents de pré-dédouanement	Collecter, transmettre et traiter des documents de pré dédouanements
	Réception et Initialisation des Dossiers
	Gérer la souscription et l'accueil des clients
	Suivre les dossiers et assister les clients

Source : nous-mêmes. (ANNEXE N°9 : 113).

- Les biens supports

Concernant ces biens, nous allons prendre connaissance des composants du système d'information, qu'il s'agisse du personnel, du matériel informatique, des locaux etc. On note que ces biens supports possèdent des vulnérabilités que des sources de menaces pourront exploiter, portant ainsi atteinte aux biens essentiels. (ANNEXE N°10 : 116).

6.1.11. Lien existant entre les biens essentiels et les biens supports.

Nous allons déterminer le lien entre les biens essentiels et les biens supports. Ceci nous permet de révéler la criticité de ces derniers, ainsi que les risques véritables pesant sur le périmètre de l'étude.

Il suffit de se demander sur quels biens supports, parmi ceux identifiés dans l'action précédente, repose chaque bien essentiel. On s'interroge ainsi sur les biens supports qui vont stocker ou traiter les biens essentiels, à un moment ou un autre de leur cycle de vie. (ANNEXE N°11 : 117).

6.1.12. Les mesures de sécurité existantes.

Il est nécessaire de recenser l'ensemble des mesures de sécurités existantes sur les supports ou d'ores et déjà prévu par le l'entité.

Pour les biens support identifié prenant en compte l'un des critères de sécurité, nous nous interrogeons sur l'existence de mesures de sécurité. Principalement, nous nous sommes basés sur le document de politique de sécurité de l'information mais au niveau de la DO.

Tableau 13 : Les mesures de sécurité existantes.

Biens supports	Mesure de sécurité
LOGiciel	mettre en place une gestion des profils d'accès, système de contrôle de la traçabilité, enregistrement des incidents dans le help desk, système d'archivage des documents déposés, suivi mensuel du bilan de la demande et des réclamations clients,

	mettre en place un indicateur pour suivre les erreurs, vérification quotidienne et relance technique, orbus assistance, suivi/assistance pour identifier les points de blocage, gestion des accès aux données,
LOCal	Vérification de l'identité d'une personne avant un accès aux locaux, Climatisation des salles hébergeant les données numériques.
MATeriel	Mise en veille par l'utilisateur avant de quitter le poste de travail, Création d'un code alphanumérique pour un accès au poste de travail pour chaque utilisateur
PERsonnel	Faire signer à l'employer le code d'éthique de GAINDE 2000, vérification et contrôle des demandes d'amendement,

Source : nous-mêmes (ANNEXE N°12 : 118).

6.2. Etude des évènements redoutés.

Nous allons voir ici les événements liés à la sécurité de l'information que la DO redoute. Et ensuite, fournir des éléments nécessaires au choix de traitement des risques y afférents et à la définition des priorités de traitement.

Tableau 14: les événements redoutés par le SI /au niveau du PO06

Evénements redoutés
1. Perte de données clients non enregistrée.
2. Intrusion dans les fichiers clients de l'entité d'une personne n'appartenant pas au GIE GAINDE 2000/DO.
3. Intrusion d'une personne non autorisé dans les locaux du GIE 2000/DO.
4. Accès à distance sur une application telle qu'ORBUS d'une personne non autorisée.

Source : nous-mêmes

6.2.1. L'analyse de tous les événements redoutés.

Nous avons porté notre étude sur l'identification et l'estimation des événements redoutés pour chaque critère de sécurité et chaque bien essentiel. Nous avons ainsi fait ressortir les besoins

de sécurité des biens essentiels, les impacts encourus au cas où ils ne seraient pas respectés les sources de menaces susceptibles d'en être à l'origine, et leur attribuer un niveau de gravité.

Chaque ligne suivant représente un événement redouté (16 éléments) par la DO (bien essentiel, critère de sécurité, besoin de sécurité selon les échelles de besoin, sources de menaces et impacts). La gravité de chaque événement redouté est estimée sans tenir compte des mesures de sécurité existantes donc « brut » (ANNEXE N°13 : 119)

6.2.2. L'évaluation de chaque événement redouté.

Pour juger l'importance des événements redoutés nous allons les hiérarchiser selon les critères de gestion des risques retenues. Puis fournir les éléments nécessaires pour décider de développer l'étude concernant chaque événement redouté, de traiter ou non les risques afférents et de prioriser la mise en œuvre de leur traitement.

Pour ce faire, nous pouvons positionner chaque événement redouté dans un tableau selon leur gravité. Nous avons utilisé un libellé court et explicite, reflétant l'atteinte d'un critère de sécurité d'un bien essentiel, pour chaque événement redouté.

L'importance relative des événements redoutés précédemment analysés (identifiés et estimés) est évaluée à l'aide de ce tableau (ANNEXE N°14 : 121)

6.3. Etude des menaces

Cette section consiste à présenter les scénarios de menaces pesant sur le périmètre de l'étude.

6.3.1. Etude des scénarios de menaces.

- l'appréciation des scénarios de menaces

Pour cette activité, nous avons fait une identification des scénarios de menaces pour chaque critère de sécurité et pour chaque bien support identifié, les estimer en termes de vraisemblance. Les scénarios de menaces ont été obtenus en questionnant les parties prenantes sur ce qu'elles savent et en approfondissant la réflexion jusqu'à ce que tous les éléments aient été formulés.

Le tableau suivant présente un extrait des scénarios de menaces potentiellement réalisables dans le cadre du sujet de l'étude. (ANNEXE N°15 : 122)

Tableau 15 : Les scenarios de menaces.

Scenario de menace	Source de menace	Vraisemblance
PER : menace pesant sur le personnel causant une indisponibilité	Employé peu sérieux Maladie Maintenance informatique non effectuée	Probable
LOG : menace pesant sur les logiciels causant une perte de donnée	Virus non ciblé Mis à jour antivirus non effectuée Absence de pare-feu	Très probable
LOC : menace pesant sur les locaux causant une intrusion	Employé peu sérieux Cotraitant Fournisseur d'accès internet Hébergeur	Peu probable
MAT : menace pesant sur le matériel informatique et autre causant un vol, des dégâts	Employé peu sérieux Panne d'électricité Clients	Peu probable

Source : nous-mêmes

6.3.2. L'évaluation de chaque scénario de menace.

Nous allons juger l'importance des scénarios de menaces en les hiérarchisant selon les critères de gestion des risques retenus. Il convient essentiellement de fournir aussi les éléments

nécessaires pour décider de traiter ou non les risques y afférents et de prioriser la mise en œuvre de leur traitement.

Pour ce faire nous avons positionné chaque scénario de menace dans un tableau trié selon leur vraisemblance. L'importance relative des scénarios de menaces précédemment analysés est évaluée de la façon suivante. (ANNEXE N°16 : 125).

6.4. Etude des risques.

Cette partie consiste à mettre en évidence et à définir les caractéristiques des risques réels pesant sur le périmètre de l'étude.

6.4.1. L'analyse des risques.

Nous avons mis en évidence l'ensemble des risques qui pèsent réellement sur le périmètre de l'étude et déterminer leur gravité et leur vraisemblable, une première fois sans tenir compte des mesures de sécurité existantes, et une seconde fois en les prenant en compte. Nous allons ainsi faire le lien entre événements redoutés et les scénarios de menaces. Pour identifier les risques nous allons pour chaque événement redouté, retenir les scenarios de menaces qui :

- Concernent les biens supports liés au bien essentiel considéré ;
- touchent le même critère de sécurité ;
- sont à l'initiative des mêmes sources de menaces.

Et pour l'estimation du niveau de chaque risque identifié en termes de gravité et de vraisemblance, nous avons exploité les données produites dans les études précédentes.

La direction des opérations a établi une liste des risques redoutés et des scenarios de menaces précédemment appréciés. Sur un ensemble de 96 risques recensé au niveau du GIE, 16 concernent la direction des opérations. Ces derniers menacent les critères de sécurité de l'information.

Les mesures de sécurité existantes ayant un effet sur chaque risque ont été identifiées. La gravité et la vraisemblance ont été estimés, sans, puis avec les mesures de sécurité. (ANNEXE N°17 : 127)

6.4.2. L'évaluation des risques.

Nous avons pu juger l'importance des risques en les hiérarchisant selon les critères de gestion des risques retenus.

Les risques précédemment analysés (identifiés et estimés) peuvent être évalués à l'aide du tableau suivant d'une cartographie des risques. (ANNEXE N°18 : 128)

- Analyse de la cartographie des risques

Nous constatons que la plupart des risques se trouvent dans la zone d'acceptabilité avec une gravité significative et une vraisemblance peu probable ; mais aussi certains risques se trouvent à un niveau modéré (limite de risque acceptable) avec une gravité importante et une vraisemblance probable.

- Identification des objectifs de sécurité

Cette partie aborde du traitement des risques. Elle nous a permis de choisir la manière dont chaque risque doit être traité au regard de son évaluation.

6.4.3. Le choix des options de traitement des risques.

Cette action permet d'identifier, les objectifs de sécurité, c'est-à-dire choisir la manière dont on va devoir traiter les risques afin que le niveau de risque résiduel devienne acceptable. Elle a été réalisée en fonction des critères de gestion des risques retenus et pour tout ou partie de chaque risque aussi, nous avons choisi parmi les options suivantes :

- l'éviter (ou le refuser) ;
- le réduire ;
- le prendre (ou le maintenir) ;
- le transférer.

Le choix des options de traitement a été fait au regard :

- Des éléments constitutifs du risque ;
- des critères de gestion des risques retenus ;
- des paramètres à prendre en compte.

Nous avons pu choisir 2 options de traitement des risques après évaluation, 10 risques devront être maintenus et 4 devront être réduits (ANNEXE N°19 : 130)

L'administrateur général souhaite essentiellement réduire les risques jugés comme prioritaires et significatifs, et prendre les risques jugés comme non prioritaires. Par exemple, nous pouvons citer :

- la gestion de la souscription et de l'accueil des clients qui peut faire ressortir une source de menace de la confidentialité, est classée comme non prioritaire ;
- la réception et l'initialisation des dossiers qui peut faire ressortir une source de menace de la disponibilité est classée prioritaire et significatif ;

6.4.4. L'analyse des risques résiduels.

Nous allons identifier ici et estimer les risques résiduels qui subsisteront quand chaque objectif de sécurité sera atteint, et vérifier que l'on sera prêt à les accepter en toute connaissance de cause.

Pour mener à bien cette action, des critères de gestion des risques ont été retenus. D'une manière générale, les risques résiduels sont mis en évidence selon le choix de traitement :

- Un risque évité ne génère aucun risque résiduel s'il est complètement évité ; sinon les risques résiduels correspondront à ce qui n'est pas évité ;
- un risque réduit mène à des risques résiduels s'il n'est pas totalement réduit ;
- un risque pris constitue un risque résiduel à part entière ;
- un risque transféré n'induit aucun risque résiduel s'il est totalement transféré ; sinon, les risques résiduels correspondront à ce qui n'est pas transféré.

A l'issue de l'identification des objectifs de sécurité, nous avons mis en évidence les risques résiduels suivants : (ANNEXE N°20 : 131)

6.5. Etude des mesures de sécurité.

Cette activité fait partie intégrante du traitement des risques. Nous déterminons ici les mesures de sécurité adéquates pour atteindre les objectifs de sécurité identifiés, et nous allons identifier les risques résiduels.

Ce tableau ci après montre les mesures de contrôle prise en fonction des événements redoutés.

Tableau 16 : la prise en compte des mesures de contrôle.

Evénements redoutés	Mesures de contrôle
1. Perte de données clients non enregistrée.	Système de back-up
2. Intrusion dans les fichiers clients de l'entité d'une personne n'appartenant pas au GIE GAINDE 2000/DO.	Mise en veille par l'utilisateur avant de quitter le poste de travail
3. Intrusion d'une personne non autorisé dans les locaux du GIE 2000/DO.	Vérification de l'identité d'une personne avant l'accès aux locaux
4. Accès à distance sur une application t elle qu'ORBUS d'une personne non autorisée.	Pare feu

Source : Nous-mêmes

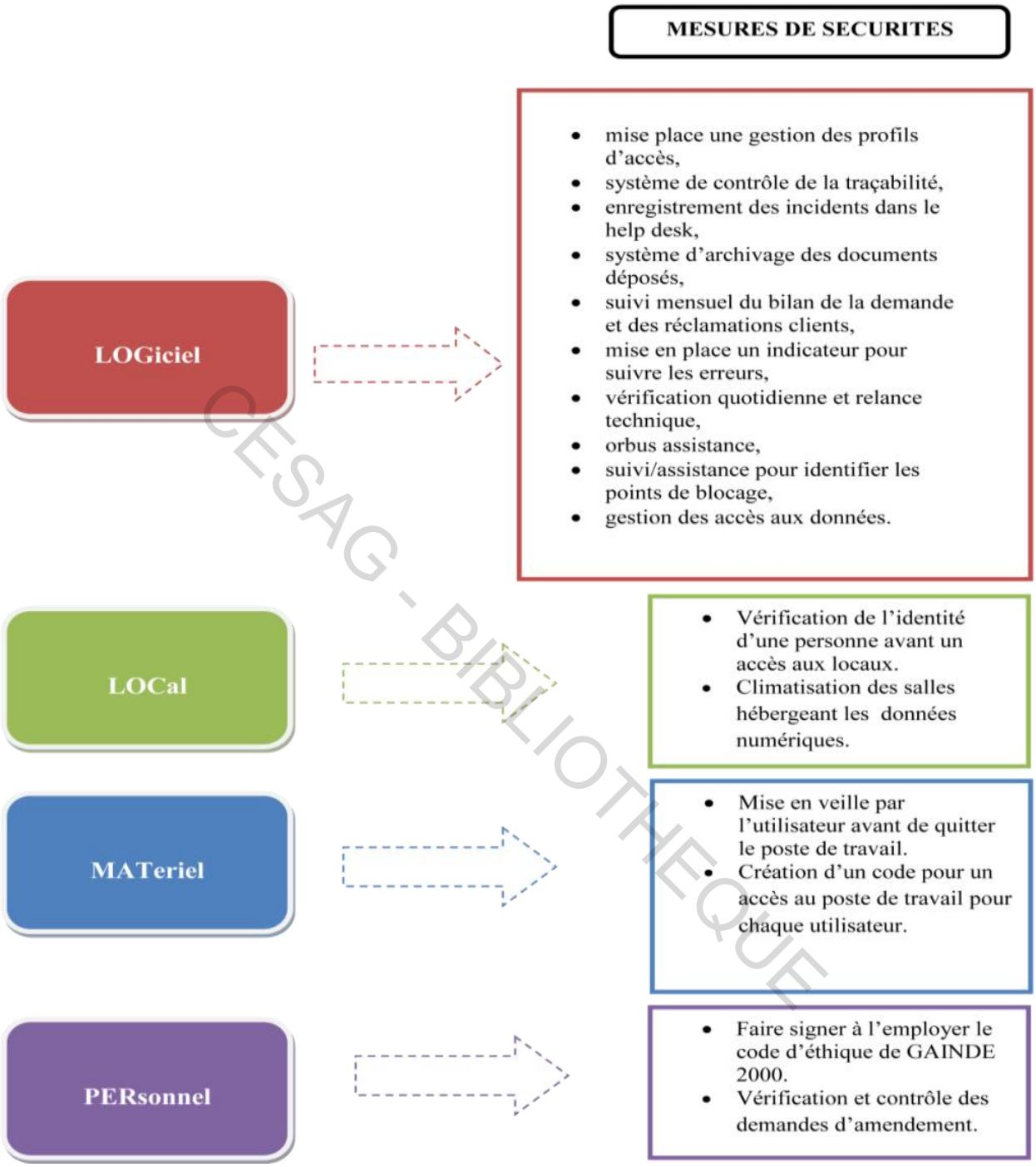
6.5.1. La détermination des mesures de sécurité.

Nous allons définir les mesures de sécurité qui vont nous permettre d'éviter, de réduire ou de transférer tout ou une partie des risques, en tenant compte des contraintes identifiées, notamment budgétaires et techniques.

Le GIE a mise en place certaines mesures de sécurité afin de minimiser les risques d'atteinte à l'intégrité, à la disponibilité ainsi qu'à la confidentialité des informations détenues par la direction des opérations.

Le schéma ci-après nous donne les mesures de sécurité définies en fonction de la DIC.

Figure 15 : les mesures de sécurité.



Source : nous-mêmes

Un tableau présentant la liste des mesures de sécurité à réduire ou transférer les risques prioritaires ainsi que les autres risques est mis en annexe. (ANNEXE N°21 : 132)

6.5.2. L'analyse des risques après évaluation du contrôle interne.

Nous allons passer à l'identification et à l'estimation des risques résiduels qui subsisteront quand chaque mesure de sécurité sera mise en œuvre.

Si les mesures de sécurité précédemment identifiées sont mises en œuvre, alors le niveau des risques jugés comme intolérables ou significatifs peut être ré-estimé comme suit :

(ANNEXE N°22 : 133)

6.5.3. L'établissement d'une déclaration d'applicabilité.

Nous allons tenter d'expliquer comment les paramètres à prendre en compte ont été retenus au sein de l'étude et aussi justifier le fait de ne pas en avoir tenu compte, le cas échéant.

La prise en compte de chaque contrainte identifiée est explicitée comme suit :

(ANNEXE N°23 : 134)

- **Mise en œuvre des mesures de sécurité.**

Nous allons passer à l'élaboration et au suivi de la réalisation du plan de traitement des risques par les mesures de sécurité afin de pouvoir prononcer l'homologation de sécurité.

Dans ce chapitre, nous avons pu mettre en place un processus de gestions des risques avec l'outil EBIOS afin de donner des réponses aux différents risques que rencontre la direction des opérations. De multiple risques ont été relevés, mais grâce au contre mesure que nous avons proposé, la DO à accepter de prendre certains de ces risques tandis que d'autres on été réduits. Ainsi dans le prochain chapitre, nous présenterons un plan d'action.

Chapitre 7: Recommandations.

L'élaboration d'un plan d'action et de suivi de la réalisation des mesures de sécurité est nécessaire.

Apres analyse avec le logiciel EBIOS des données recueilli à travers des entretiens ainsi qu'à travers l'accès à une documentation du GIE GAINDE 2000, nous avons identifié parmi les mesures de sécurité formalisées celles qui ne seraient pas déjà appliquées et, planifié les actions nécessaires à leur mise en œuvre.

Le plan d'action du GIE GAINDE 2000, trié par terme, avancement et coût financier, présenté par le logiciel EBIOS est établi comme suit : (ANNEXE N°24 : 135) suivi d'une dernière analyse des risques résiduels (ANNEXE N°25 : 136).

Mais nous avons ajouté à cette liste d'autres recommandations suivant les 5 modules de la méthode EBIOS :

7.1. Etude du contexte.

- **Recommandations sur l'identification des biens**

Une base de donnée mieux référencée et mise à jour à chaque semestre, permettrai de faciliter l'identification des biens supports pour un travail rapide et pertinent.

- **Recommandations sur la prise en comptes des bonnes pratiques**

Avec la mise en place d'une politique de sécurité du système d'information, il conviendra de faire évoluer régulièrement ce document, au regard des modifications des systèmes et outils informatiques utilisés par le GIE GAINDE 2000.

Il faudra aussi convaincre, sensibiliser, éduquer, former les personnels et développer une culture de l'entreprise intégrant bien la notion de risque. Le facteur humain reste déterminant. Rien ne peut se faire sans une adhésion de la personne.

7.2. Etudes des évènements redoutés.

- **Recommandations sur la sauvegarde de donnée**

Avec un environnement informatique instable ainsi que des risques multiples, il faudra établir impérativement un plan de sauvegarde ("back-up", "mirroring"...) au moins pour les données

stratégiques. L'utilisation du « clouding » bien sécurisé et même envisageable dans le stockage des données.

- **Recommandations sur le réseau sans fil**

Il conviendra de changer le mot de passe du réseau sans fil (wifi) de manière périodique ou d'opter pour un filtrage d'adresse MAC des appareils tels que les Smartphones, tablettes et ordinateur portable afin de limiter le risque d'intrusion pouvant aboutir à des vols de fichiers au niveau de la direction des opérations ou des données personnelles extrêmement sensibles sont traitées.

- **Recommandations sur l'accès physique aux locaux**

Il faudra aussi renforcer l'accès aux locaux sensibles, tels que les salles hébergeant les serveurs informatiques et les éléments du réseau. Ces locaux doivent faire l'objet d'une sécurisation particulière : vérification des habilitations, gardiennage, portes fermées à clé, digicode, contrôle d'accès par badge nominatifs, etc. La DSI ou le responsable informatique doit veiller à ce que les documentations techniques, plans d'adressages réseau, contrats, etc. soient eux aussi protégés.

- **Recommandations sur les applications**

Le principe d'une politique de définition des mots de passe pour sécurisé les applications que le GIE GAINDE 2000 a déjà mise en place est évident : permettre l'accès uniquement aux utilisateurs autorisés. Il conviendra d'ajouter juste que les mots de passe faibles simplifient la tâche des pirates car ils sont faciles à deviner ou à déchiffrer. En dépit de cette vulnérabilité importante qui concerne tous les systèmes, de nombreuses organisations ne prennent pas le problème sérieusement.

Il faudra appliquer une politique pour créer des mots de passe efficaces, en suivant notamment ces conseils :

- utiliser des mots de passe longs. Plus ils contiennent de caractères, plus ils sont sûrs ;
- utiliser des chiffres, des symboles et des caractères avec minuscules et majuscules ;
- n'utiliser pas d'informations personnelles telles que votre nom de famille, votre date de naissance, le nom de votre animal domestique ;

- changer fréquemment de mots de passe ;
- éviter les mots de passe trop compliqués à retenir ou utilisez un outil d'administration centralisée des mots de passe simple et sécurisé. Ne laissez jamais votre mot de passe écrit sur un post-it à côté de votre ordinateur.

7.3. Etudes des scénarios de menaces.

- **Recommandations sur l'audit des risques**

Il faudra procéder à des études formalisées (auditable) des risques/menaces de manière régulière(le temps sera déterminé en fonction du besoin). Et pour cela il conviendra :

- de voir l'origine des menaces,
- d'examiner les causes des risques,
- d'imaginer les scénarios catastrophes et de chiffrer les (coûts, probabilité...).

Aussi il faudra procéder à une analyse des vulnérabilités de l'établissement, et faire un rapport qui sera communiqué aux dirigeants.

Il est nécessaire d'agir en prévision des risques nouveaux. L'analyse globale des risques doit être renouvelée, mieux : devenir une action permanente.

7.4. Etude des risques.

Il faudra mettre à jour les mesures de sécurité en tenant compte des nouvelles menaces qui pèsent sur le processus PO06.

7.5. Etude des mesures de sécurité.

Il conviendra après études des scénarios de menaces et une étude approfondi des risques, d'établir pour les dirigeants un plan d'action périodique (parades, coûts/avantages...), pour actualiser les mesures de sécurité face à de nouveaux risques.

Au terme de ce chapitre, les résultats de l'évaluation donnent une image plus ou moins positive du point de vue de la pertinence de l'action de l'équipe chargée de la sécurité du système d'information. Toutefois, à travers nos études, nous avons relevé des faiblesses notamment, des indisponibilités du système ou des incidents non résolus dans les délais pouvant ralentir l'activité du GIE.

Conclusion de la deuxième partie

La deuxième partie de notre mémoire a été consacrée à l'étude de nos travaux réalisés sur le terrain. Dans un premier temps, nous avons eu à présenter le GIE GAINDE 2000, décrire l'existant à étudier et relever la problématique rencontrée. Dans un second temps, nous avons effectué une présentation et une analyse des résultats du processus collecte électronique des documents de pré-dédouanement appelé aussi Processus 06 ou PO06.

Et enfin, nous avons proposé des perspectives d'amélioration des faiblesses que nous avons eu à diagnostiquer lors de notre étude.

CONCLUSION GENERALE

Un système d'information automatisé se présente à l'heure actuelle comme indispensable pour la bonne gestion d'une organisation. A cet effet, la gestion des risques du système d'information est incontournable dans le management de l'entreprise.

L'utilisation des méthodes de gestion des risques est devenue systématique pour les entreprises soucieuses de leur sécurité. EBIOS, en tant que véritable boîte à outil de la gestion des risques, contribue à de nombreuses démarches de sécurité permettant d'élaborer le socle de la SSI (schéma directeur, politique de sécurité, tableaux de bord) et de rédiger des spécifications de sécurité (, profil de protection, cible de sécurité, politique de certification ou d'autres formes de cahiers des charges et plans d'action).

La méthode EBIOS présente l'avantage de structurer une démarche complète de construction du risque, à partir de l'existant de l'organisation concernée. Associées à cette démarche, les bases de connaissance, remises à jour constamment, ainsi qu'un logiciel "open source" disponible gratuitement, fournissent un support rapide et efficace. La méthode EBIOS est souvent présentée en "concurrence", avec d'autres méthodes de gestion des risques SSI. Cependant, au-delà des comparaisons, EBIOS propose une démarche singulière de construction des risques, dégagée de toute préoccupation commerciale, et s'adaptant à tout type d'organisation, qu'elle soit privée ou publique.

Avec l'émergence de la norme ISO 27005, dans la lignée de l'ISO 9001 pour la qualité, le nombre de certificats 27005 ne cesse d'augmenter avec l'exemple du GIE GAINDE 2000 qui a déjà entamé les démarches de certification, et le domaine de la normalisation de la SSI s'organise ainsi pour créer un cadre homogène de normes adaptées à ces évolutions. Il convient, dès lors, à tout niveau de l'entreprise, de tenir compte de ces développements ; c'est notamment le rôle du RSSI, en première ligne, qui se doit aussi de connaître les outils à sa disposition, pour assurer la mise en place, la maintenance et l'amélioration continue de la sécurité de l'information de manière globale. De fait, les méthodes phares de gestion des risques, telle qu'EBIOS, retiennent plus que jamais l'attention.

La mise en place d'un processus de gestion des risques du SI nous a permis avec le GIE GAINDE 2000 d'analyser et d'évaluer les données, de présenter les résultats (la cartographie des risques du SI) et d'élaborer un plan d'action à suivre. Ce processus appliqué au GIE a été rendu possible grâce au logiciel français EBIOS conformément à la famille des normes 27000.

Ledit processus est le fruit de la norme ISO 27005 ; ceci lui permet d'incorporer les bonnes pratiques universelles adoptées pour assurer au GIE de façon générale une maitrise de ses risques afin de les gérer et de les anticiper.

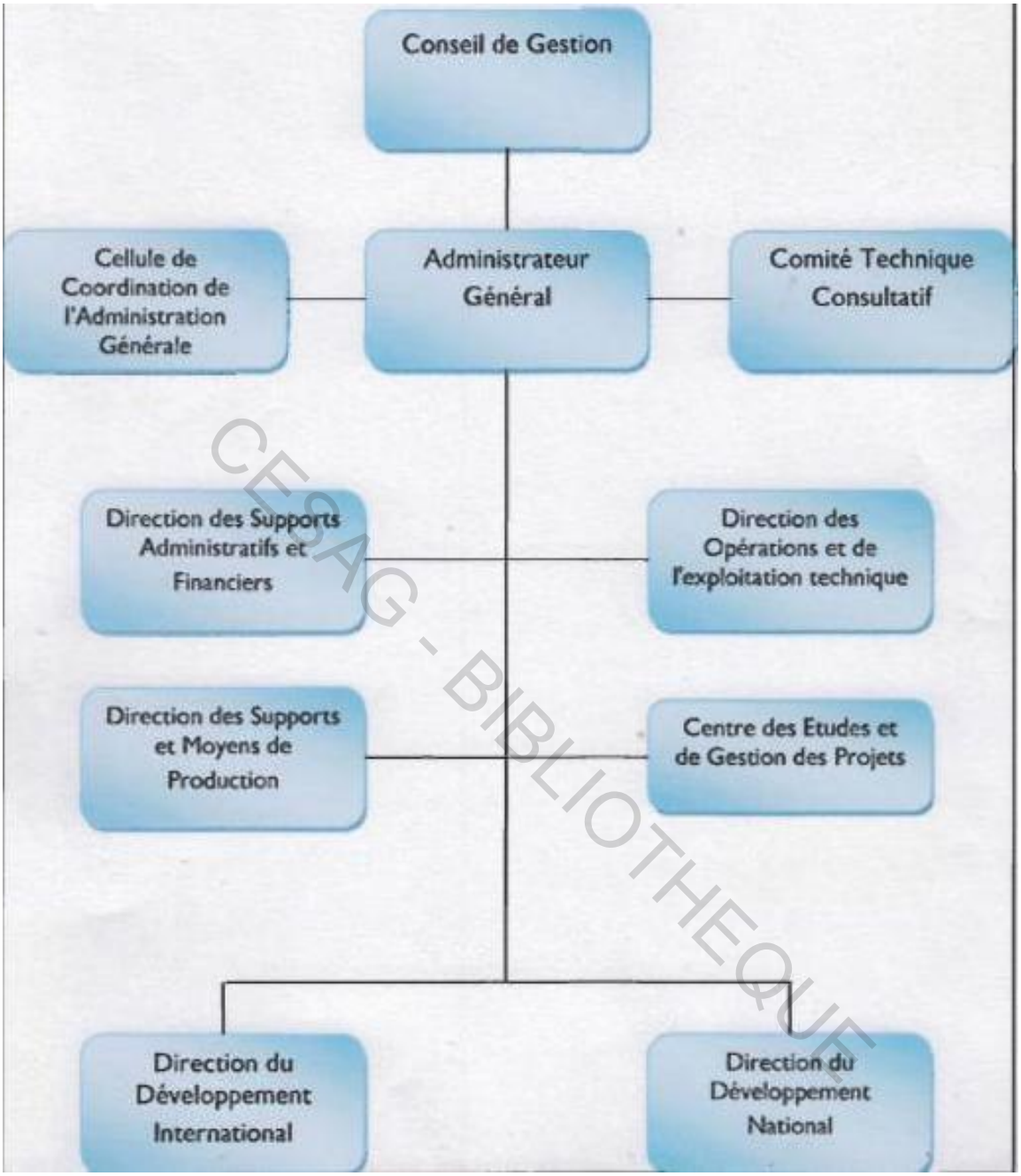
Nous pensons par la même occasion que l'utilisation des informations traitées au niveau de la direction des opérations ne saurait être pertinente sans l'intervention préalable d'une assurance de la fiabilité du SI. Car le niveau de pénétration de la technologie de l'information dans les organisations est très élevé et, ces derniers sont exposées à des risques pouvant déformer l'information (fausses informations = prise de décisions stratégiques pouvant amener une entreprise en faillite).

En définitive, cet apprentissage d'une durée de deux (2) mois au sein du GIE GAINDE 2000 m'a permis de découvrir la famille des normes 27000, de voir la gestion des flux d'informations qui circulaient au niveau de l'entreprise particulièrement au niveau de la direction des opérations. J'ai pu également acquérir une grande connaissance dans le fonctionnement d'un système d'information. Aussi, avec le logiciel de gestion des risques, j'ai procédé à une analyse approfondie et une évaluation pertinente des risques pouvant affecter le SI de la direction. Afin d'en faire ressortir une cartographie des risques (présentée en annexe) et proposer ainsi des recommandations. Des recommandations qui iront dans le sens d'une amélioration de la qualité du fonctionnement des activités de ce département mais aussi du GIE de manière globale.

Ceci nous amène à affirmer sans nous tromper que l'audit des SI est devenu la profession de cette ère technologique et une réelle aubaine pour l'Afrique émergente.

ANNEXES

ANNEXE N°1 : Organigramme du GIE GAINDE 2000



Source :GIE GAINDE 2000

ANNEXE N°2 : Nomenclature des biens supports (matériels, logiciels systèmes, locaux, personnels) utilisés au niveau de la direction des opérations (processus collecte de document-PO06)

PO06	**Collecte électronique des documents**		
PO06_ACT1	Gère la souscription et l'accueil des clients	ACT: Activité métier	PHY_LIE.1.3, MAT_ACT.3.4
PO06_ACT2	Réception et Initialisation des Dossiers	ACT: Activité métier	LOG_APP.1.6, MAT_ACT.2.1, PHY_LIE.1.4
PO06_ACT3	Collecter transmettre traiter documents de pré dédouanements	ACT: Activité métier	MAT_ACT.3.4
PO06_ACT4	Suivre les dossiers et assister les clients	ACT: Activité métier	LOG_APP.1.10, PHY_LIE.1.2, MAT_ACT.2.4, PHY_LIE.1.3
PO06_INF.1	Demande de Souscription	INF: Informations	MAT_ACT.2.4, LOG_APP.1.6
PO06_INF.2	Formulaire Initialisation-Facture Commerciale-Souscription	INF: Informations	PHY_LIE.1.1, MAT_ACT.2.14, PER_EXP.1.5
PO06_INF.3	Référence Souscription Code d'accès Remise Token	INF: Informations	MAT_ACT.2.9
PO06_INF.4	Besoin en Formation Besoin en Installation	INF: Informations	LOG_APP.1.4, MAT_ACT.3.1, MAT_PAS.2.9, PER_EXP.1.2
PO06_INF.5	Facture Règlement	INF: Informations	MAT_ACT.2.2, LOG_APP.1.1
PO06_INF.6	Données du Document	INF: Informations	MAT_ACT.2.10, LOG_APP.1.10, PER_EXP.1.5
PO06_INF.7	Obtention Numéro Orbus Facture Provisoire	INF: Informations	PER_EXP.1.5, MAT_ACT.1.3
PO06_INF.8	Documents de Pré-dédouanement	INF: Informations	PER_UTI.1.1, MAT_ACT.2.2
PO06_INF.10	Requête état des dossiers	INF: Informations	MAT_ACT.2.7, LOG_APP.1.12, PER_UTI.1.3
PO06_INF.11	Information état des dossiers	INF: Informations	MAT_ACT.3.7
PO06_INF.12	Demande Amendement Dossiers Orbus Autorisation	INF: Informations	PER_UTI.1.4, MAT_PAS.2.15 ,LOG_APP.1.12

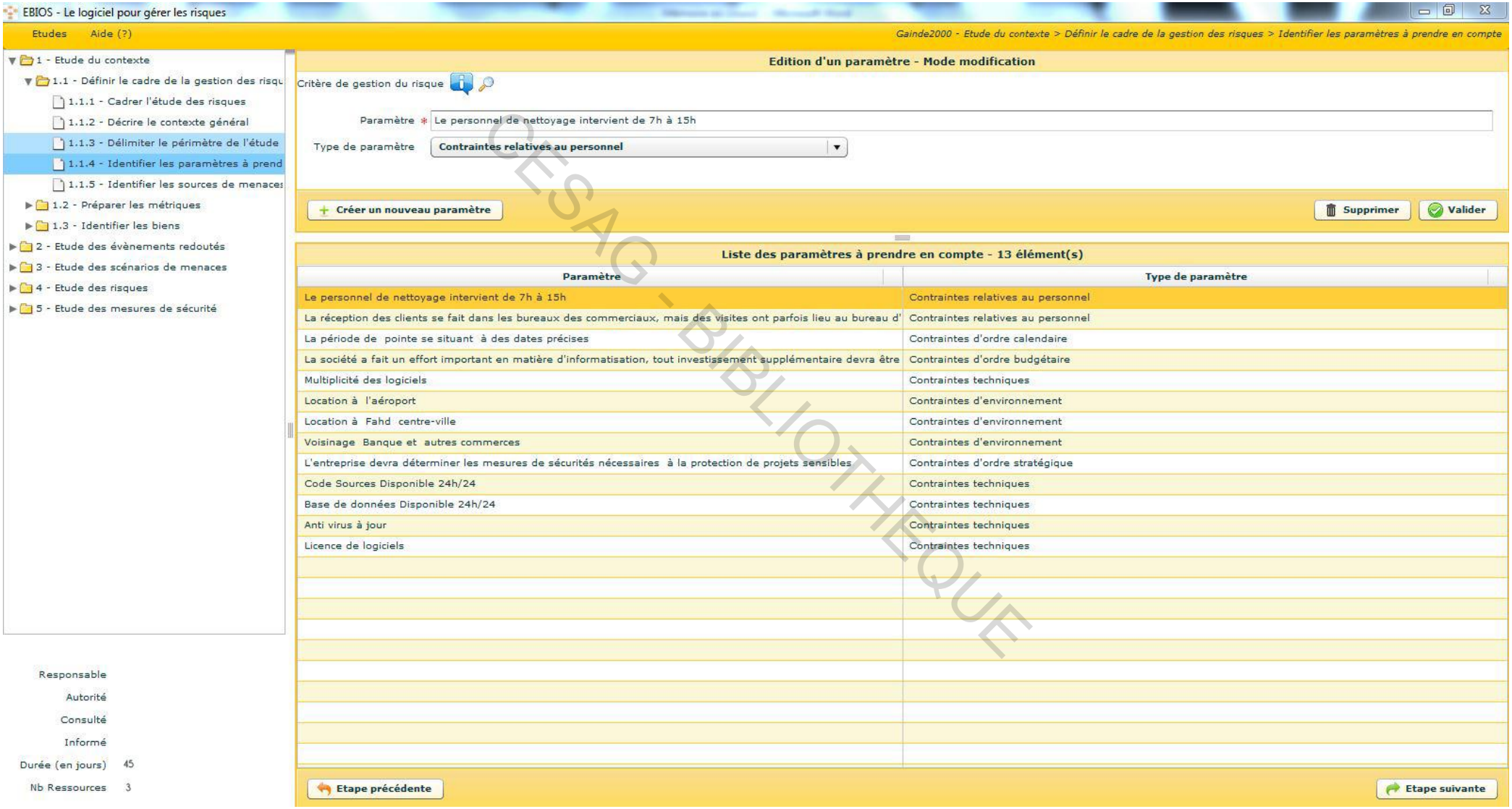
Source :GIE GAINDE 2000

Id	Désignation	Type
PHY_LIE.1.3	Locaux	Centre de données
MAT_ACT.3.4	Périphérique de traitement	Rappel téléphonique du client après prise en charge
LOG_APP.1.6	ORBUS	Application métier spécifique
MAT_ACT.2.1	Matériel fixe	Pour accéder à Orbus
PHY_LIE.1.4	Zone	Bureaux sécurisés interdit aux clients
MAT_ACT.3.4	Périphérique de traitement	Rappel téléphonique du client après prise en charge
LOG_APP.1.10	FORMULAIRE	Application métier spécifique
PHY_LIE.1.2	Locaux	Centre d'appel
MAT_ACT.2.4	Matériel fixe	Téléphone pour recevoir les appels des clients
PHY_LIE.1.3	Locaux	Centre de données
MAT_ACT.2.4	Matériel fixe	Téléphone pour recevoir les appels des clients
LOG_APP.1.6	ORBUS	Application métier spécifique
PHY_LIE.1.1	Locaux	Centre de développement
MAT_ACT.2.14	Matériel fixe	Pour saisir des données dans le système-Ordinateur
PER_EXP.1.5	Exploitant / Maintenance	Pour sauvegarder les données du système
MAT_ACT.2.9	Matériel fixe	Serveur d'installation
LOG_APP.1.4	WORD	Application métier standard
MAT_ACT.3.1	Périphérique de traitement	Imprimante pour impression formulaire
MAT_PAS.2.9	Autres supports	Besoins en utilisateurs à Former (mail ou formulaire d'inscription)
PER_EXP.1.2	Exploitant / Maintenance	service support
MAT_ACT.2.2	Matériel fixe	Se connecter aux applications
LOG_APP.1.1	FACTURATION	Application métier spécifique

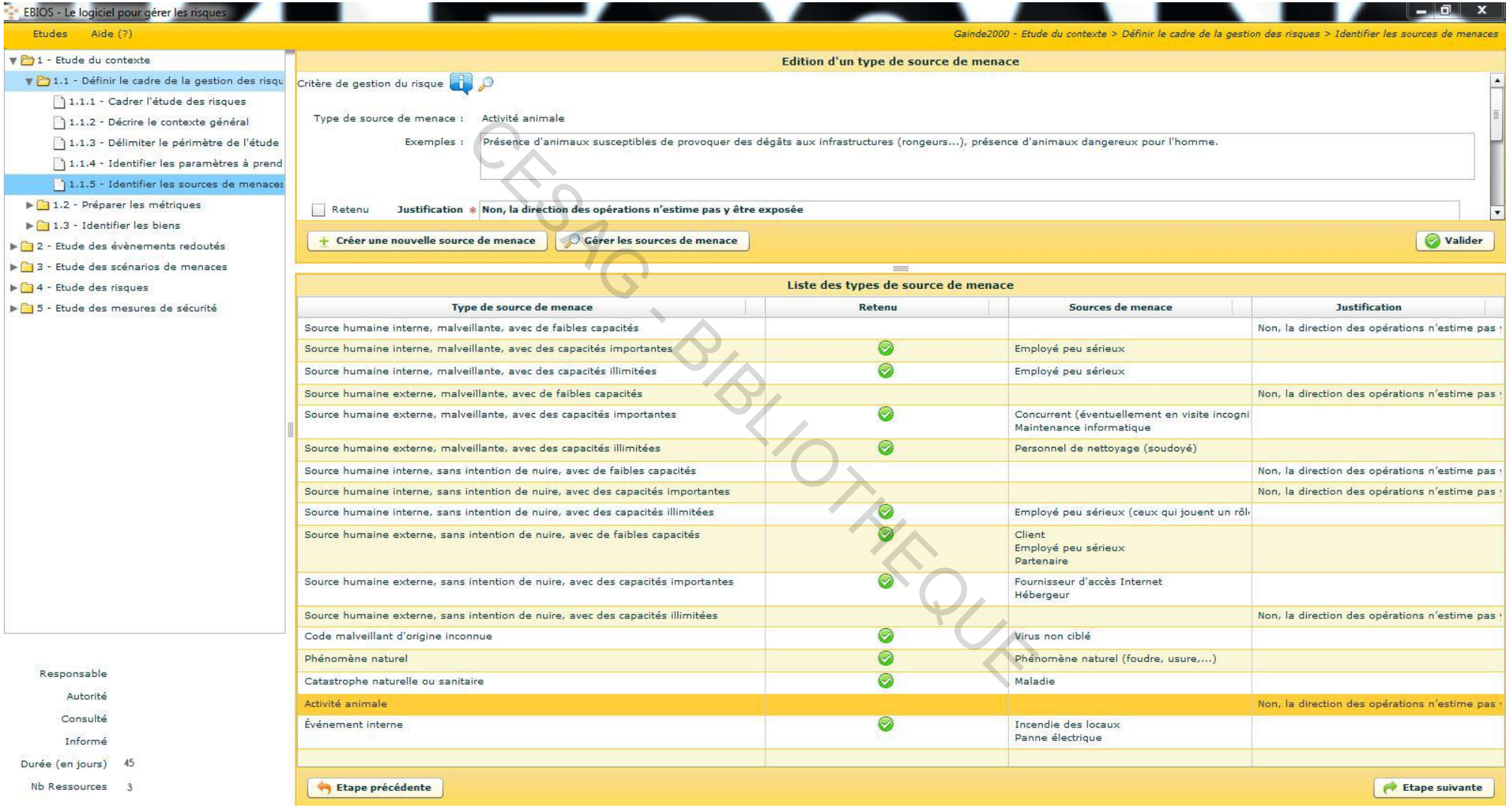
MAT_ACT.2.10	Matériel fixe	Postes de travail et Serveurs
LOG_APP.1.10	FORMULAIRE	Application métier spécifique
PER_EXP.1.5	Exploitant / Maintenance	Pour sauvegarder les données du système
PER_EXP.1.5	Exploitant / Maintenance	Pour sauvegarder les données du système
MAT_ACT.1.3	Matériel transportable	Retro projecteur, ordinateur portable
PER_EXP.1.1	Exploitant / Maintenance	Ressource humaine pour achemine le courrier
MAT_ACT.2.2	Matériel fixe	Se connecter aux applications
MAT_ACT.2.7	Matériel fixe	Serveur de Partage de Source
LOG_APP.1.12	LOGICIEL	Application métier spécifique
PER_EXP.1.3	Exploitant / Maintenance	service maintenance
MAT_ACT.3.7	Périphérique de traitement	Scanner pour les fiches d'incidents
PER_EXP.1.4	Exploitant / Maintenance	Acheminer les factures
MAT_PAS.2.15	Autres supports	Pour se connecter aux module amendement
LOG_APP.1.12	LOGICIEL	Application métier spécifique

Source :GIE GAINDE2000

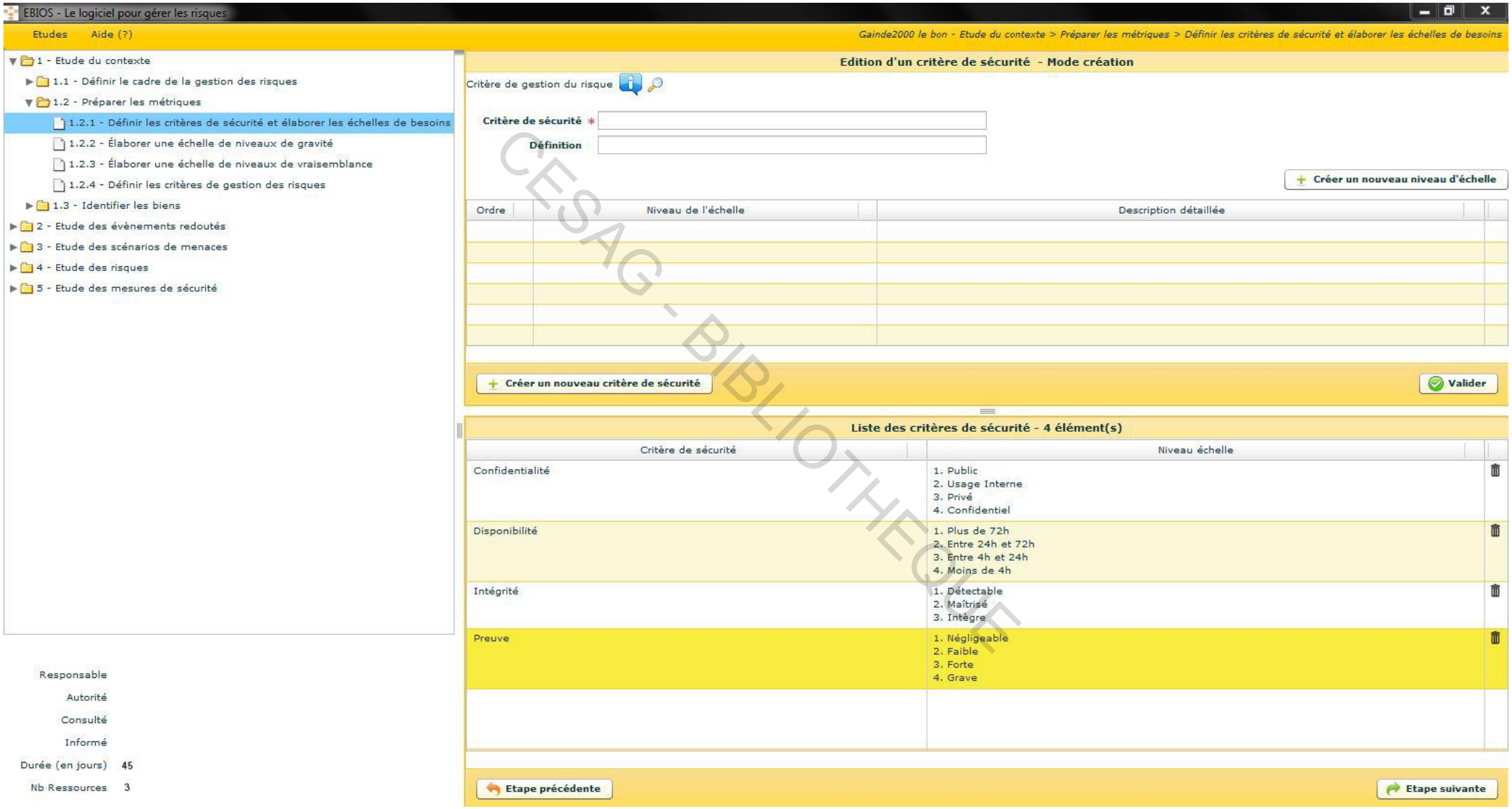
ANNEXE N°3 : Identification des paramètres à prendre en comptes



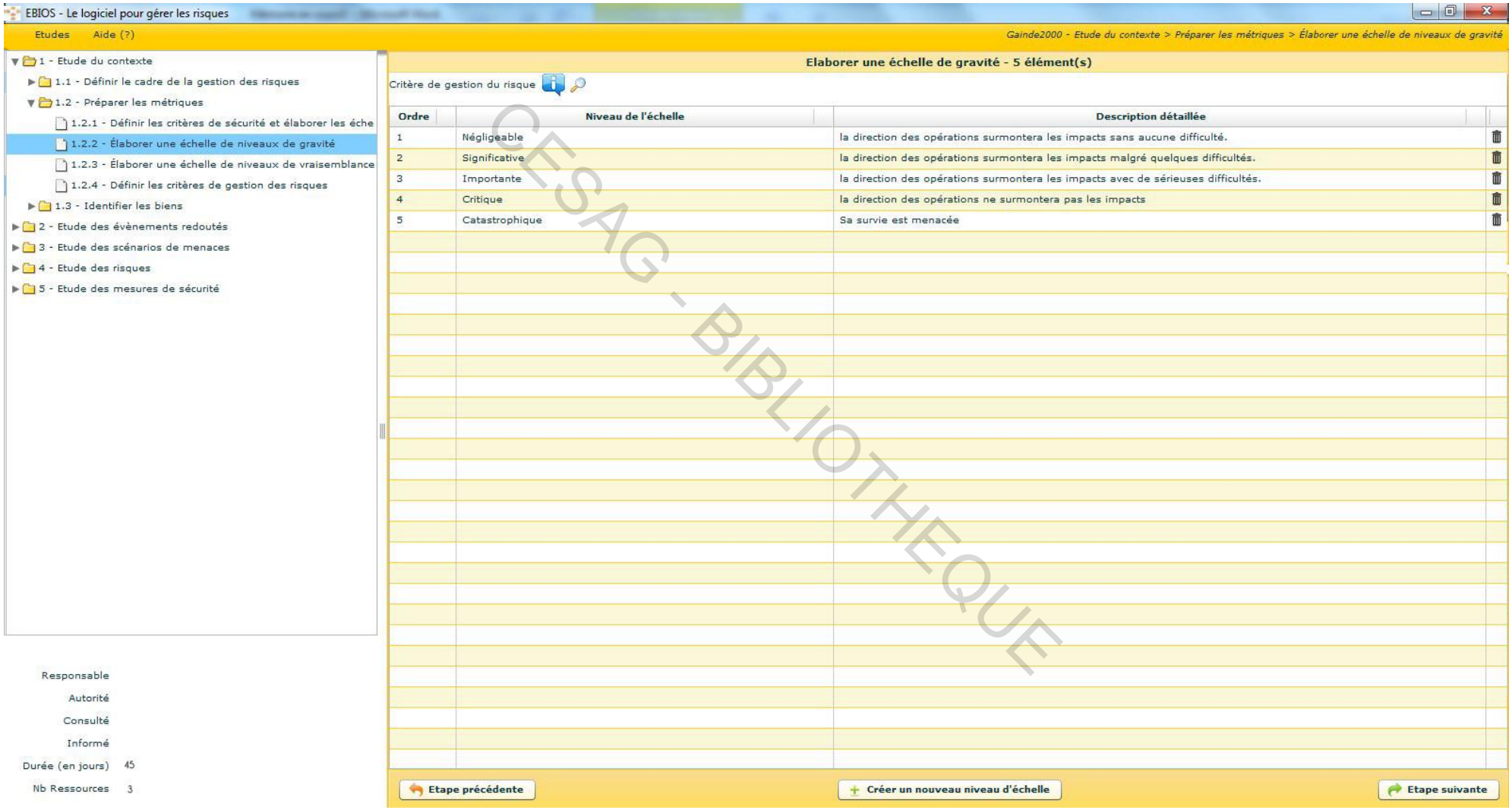
ANNEXE N°4 : identification les sources de menaces



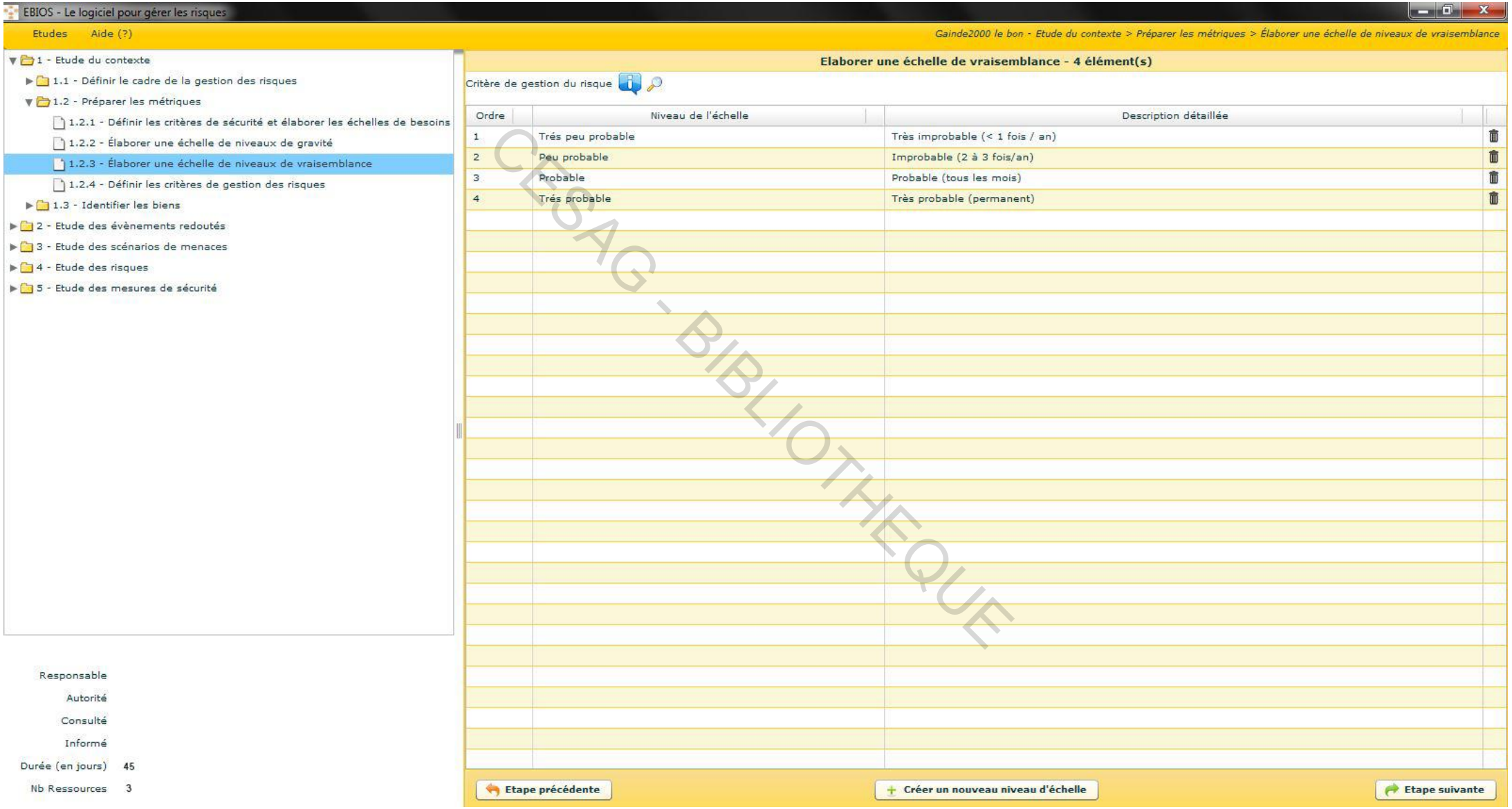
ANNEXE N°5 : definir les critéres de securité et élaborer les echelles de besoins



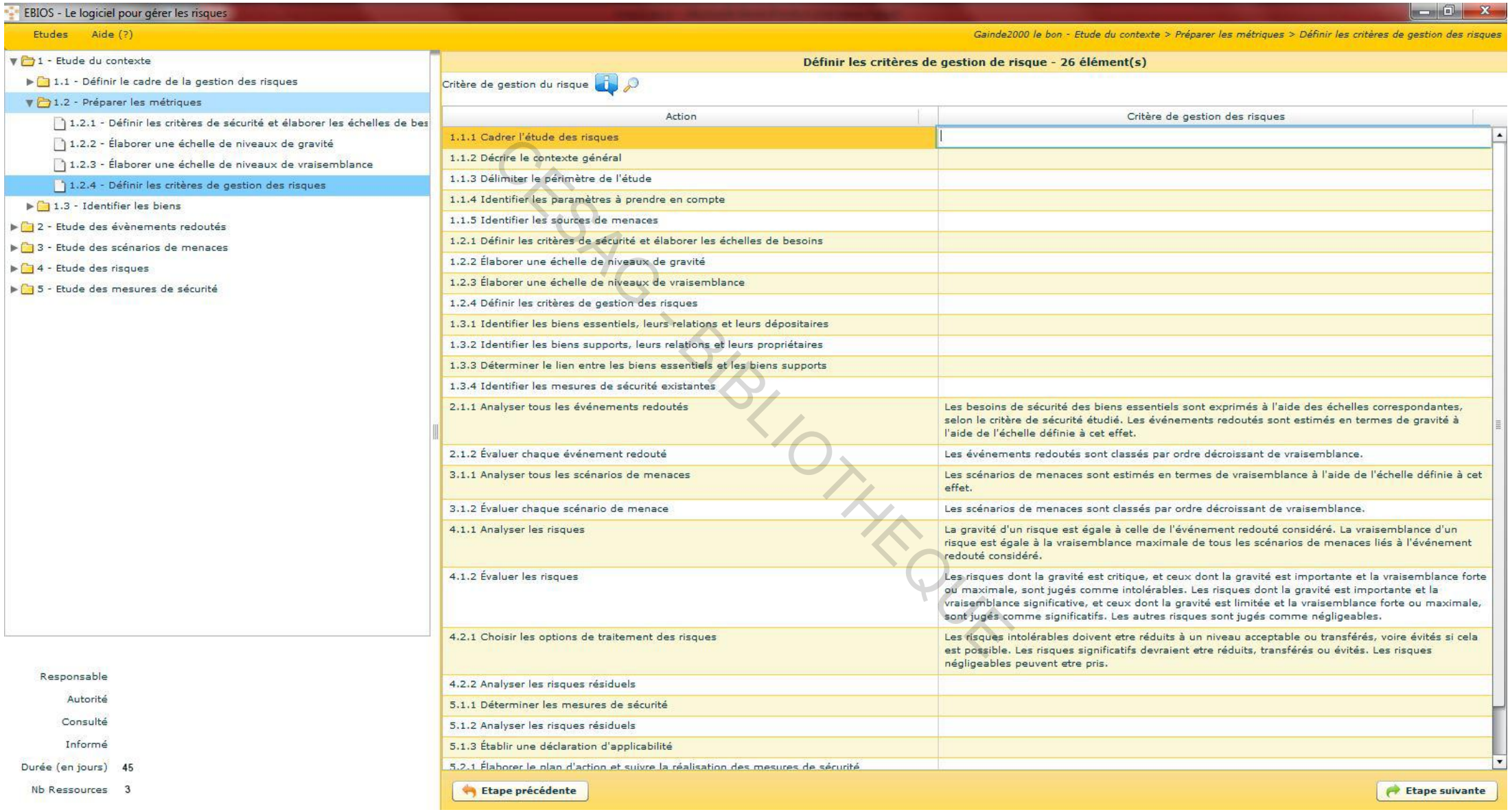
ANNEXE N°6 : élaboreration d'une echelle de niveaux de gravité



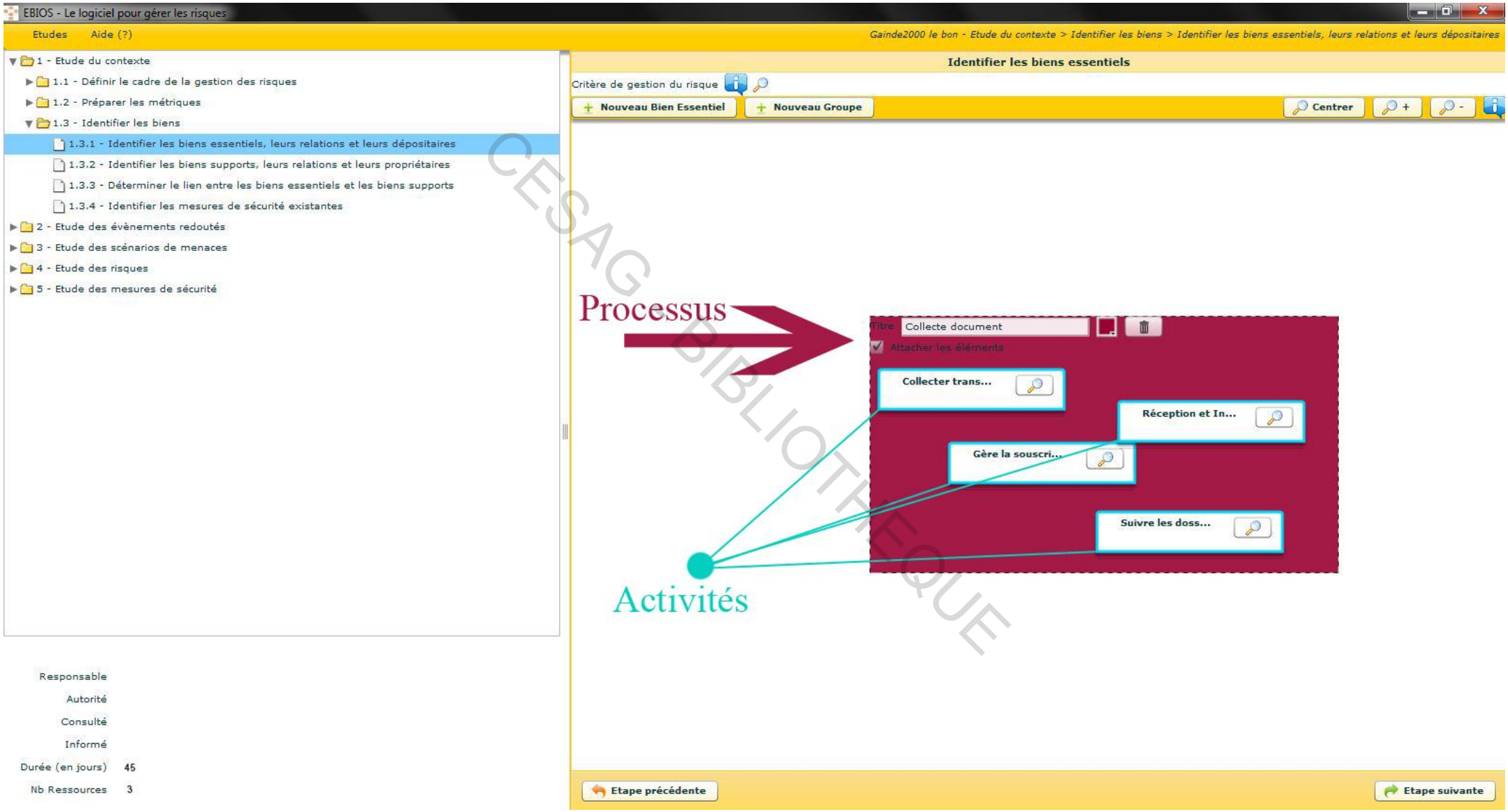
ANNEXE N°7 : élaboration d'une échelle de niveaux de vraisemblance



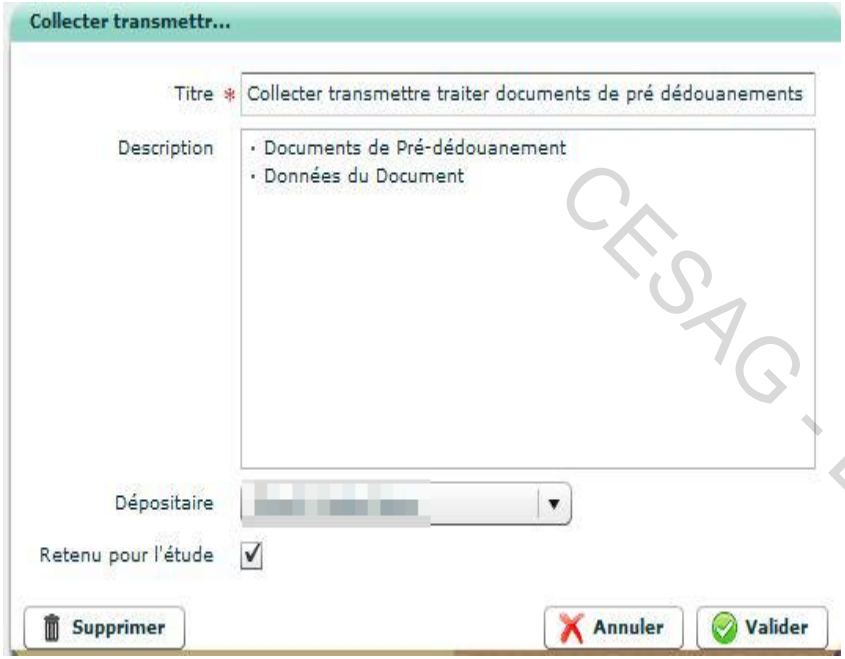
ANNEXE N°8 : définition des critères de gestion des risques

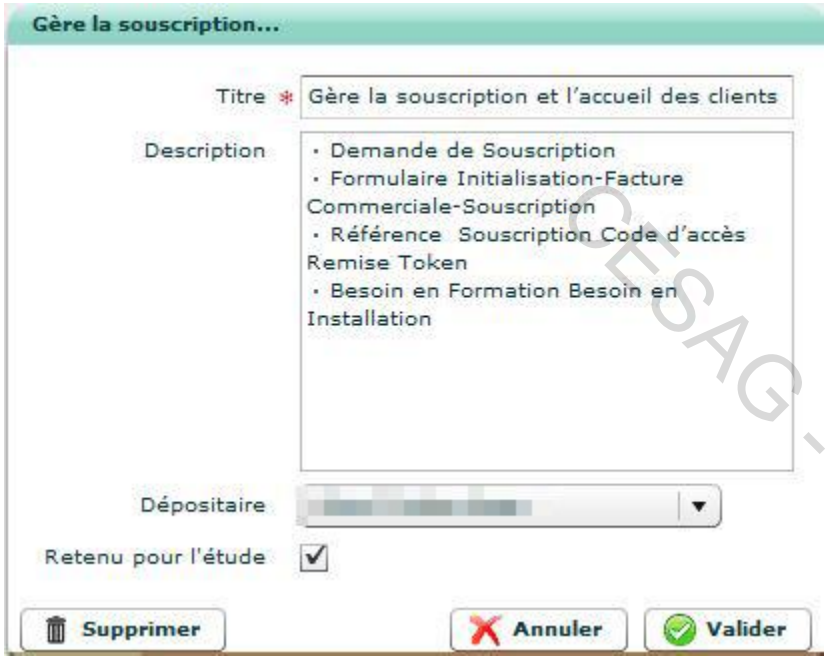


ANNEXE N°9 : identification des biens essentiels



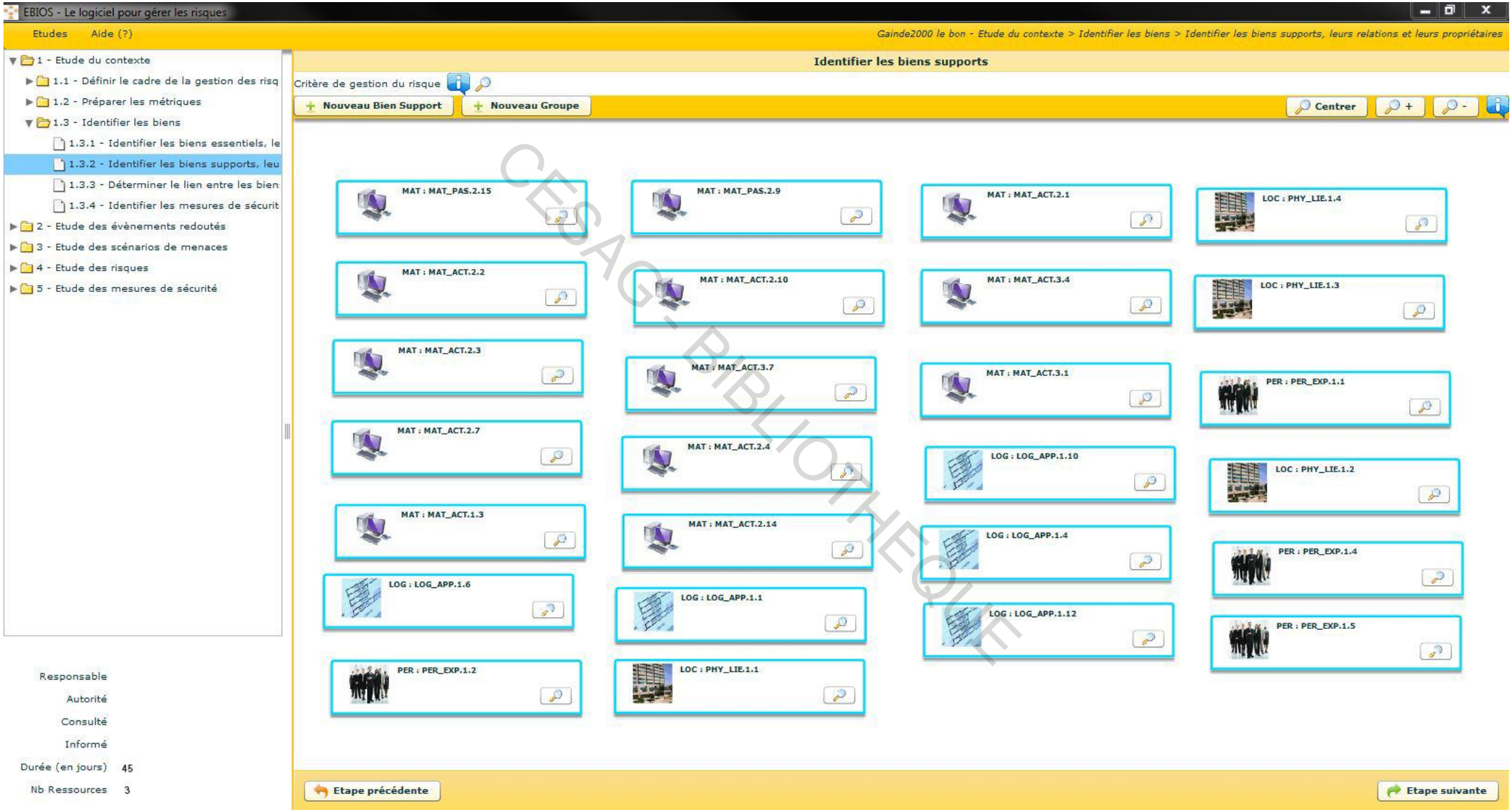
- Les activités.



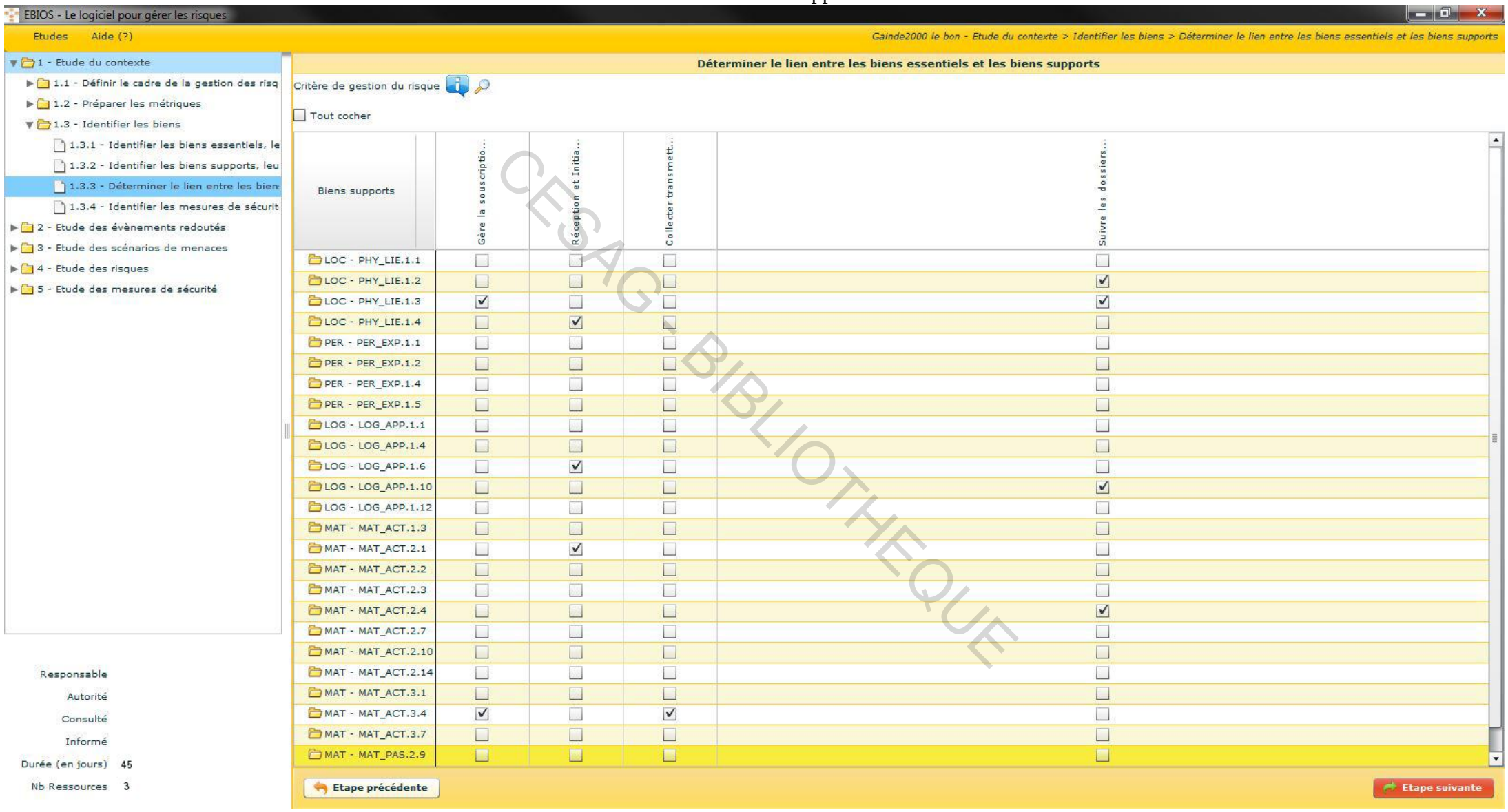


PS : Pour des raisons de confidentialité, nous avons flouté le nom du dépositaire

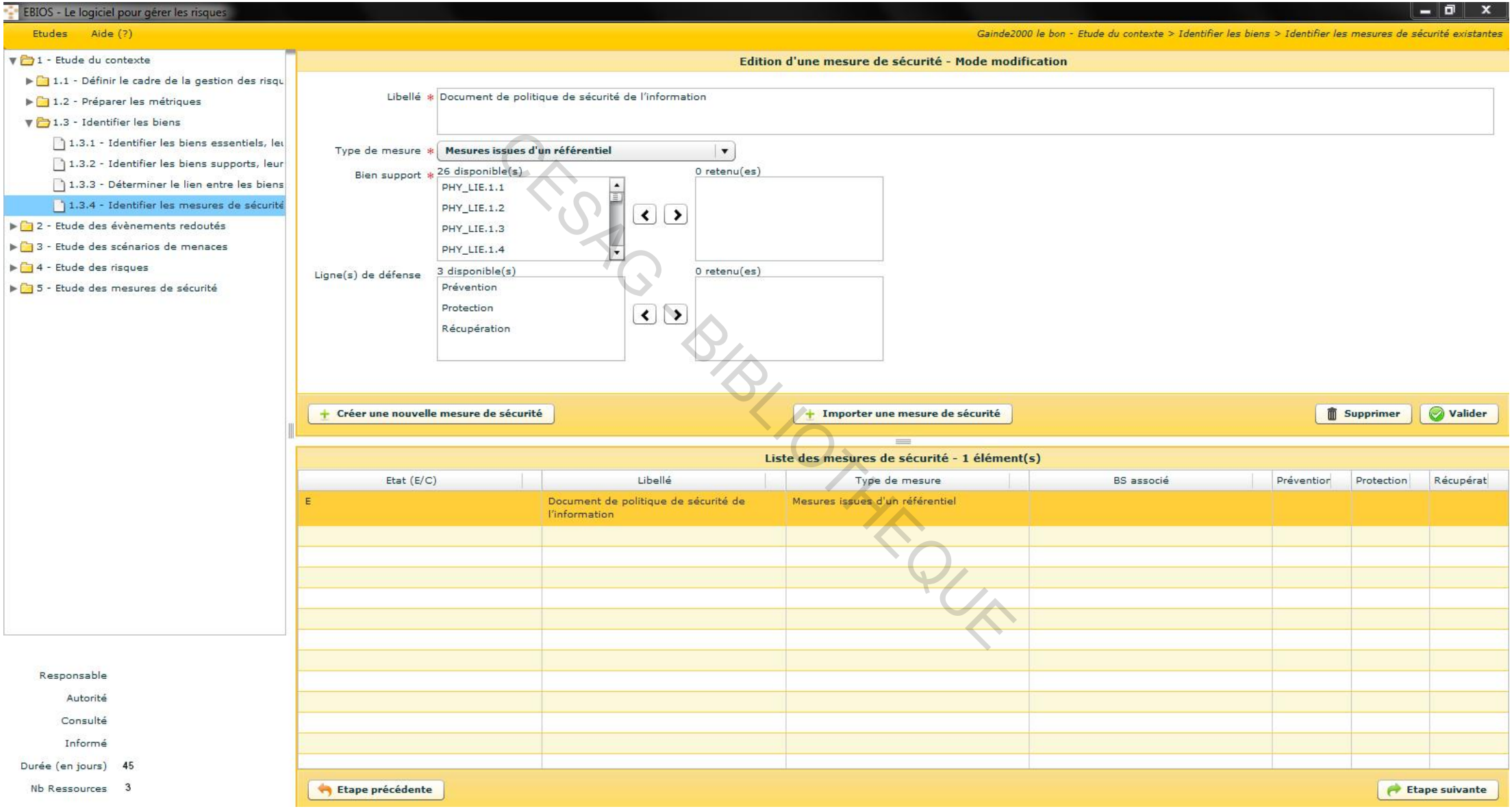
ANNEXE N°10 : identification des biens supports



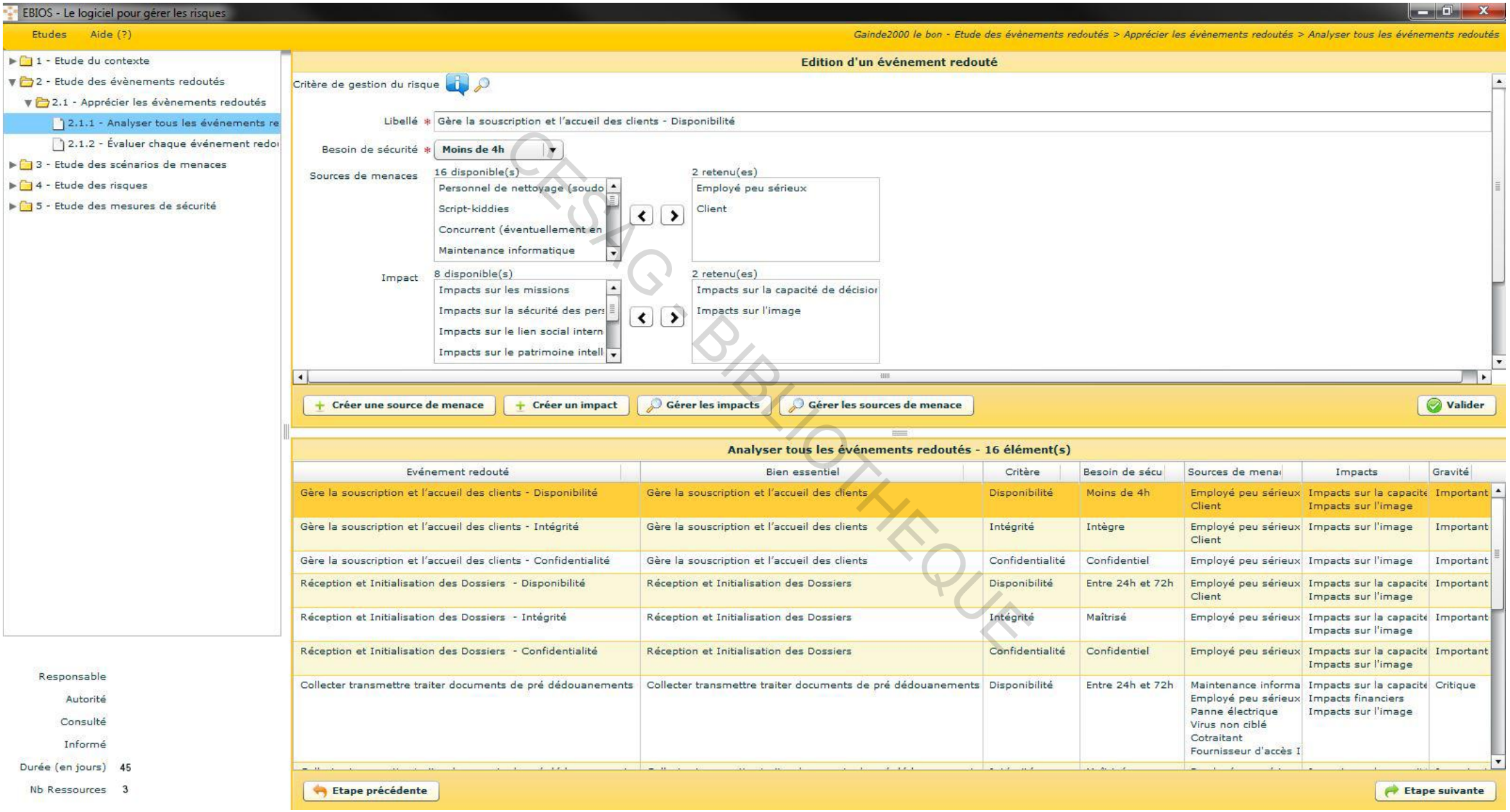
ANNEXE N°11 : détermination du lien entre les biens essentiels et les biens supports



ANNEXE N°12 : détermination d'une mesure de sécurité



ANNEXE N°13 : analyse des événements redoutés



EBIOS - Le logiciel pour gérer les risques

Etudes Aide (?)

Gainde2000 le bon - Etude des évènements redoutés > Apprécier les évènements redoutés > Analyser tous les événements redoutés

- 1 - Etude du contexte
- 2 - Etude des évènements redoutés
  - 2.1 - Apprécier les évènements redoutés
    - 2.1.1 - Analyser tous les événements re
    - 2.1.2 - Évaluer chaque événement redo
- 3 - Etude des scénarios de menaces
- 4 - Etude des risques
- 5 - Etude des mesures de sécurité

Analyser tous les événements redoutés - 16 élément(s)

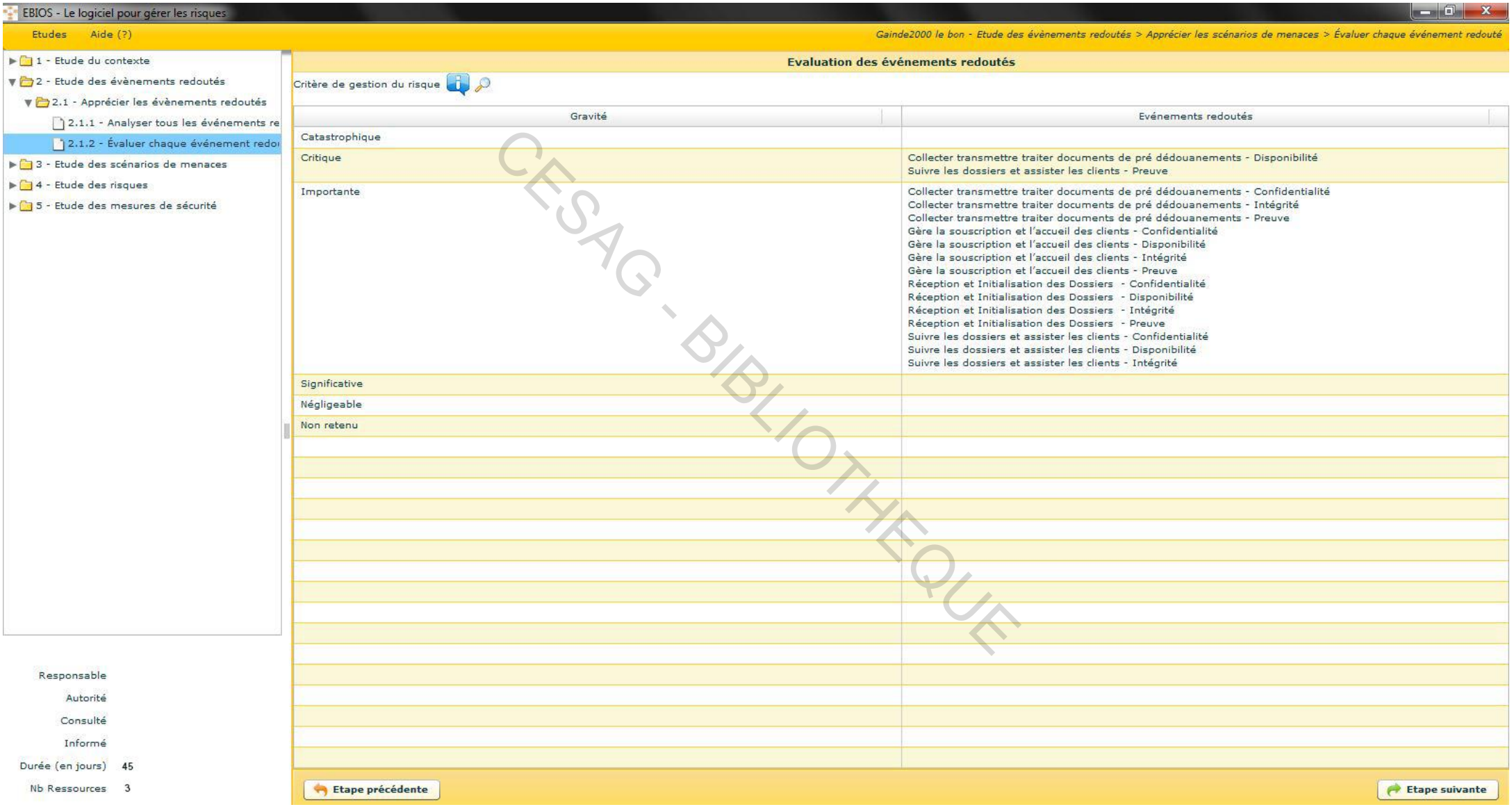
Evénement redouté	Bien essentiel	Critère	Besoin de sécu	Sources de menac	Impacts	Gravité
Gère la souscription et l'accueil des clients - Disponibilité	Gère la souscription et l'accueil des clients	Disponibilité	Moins de 4h	Employé peu sérieux Client	Impacts sur la capacité Impacts sur l'image	Importante
Gère la souscription et l'accueil des clients - Intégrité	Gère la souscription et l'accueil des clients	Intégrité	Intègre	Employé peu sérieux Client	Impacts sur l'image	Importante
Gère la souscription et l'accueil des clients - Confidentialité	Gère la souscription et l'accueil des clients	Confidentialité	Confidentiel	Employé peu sérieux	Impacts sur l'image	Importante
Réception et Initialisation des Dossiers - Disponibilité	Réception et Initialisation des Dossiers	Disponibilité	Entre 24h et 72h	Employé peu sérieux Client	Impacts sur la capacité Impacts sur l'image	Importante
Réception et Initialisation des Dossiers - Intégrité	Réception et Initialisation des Dossiers	Intégrité	Maîtrisé	Employé peu sérieux	Impacts sur la capacité Impacts sur l'image	Importante
Réception et Initialisation des Dossiers - Confidentialité	Réception et Initialisation des Dossiers	Confidentialité	Confidentiel	Employé peu sérieux	Impacts sur la capacité Impacts sur l'image	Importante
Collecter transmettre traiter documents de pré dédouanements	Collecter transmettre traiter documents de pré dédouanements	Disponibilité	Entre 24h et 72h	Maintenance informa Employé peu sérieux Panne électrique Virus non ciblé Cotraitant Fournisseur d'accès I	Impacts sur la capacité Impacts financiers Impacts sur l'image	Critique
Collecter transmettre traiter documents de pré dédouanements	Collecter transmettre traiter documents de pré dédouanements	Intégrité	Maîtrisé	Employé peu sérieux Virus non ciblé	Impacts sur la capacité Impacts financiers Impacts sur l'image	Importante
Collecter transmettre traiter documents de pré dédouanements	Collecter transmettre traiter documents de pré dédouanements	Confidentialité	Confidentiel	Employé peu sérieux	Impacts sur l'image	Importante
Suivre les dossiers et assister les clients - Disponibilité	Suivre les dossiers et assister les clients	Disponibilité	Moins de 4h	Employé peu sérieux	Impacts sur l'image	Importante
Suivre les dossiers et assister les clients - Intégrité	Suivre les dossiers et assister les clients	Intégrité	Maîtrisé	Employé peu sérieux	Impacts sur l'image	Importante
Suivre les dossiers et assister les clients - Confidentialité	Suivre les dossiers et assister les clients	Confidentialité	Confidentiel	Employé peu sérieux Client	Impacts sur l'image	Importante
Gère la souscription et l'accueil des clients - Preuve	Gère la souscription et l'accueil des clients	Preuve	Forte	Employé peu sérieux	Impacts sur l'image	Importante
Réception et Initialisation des Dossiers - Preuve	Réception et Initialisation des Dossiers	Preuve	Forte	Employé peu sérieux	Impacts sur l'image	Importante
Collecter transmettre traiter documents de pré dédouanements	Collecter transmettre traiter documents de pré dédouanements	Preuve	Forte	Employé peu sérieux	Impacts sur l'image	Importante
Suivre les dossiers et assister les clients - Preuve	Suivre les dossiers et assister les clients	Preuve	Grave	Employé peu sérieux	Impacts sur l'image	Critique

Responsable
Autorité
Consulté
Informé
Durée (en jours) 45
Nb Ressources 3

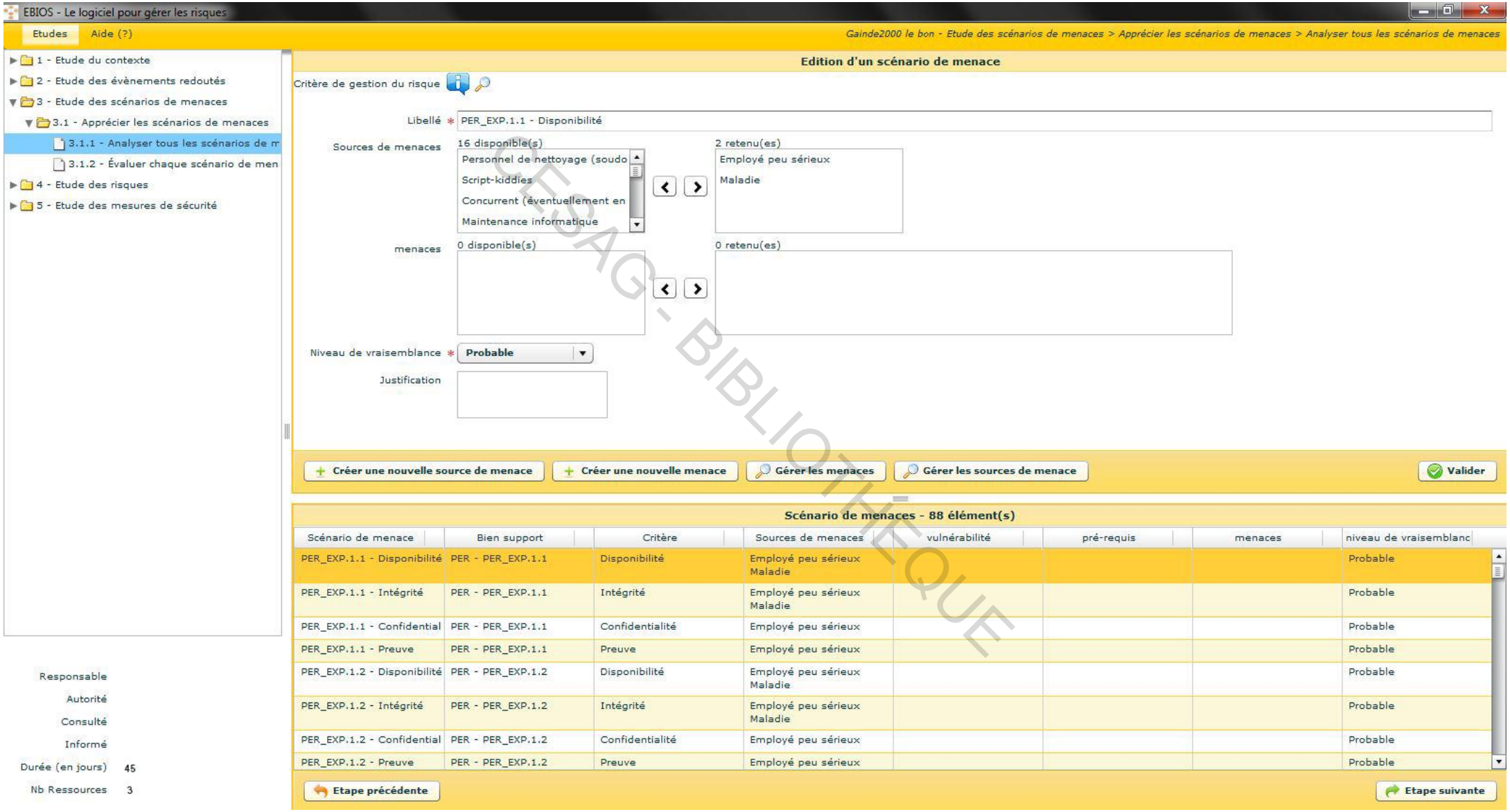
Etape précédente

Etape suivante

ANNEXE N°14 : évaluation des événements redoutés



ANNEXE N°15 : analyse des scénarios de menace



EBIOS - Le logiciel pour gérer les risques

Etudes Aide (?)

Gainde2000 le bon - Etude des scénarios de menaces > Apprécier les scénarios de menaces > Analyser tous les scénarios de menaces

- 1 - Etude du contexte
- 2 - Etude des évènements redoutés
- 3 - Etude des scénarios de menaces
  - 3.1 - Apprécier les scénarios de menaces
    - 3.1.1 - Analyser tous les scénarios de m
    - 3.1.2 - Évaluer chaque scénario de men
- 4 - Etude des risques
- 5 - Etude des mesures de sécurité

Responsable
Autorité
Consulté
Informé
Durée (en jours) 45
Nb Ressources 3

Edition d'un scénario de menace

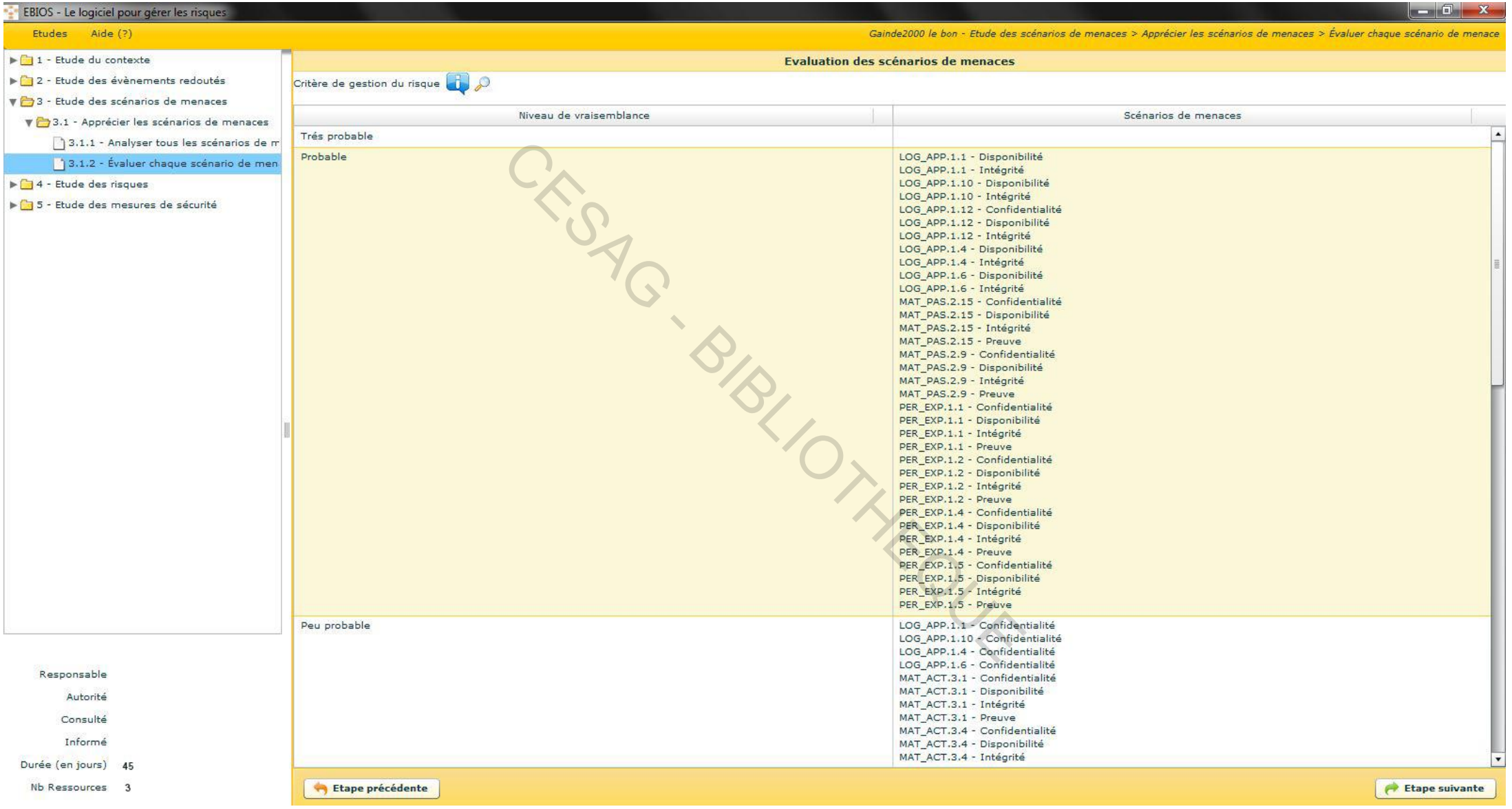
Scénario de menaces - 88 élément(s)

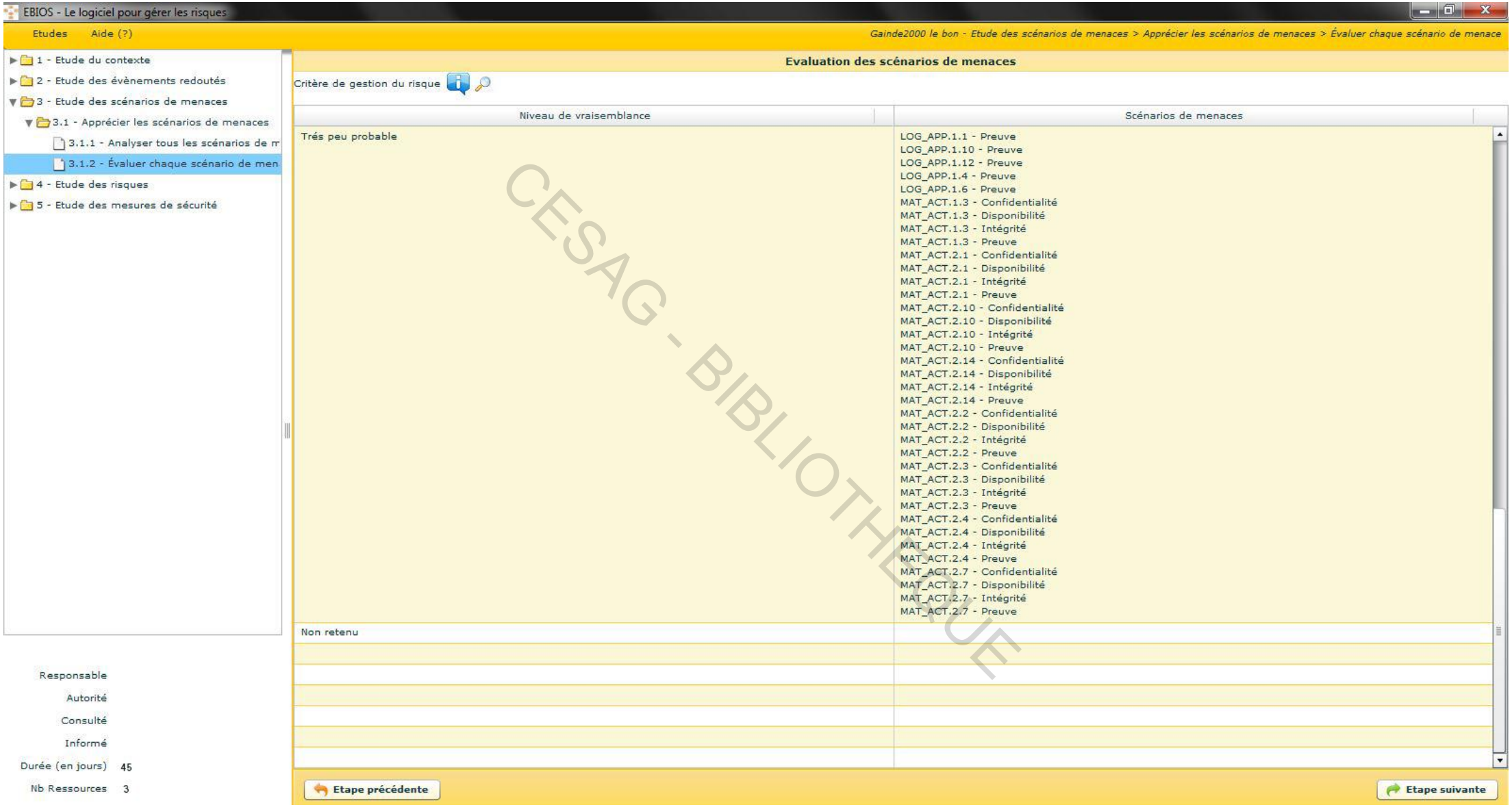
Scénario de menace	Bien support	Critère	Sources de menaces	vulnérabilité	pré-requis	mena	niveau de vraisemblance
PER_EXP.1.1 - Disponibilité	PER - PER_EXP.1.1	Disponibilité	Employé peu sérieux Maladie				Probable
PER_EXP.1.1 - Intégrité	PER - PER_EXP.1.1	Intégrité	Employé peu sérieux Maladie				Probable
PER_EXP.1.1 - Confidential	PER - PER_EXP.1.1	Confidentialité	Employé peu sérieux				Probable
PER_EXP.1.1 - Preuve	PER - PER_EXP.1.1	Preuve	Employé peu sérieux				Probable
PER_EXP.1.2 - Disponibilité	PER - PER_EXP.1.2	Disponibilité	Employé peu sérieux Maladie				Probable
PER_EXP.1.2 - Intégrité	PER - PER_EXP.1.2	Intégrité	Employé peu sérieux Maladie				Probable
PER_EXP.1.2 - Confidential	PER - PER_EXP.1.2	Confidentialité	Employé peu sérieux				Probable
PER_EXP.1.2 - Preuve	PER - PER_EXP.1.2	Preuve	Employé peu sérieux				Probable
PER_EXP.1.4 - Disponibilité	PER - PER_EXP.1.4	Disponibilité	Employé peu sérieux Maladie				Probable
PER_EXP.1.4 - Intégrité	PER - PER_EXP.1.4	Intégrité	Employé peu sérieux Maladie				Probable
PER_EXP.1.4 - Confidential	PER - PER_EXP.1.4	Confidentialité	Employé peu sérieux				Probable
PER_EXP.1.4 - Preuve	PER - PER_EXP.1.4	Preuve	Employé peu sérieux				Probable
PER_EXP.1.5 - Disponibilité	PER - PER_EXP.1.5	Disponibilité	Employé peu sérieux Maladie				Probable
PER_EXP.1.5 - Intégrité	PER - PER_EXP.1.5	Intégrité	Employé peu sérieux				Probable
PER_EXP.1.5 - Confidential	PER - PER_EXP.1.5	Confidentialité	Employé peu sérieux				Probable
PER_EXP.1.5 - Preuve	PER - PER_EXP.1.5	Preuve	Employé peu sérieux				Probable
LOG_APP.1.1 - Disponibilité	LOG - LOG_APP.1.1	Disponibilité	Maintenance informatique Panne électrique Virus non ciblé Employé peu sérieux (ceux Fournisseur d'accès Interne Hébergeur				Probable
LOG_APP.1.1 - Intégrité	LOG - LOG_APP.1.1	Intégrité	Maintenance informatique Panne électrique Virus non ciblé Employé peu sérieux (ceux Fournisseur d'accès Interne Hébergeur				Probable
LOG_APP.1.1 - Confidentia	LOG - LOG_APP.1.1	Confidentialité	Employé peu sérieux Virus non ciblé				Peu probable

Etape précédente

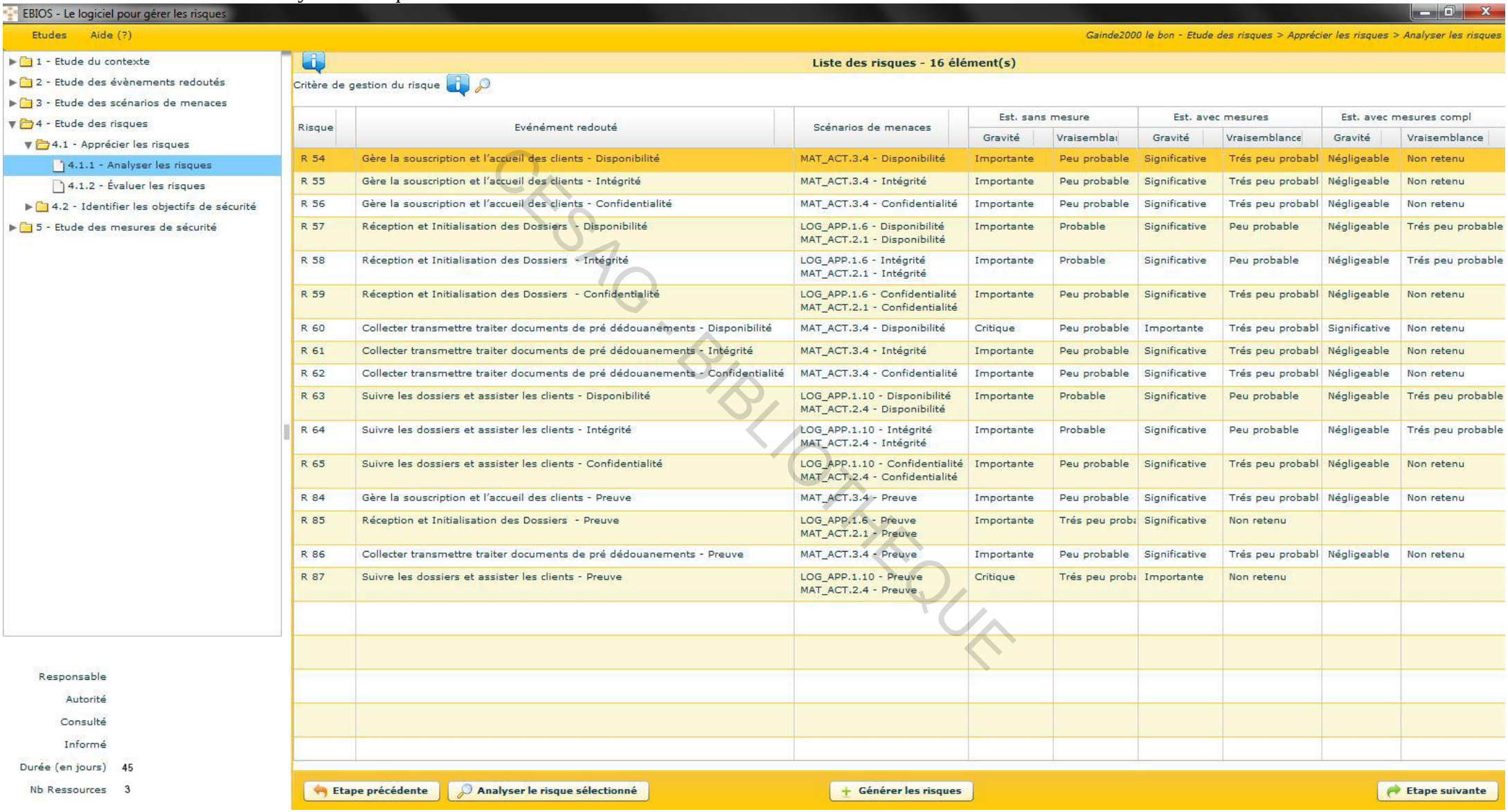
Etape suivante

ANNEXE N°16 : évaluation des scenarios de menace





ANNEXE N°17 :analyse des risques



EBIOS - Le logiciel pour gérer les risques

Etudes Aide (?)

Gainde2000 le bon - Etude des risques > Apprécier les risques > Analyser les risques

- 1 - Etude du contexte
- 2 - Etude des évènements redoutés
- 3 - Etude des scénarios de menaces
- 4 - Etude des risques
  - 4.1 - Apprécier les risques
    - 4.1.1 - Analyser les risques
    - 4.1.2 - Évaluer les risques
  - 4.2 - Identifier les objectifs de sécurité
- 5 - Etude des mesures de sécurité

Liste des risques - 16 élément(s)

Critère de gestion du risque

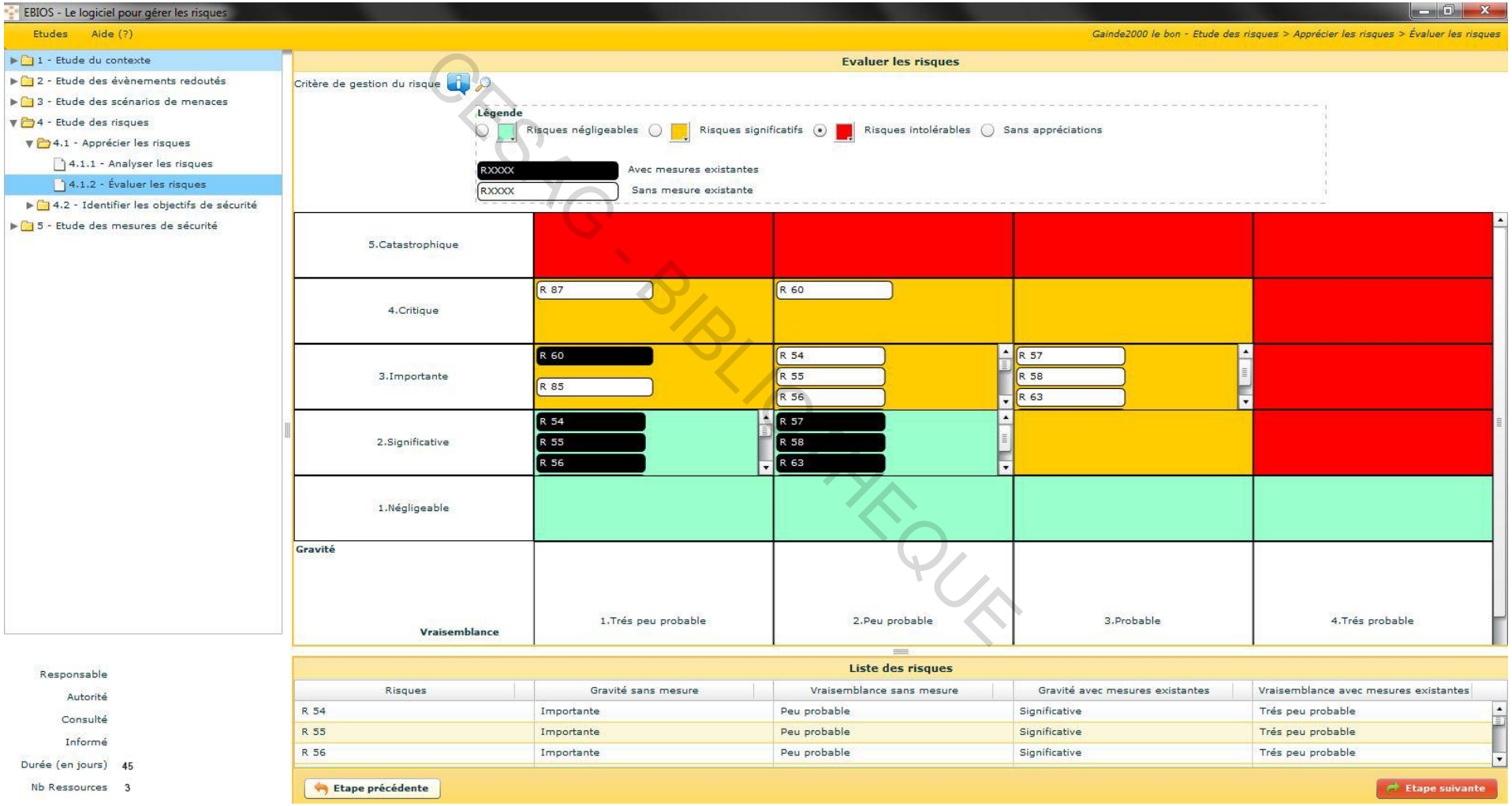
Risque	Evénement redouté	Scénarios de menaces	Est. sans mesure		Est. avec mesures		Est. avec mesures compl	
			Gravité	Vraisemblai	Gravité	Vraisemblance	Gravité	Vraisemblance
R 54	Gère la souscription et l'accueil des clients - Disponibilité	MAT_ACT.3.4 - Disponibilité	Importante	Peu probable	Significative	Trés peu probabl	Négligeable	Non retenu
R 55	Gère la souscription et l'accueil des clients - Intégrité	MAT_ACT.3.4 - Intégrité	Importante	Peu probable	Significative	Trés peu probabl	Négligeable	Non retenu
R 56	Gère la souscription et l'accueil des clients - Confidentialité	MAT_ACT.3.4 - Confidentialité	Importante	Peu probable	Significative	Trés peu probabl	Négligeable	Non retenu
R 57	Réception et Initialisation des Dossiers - Disponibilité	LOG_APP.1.6 - Disponibilité MAT_ACT.2.1 - Disponibilité	Importante	Probable	Significative	Peu probable	Négligeable	Trés peu probable
R 58	Réception et Initialisation des Dossiers - Intégrité	LOG_APP.1.6 - Intégrité MAT_ACT.2.1 - Intégrité	Importante	Probable	Significative	Peu probable	Négligeable	Trés peu probable
R 59	Réception et Initialisation des Dossiers - Confidentialité	LOG_APP.1.6 - Confidentialité MAT_ACT.2.1 - Confidentialité	Importante	Peu probable	Significative	Trés peu probabl	Négligeable	Non retenu
R 60	Collecter transmettre traiter documents de pré dédouanements - Disponibilité	MAT_ACT.3.4 - Disponibilité	Critique	Peu probable	Importante	Trés peu probabl	Significative	Non retenu
R 61	Collecter transmettre traiter documents de pré dédouanements - Intégrité	MAT_ACT.3.4 - Intégrité	Importante	Peu probable	Significative	Trés peu probabl	Négligeable	Non retenu
R 62	Collecter transmettre traiter documents de pré dédouanements - Confidentialité	MAT_ACT.3.4 - Confidentialité	Importante	Peu probable	Significative	Trés peu probabl	Négligeable	Non retenu
R 63	Suivre les dossiers et assister les clients - Disponibilité	LOG_APP.1.10 - Disponibilité MAT_ACT.2.4 - Disponibilité	Importante	Probable	Significative	Peu probable	Négligeable	Trés peu probable
R 64	Suivre les dossiers et assister les clients - Intégrité	LOG_APP.1.10 - Intégrité MAT_ACT.2.4 - Intégrité	Importante	Probable	Significative	Peu probable	Négligeable	Trés peu probable
R 65	Suivre les dossiers et assister les clients - Confidentialité	LOG_APP.1.10 - Confidentialité MAT_ACT.2.4 - Confidentialité	Importante	Peu probable	Significative	Trés peu probabl	Négligeable	Non retenu
R 84	Gère la souscription et l'accueil des clients - Preuve	MAT_ACT.3.4 - Preuve	Importante	Peu probable	Significative	Trés peu probabl	Négligeable	Non retenu
R 85	Réception et Initialisation des Dossiers - Preuve	LOG_APP.1.6 - Preuve MAT_ACT.2.1 - Preuve	Importante	Trés peu probi	Significative	Non retenu		
R 86	Collecter transmettre traiter documents de pré dédouanements - Preuve	MAT_ACT.3.4 - Preuve	Importante	Peu probable	Significative	Trés peu probabl	Négligeable	Non retenu
R 87	Suivre les dossiers et assister les clients - Preuve	LOG_APP.1.10 - Preuve MAT_ACT.2.4 - Preuve	Critique	Trés peu probi	Importante	Non retenu		

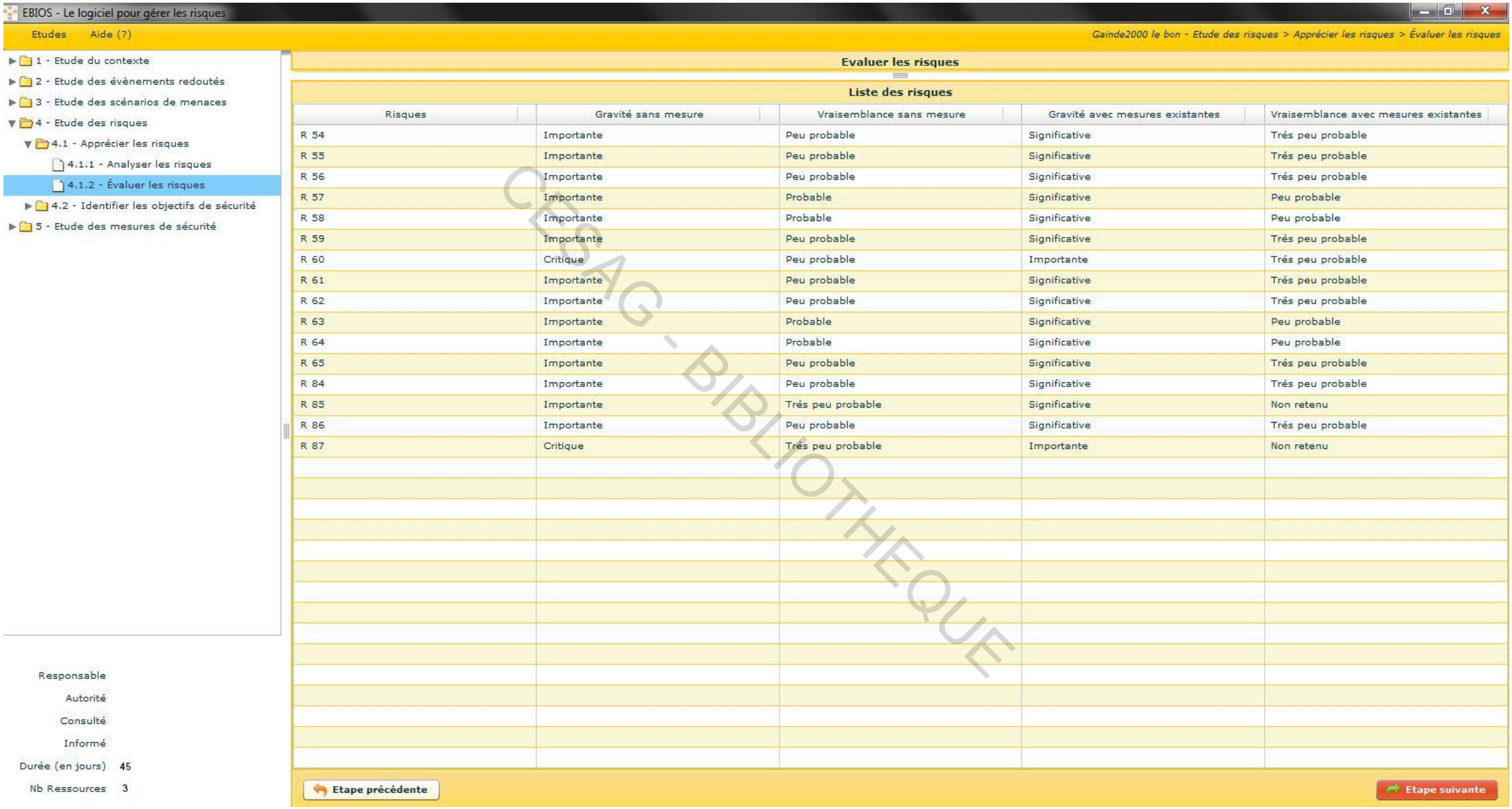
Responsable
Autorité
Consulté
Informé
Durée (en jours) 45
Nb Ressources 3

Etape précédente | Analyser le risque sélectionné | Générer les risques | Etape suivante

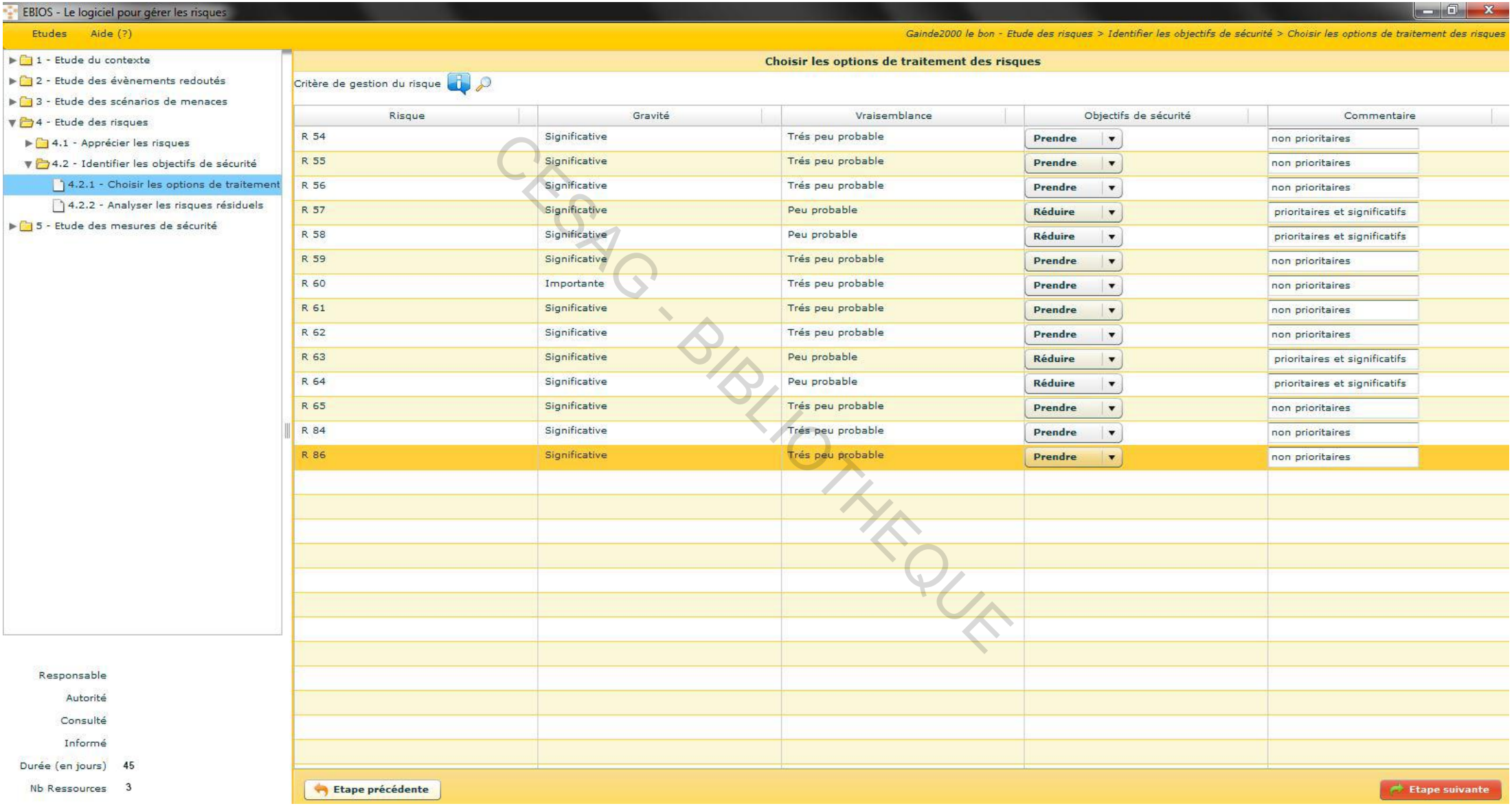
ANNEXE N°18 : évaluation des risques

Nous constatons que la plupart des risques se trouvent dans la zone d'acceptabilité avec une gravité significative et une vraisemblance peu probable ; mais aussi certains risques se trouvent à un niveau modéré (limite de risque acceptable) avec une gravité importante et une vraisemblance probable.

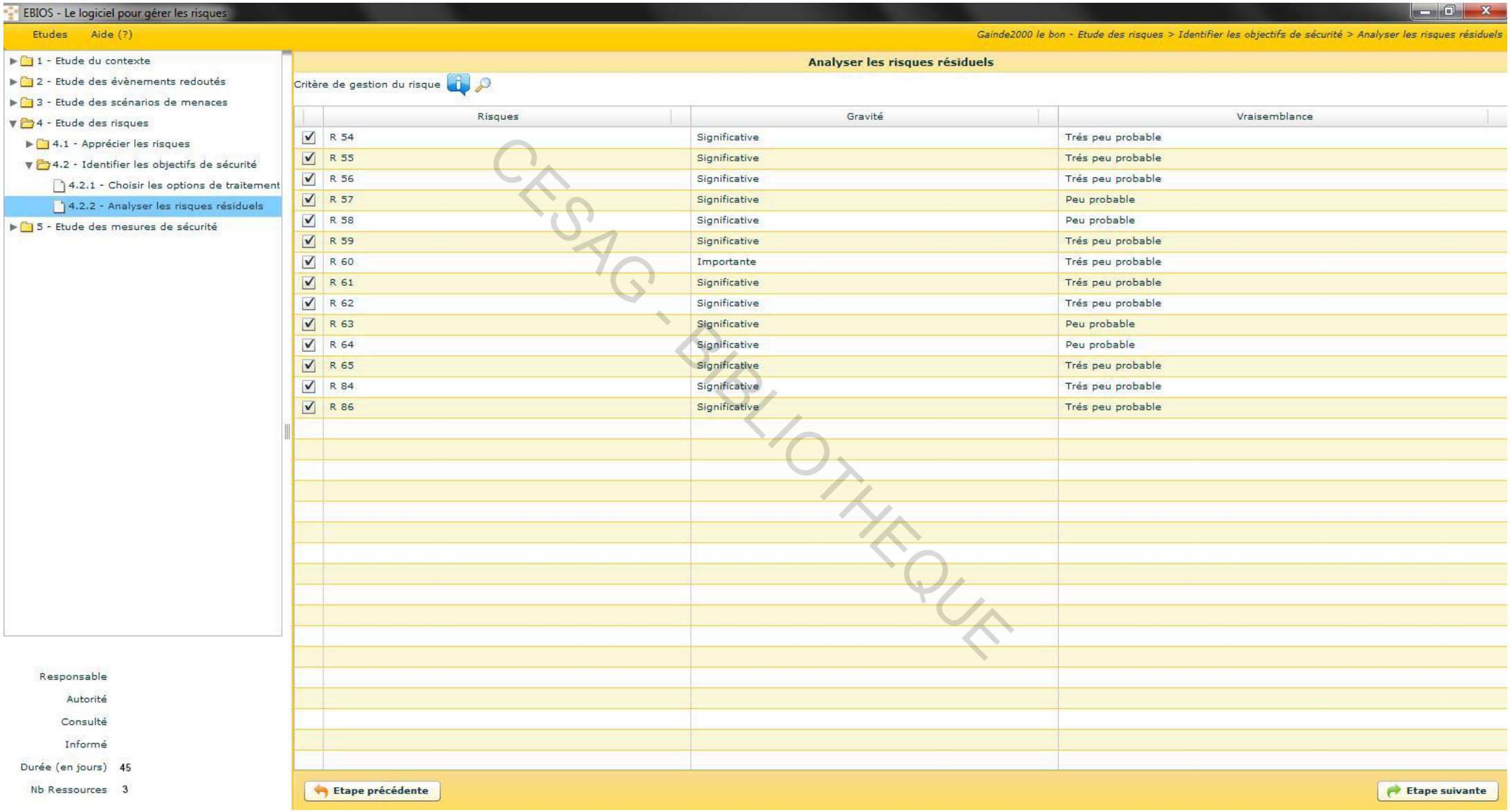




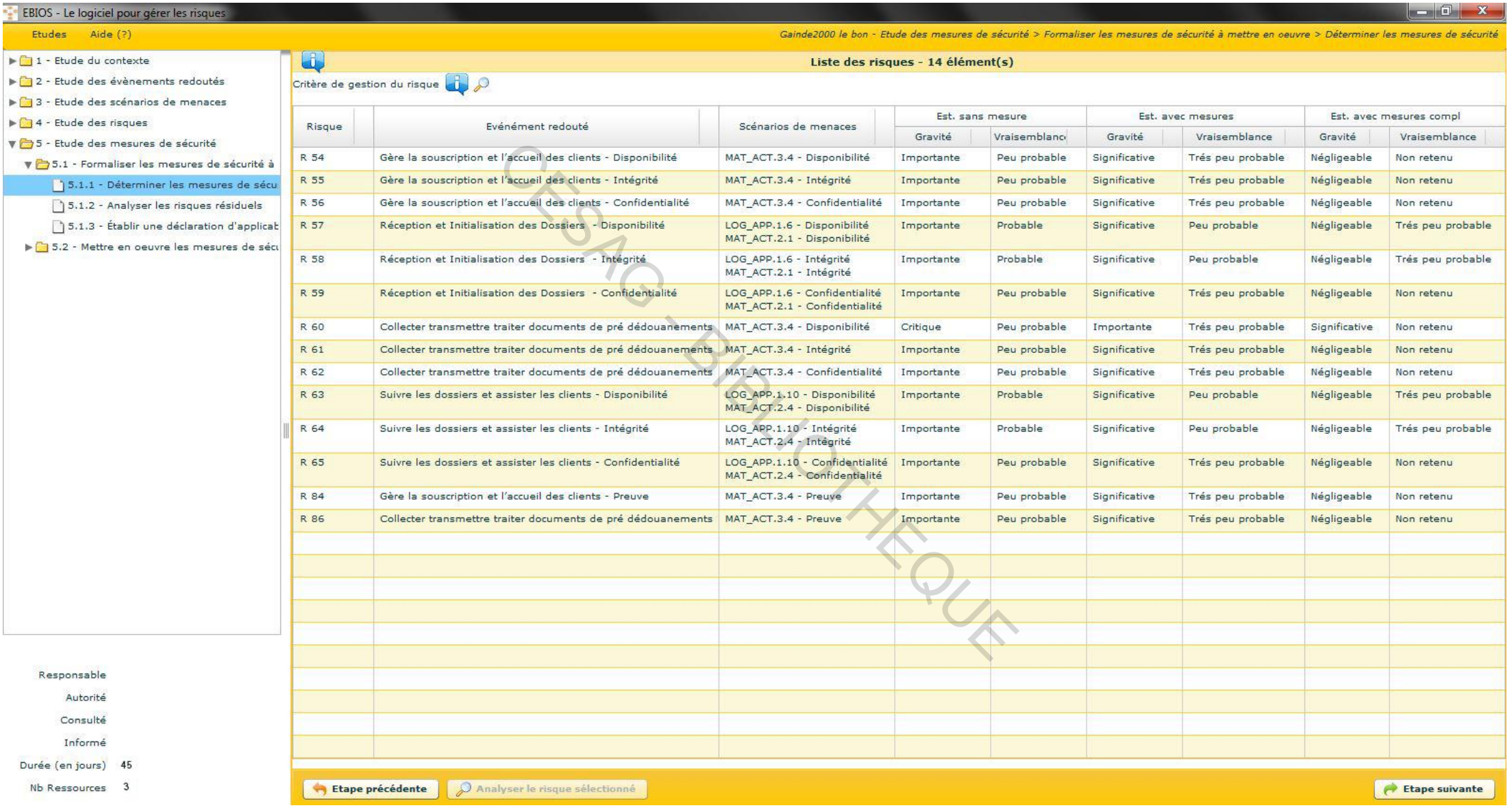
ANNEXE N°19 : choix des options de traitement des risques



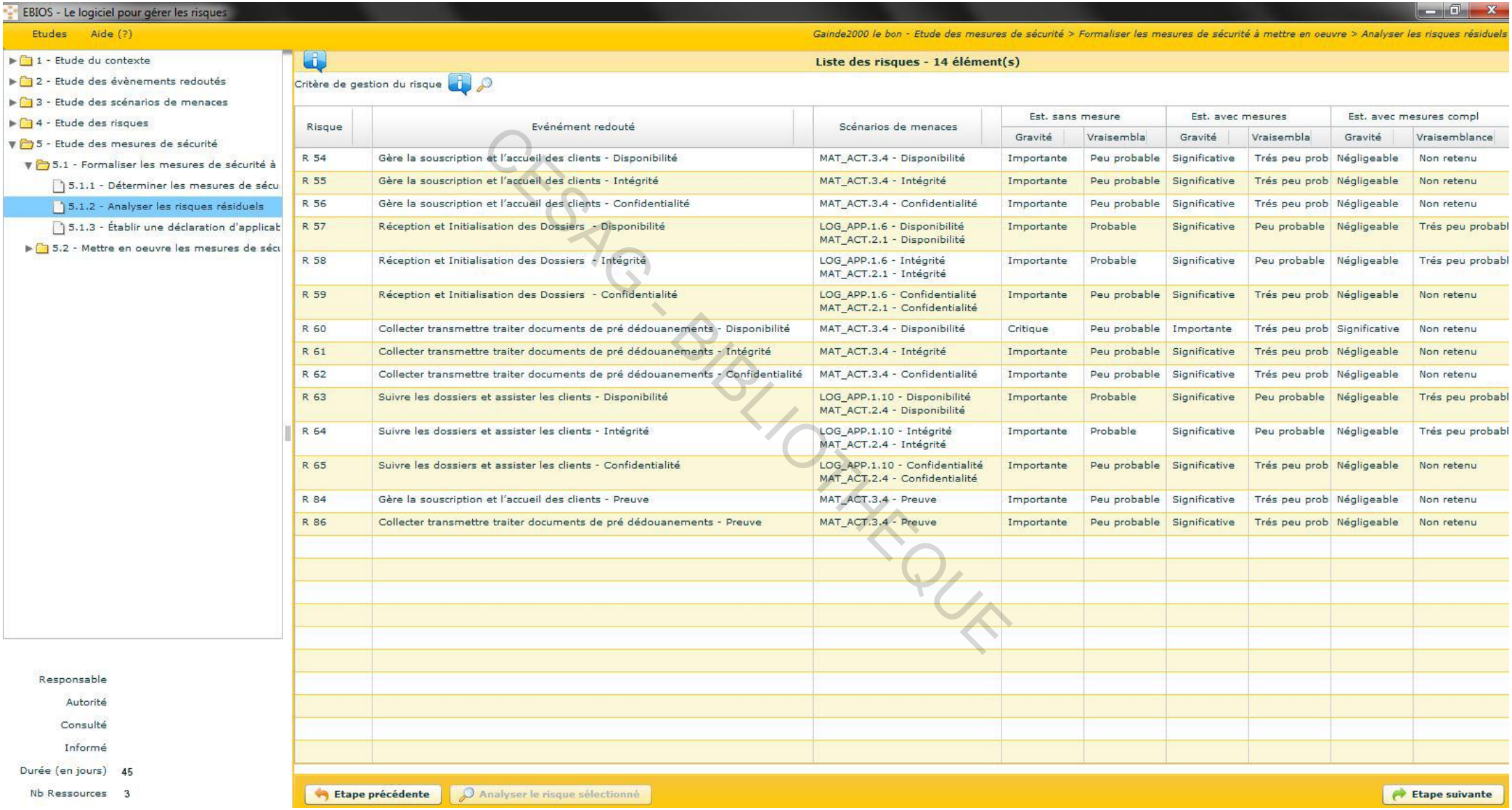
ANNEXE N°20 : analyse des risques résiduels



ANNEXE N°21 : détermination des mesures de sécurité



ANNEXE N°22 : analyse des risques résiduels



EBIOS - Le logiciel pour gérer les risques

Etudes Aide (?)

Gainde2000 le bon - Etude des mesures de sécurité > Formaliser les mesures de sécurité à mettre en oeuvre > Analyser les risques résiduels

- 1 - Etude du contexte
- 2 - Etude des évènements redoutés
- 3 - Etude des scénarios de menaces
- 4 - Etude des risques
- 5 - Etude des mesures de sécurité
  - 5.1 - Formaliser les mesures de sécurité à
    - 5.1.1 - Déterminer les mesures de sécu
    - 5.1.2 - Analyser les risques résiduels
    - 5.1.3 - Établir une déclaration d'applicat
  - 5.2 - Mettre en oeuvre les mesures de sécu

Responsable
Autorité
Consulté
Informé
Durée (en jours) 45
Nb Ressources 3

Liste des risques - 14 élément(s)

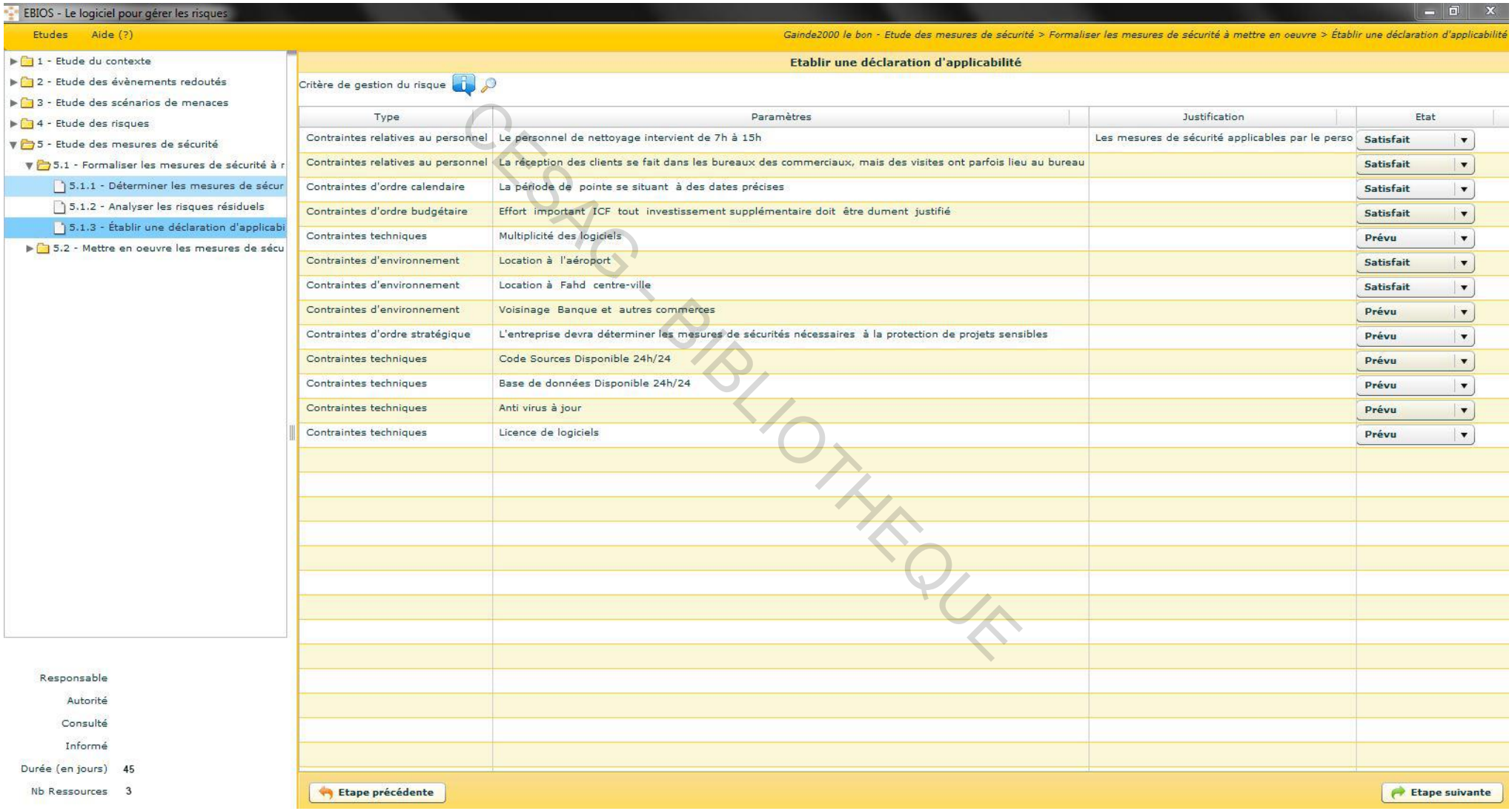
Critère de gestion du risque

Risque	Evénement redouté	Scénarios de menaces	Est. sans mesure		Est. avec mesures		Est. avec mesures compl	
			Gravité	Vraisembla	Gravité	Vraisembla	Gravité	Vraisemblance
R 54	Gère la souscription et l'accueil des clients - Disponibilité	MAT_ACT.3.4 - Disponibilité	Importante	Peu probable	Significative	Trés peu prob	Négligeable	Non retenu
R 55	Gère la souscription et l'accueil des clients - Intégrité	MAT_ACT.3.4 - Intégrité	Importante	Peu probable	Significative	Trés peu prob	Négligeable	Non retenu
R 56	Gère la souscription et l'accueil des clients - Confidentialité	MAT_ACT.3.4 - Confidentialité	Importante	Peu probable	Significative	Trés peu prob	Négligeable	Non retenu
R 57	Réception et Initialisation des Dossiers - Disponibilité	LOG_APP.1.6 - Disponibilité MAT_ACT.2.1 - Disponibilité	Importante	Probable	Significative	Peu probable	Négligeable	Trés peu probabl
R 58	Réception et Initialisation des Dossiers - Intégrité	LOG_APP.1.6 - Intégrité MAT_ACT.2.1 - Intégrité	Importante	Probable	Significative	Peu probable	Négligeable	Trés peu probabl
R 59	Réception et Initialisation des Dossiers - Confidentialité	LOG_APP.1.6 - Confidentialité MAT_ACT.2.1 - Confidentialité	Importante	Peu probable	Significative	Trés peu prob	Négligeable	Non retenu
R 60	Collecter transmettre traiter documents de pré dédouanements - Disponibilité	MAT_ACT.3.4 - Disponibilité	Critique	Peu probable	Importante	Trés peu prob	Significative	Non retenu
R 61	Collecter transmettre traiter documents de pré dédouanements - Intégrité	MAT_ACT.3.4 - Intégrité	Importante	Peu probable	Significative	Trés peu prob	Négligeable	Non retenu
R 62	Collecter transmettre traiter documents de pré dédouanements - Confidentialité	MAT_ACT.3.4 - Confidentialité	Importante	Peu probable	Significative	Trés peu prob	Négligeable	Non retenu
R 63	Suivre les dossiers et assister les clients - Disponibilité	LOG_APP.1.10 - Disponibilité MAT_ACT.2.4 - Disponibilité	Importante	Probable	Significative	Peu probable	Négligeable	Trés peu probabl
R 64	Suivre les dossiers et assister les clients - Intégrité	LOG_APP.1.10 - Intégrité MAT_ACT.2.4 - Intégrité	Importante	Probable	Significative	Peu probable	Négligeable	Trés peu probabl
R 65	Suivre les dossiers et assister les clients - Confidentialité	LOG_APP.1.10 - Confidentialité MAT_ACT.2.4 - Confidentialité	Importante	Peu probable	Significative	Trés peu prob	Négligeable	Non retenu
R 84	Gère la souscription et l'accueil des clients - Preuve	MAT_ACT.3.4 - Preuve	Importante	Peu probable	Significative	Trés peu prob	Négligeable	Non retenu
R 86	Collecter transmettre traiter documents de pré dédouanements - Preuve	MAT_ACT.3.4 - Preuve	Importante	Peu probable	Significative	Trés peu prob	Négligeable	Non retenu

Etape précédente | Analyser le risque sélectionné | Etape suivante

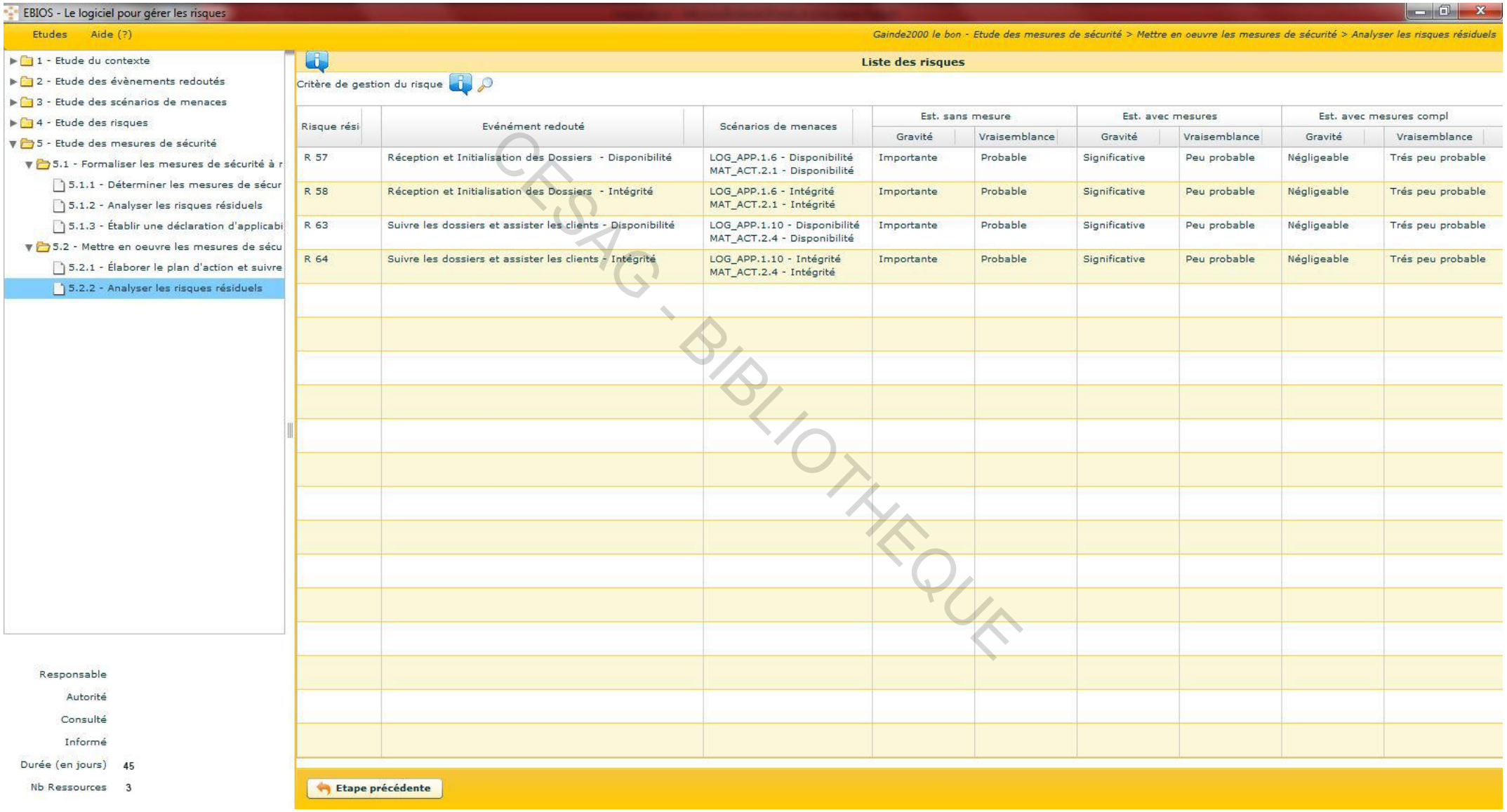
ANNEXE N°23 : établissement d'une déclaration d'applicabilité

Justification : Les mesures de sécurité applicables par le personnel ne demandent pas une grande expertise.



ANNEXE N°24 : élaboration d'un plan d'action et suivie ; *PS : Pour des raisons de confidentialité, nous avons flouté le nom Des responsables.*

ANNEXE N°25: analyse risques résiduels



ANNEXE N°26: Overview of ISO 27001:2013 Annex A

Annex A of ISO 27001 is probably the most famous annex of all the ISO standards – this is because it provides an essential tool for managing security: a list of security controls (or safeguards) that are to be used to improve security of information.

- **A.5 Information security policies** – controls on how the policies are written and reviewed
- **A.6 Organization of information security** – controls on how the responsibilities are assigned; also includes the controls for mobile devices and teleworking
- **A.7 Human resources security** – controls prior to employment, during, and after the employment
- **A.8 Asset management** – controls related to inventory of assets and acceptable use, also for information classification and media handling
- **A.9 Access control** – controls for Access control policy, user access management, system and application access control, and user responsibilities
- **A.10 Cryptography** – controls related to encryption and key management
- **A.11 Physical and environmental security** – controls defining secure areas, entry controls, protection against threats, equipment security, secure disposal, clear desk and clear screen policy, etc.
- **A.12 Operational security** – lots of controls related to management of IT production: change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, etc.
- **A.13 Communications security** – controls related to network security, segregation, network services, transfer of information, messaging, etc.
- **A.14 System acquisition, development and maintenance** – controls defining security requirements and security in development and support processes
- **A.15 Supplier relationships** – controls on what to include in agreements, and how to monitor the suppliers
- **A.16 Information security incident management** – controls for reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence
- **A.17 Information security aspects of business continuity management** – controls requiring the planning of business continuity, procedures, verification and reviewing, and IT redundancy
- **A.18 Compliance** – controls requiring the identification of applicable laws and regulations, intellectual property protection, personal data protection, and reviews of information security

One of the biggest myths about ISO 27001 is that it is focused on IT – as you can see from the above sections, this is not quite true: while IT is certainly important, IT alone cannot protect information. Physical security, legal protection, human resources management, organizational issues – all of them together are required to secure the information.

The best way to understand Annex A is to think of it as a catalogue of security controls you can select from – out of the 114 controls that are listed in Annex A, you can choose the ones that are applicable to your company.

BIBLIOGRAPHIE

1. ANSSI (2015), présentation de la méthode EBIOS, http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

2. AUTISSIER David, DELAYE Valérie (2008), *Mesurer la performance du système d'information*, EYROLLES éditions d'organisation, paris, 214 pages.

3. BALLE Francis (2003), *Médias et société*, Édition Montchrestien, Paris ,835 pages.

4. BAPTISTE Jean l. (2012) , *MERISE guide pratique*, ENI éditions, Paris, 280 pages.

5. BARTHELEMY Bernard, COURREGE Philippe (2004), *Gestion des risques: méthode d'optimisation globale*, Editions d'Organisation, Paris, 480 pages.

6. BESSON Bernard, POSSIN Jean-Claude (2012), Pourquoi gérer ces nouveaux risques ? http://www.gpomag.fr/web/index.php/2013-07-22-14-06-19/gestion-finance/financement-d-activite/2540-pourquoi-gerer-ces-nouveaux-risques

7. BOURASSA Michel (2015), Une gestion rigoureuse et structurée des risques de projet pour faire face à un environnement de plus en plus complexe et incertain, http://agrmpi.ca/une-gestion-rigoureuse-et-structuree-des-risques-de-projet-pour-faire-face-a-un-environnement-de-plus-en-plus-complexe-et-incertain/

8. BOURROUILH Olivier, SCHICK Pierre & VERA Jacques (2010), *Audit interne et référentiels de risques*, DUNOD, Paris, 340 pages.

9. BREILLAT Jacques (2007) Article paru le 11-05-2007 dans APS N°1578 – Les clefs de l'Intelligence Economique, http://jacques.breillat.fr/veille-strategique/de-la-superiorite-de-l%E2%80%99informel

10. BRETON Philippe, PROULX Serge (2002), *L'explosion de la communication à l'aube du XXI^e siècle*, La Découverte Edition, Paris, 389 pages.

11. CLEARY Sean, MALLERET Thierry (2006), *Risques - Perception, évaluation, gestion*, MAXIMA, Paris, 253 pages.

12. Club des contrôleurs de gestion des ministères économiques et financiers (2013), Recommandations pour la collecte et le traitement de données. http://www.performance-publique.budget.gouv.fr/sites/performance_publique/files/files/documents/performance/controle_gestion/documentation/guides/17reco-collecte-donnees.pdf

13. CLUSIF (2004), Méthode Harmonisée d'Analyse de Risques (MEHARI), Principes et mécanismes, Version 3, http://www.clusif.asso.fr/fr/production/mehari/presentation.asp

14. Comment ca marche (2014), Introduction à la sécurité informatique http://static.ccm2.net/www.commentcamarche.net/contents/pdf/introduction-a-la-securite-informatique-1033-mvt6x9.pdf

15. CORNUEJOLS Antoine (2009), bases de données concepts et programmation, https://www.lri.fr/~antoine/Courses/AGRO/Cours-BD/Poly-BD.pdf

16. DELMOND Marie-Hélène, PETIT Yves, GAUTIER Jean-Michel (2003), *Management des systèmes d'information*, Edition Dunod, Paris, 222 pages

17. DELEPONE J.F. (2004), *Introduction théorique à l'informatique*, AfricaComputing, Abidjan, 510 pages.

18. DIENG Aissatou (2015), Méthode d'Appréciation et analyse des risques, *document-GAINDE2000*, 10 pages.

19. Direction Centrale de la Sécurité des Systèmes d'Information (2004), Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS), http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html

20. DUCRET Linda (2012), Pourquoi gérer ces nouveaux risques ? http://www.gpomag.fr/web/index.php/2013-07-22-14-06-19/gestion-finance/financement-d-activite/2540-pourquoi-gerer-ces-nouveaux-risques

21. ETIEVANT Hugo (2006) Normes de sécurité : les méthodes d'analyse des risques, Mis à jour le 19 août 2006, http://cyberzoide.developpez.com/securite/methodes-analyse-risques/

22. ETIEVANT Hugo (2006), CCTA Risk Analysis and Management Method (cramm) http://cyberzoide.developpez.com/securite/methodes-analyse-risques/

23. FONDIN Hubert (2001), La science de l'information : posture épistémologique et spécificité disciplinaire, *Documentaliste - Sciences de l'information*, vol. 38, 112-122.

24. GRAWITZ Madeleine(1979), *Méthodes des sciences sociales*, Dalloz 4ieme édition, Paris, 1102 pages.

25. IFACI(2007*), Le management des risques d'entreprise/cadre de référence, techniques d'application*, EYROLLES édition d'organisation, Paris, 338 pages.

26. ISO Guide 73:2009 Management du risque/Vocabulaire, 15 pages.

27. JLS (2010) Démarche ISO 2700, http://www.fidens.fr/articles/qu-est-ce-que-la-norme-iso27005-59.html

28. LAFITTE Michel (2003), Sécurité des systèmes d'information et maîtrise des risques, revue banque Edition, Paris, 127 pages.

29. LAMBIN Jean jacques(1990), *La Recherche marketing,* analyser mesurer prévoir, Edition Mcgraw-Hill, Paris, 424pages.

30. LEGER Marc-André(2013), *Introduction à la gestion de risque informationnel*, CRHOMA, Paris, 238 pages.

31. LENDREVIE Jacques, EMPRIN Catherine, BAYNAST Arnaud de (2008), *Publicitor : Communication 360° off et on line*, Dunod 7ieme Edition, 669 pages.

32. MARCINIAK Roland, ROWE Frantz (2000), *Systèmes d'Information, Dynamique et Organisation*, 2ème édition Economica, Paris, 111 pages.

33. MARTINET Bruno et MARTI Yves-Michel (1995), *L'intelligence économique (les yeux et les oreilles de l'entreprise), Editions* d'organisation, Paris, 244 pages.

34. MAYER Nicolas, HUMBERT Jean-Philippe (2006), la gestion des risques pour les systèmes d'information,http://www.nmayer.eu/publis/NMA-JPH_MISC24.pdf

35. MELLON Carnegie - Software Engineering Institute (2014), Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), http://www.cert.org/octave/

36. MOISAND Dominique, GARNIER DE LABAREYRE Fabrice (2009), *CobiT Pour une meilleure gouvernance des systèmes d'information*, EYROLLES éditions, paris, 258 pages.

37. PILLOUX Jean François, CAILLEREZ pascal (2011) *Tout sur les systèmes informations. Grandes, moyennes et petites entreprises*, 2ieme Edition DUNOD, 208 pages.

38. PUYBAREAU Florence (2014), la gestion du risque : une problématique qui monte dans les entreprises, *supplément option finance N°1255*, 26.

39. REIX Robert (2011), *Systèmes d'information et management des organisations*, 6e édition Vuibert, Paris, 480 pages.

40. REIX Robert (2002), *Système d'information et management des organisations*, 4ème édition Vuibert, Paris, 443 pages.

41. REIX Robert, ROWE Frantz(2002), *Faire de la recherche en systèmes d'information*, Éditions Vuibert, 359 pages.

42. RENARD jacques (2010*) Théorie et pratique de l'audit interne*, Éditions d'Organisation Groupe Eyrolles, Paris ,471 pages.

43. ROWE Frantz(2002), *Faire de la recherche en SI*, Edition Vuibert, Paris, 359 pages.

44. Scala R.M. Di (2004), *L'essentiel de l'informatique et de la programmation*, Berti EDS, Paris, 1018 pages.

45. SHANNON Claude E. et WEAVER Warren (1975), trad. française : *La théorie mathématique de la communication*, Retz-CEPL, Paris, 188 pages.

46. SIMONNET Véronique (2003), *Le capital humain dans Encyclopédie des ressources humaines (José Allouche)*, Edition Vuibert, paris, 144 pages.

47. TARDIEU Hubert (1994), *La Méthode MERISE : principes et outils*, Tome 1. Edition Organisation, Paris, 352 pages.

48. TIRATAYFrédéric (2013), Sécurité du système d'information : encore un centre de coût?http://www.journaldunet.com/solutions/expert/53968/securite-du-systeme-d-information---encore-un-centre-de-cout.shtml

49. ZMUD Robert W., BOYNTON Andrew C. (1990), *AC. Management information Systems: Reading and Cases*, Scott Foresman Edition, Boston, 511 pages.