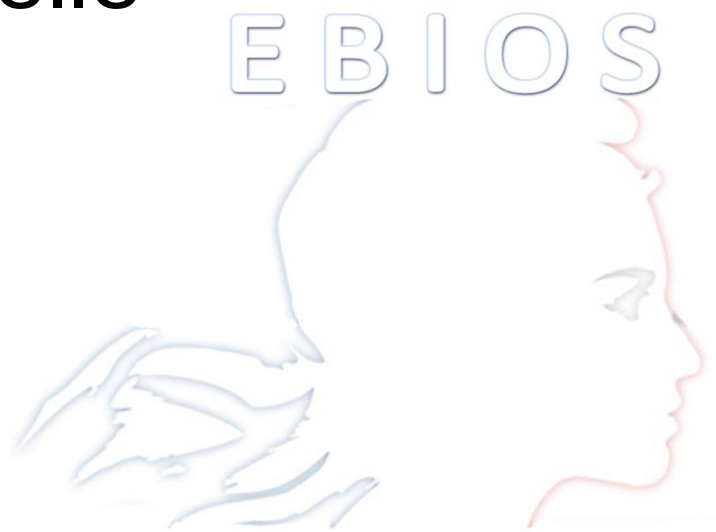
outil EBIOS 2010

retour d’expérience de l'utilisation de l'outil en situation réelle



Alain MARCAY

Laurent JUIN

Xavier GUEGUEN

Orange Consulting

sommaire

- le contexte d’utilisation de l’outil en situation réelle
- notre retour d’expérience sur 4 points :
  - l'ergonomie et l’utilisation de l’interface ;
  - l'identification de la cause des risques et des mesures ;
  - l'export des données vers un document (FEROS) ;
  - L’actualisation de l’analyse des risques.
- notre conclusion
  - un outil au support de la méthodologie ;
  - des améliorations attendues.

le contexte de l'utilisation de l'outil

réalisation de deux études de risques dans un contexte étatique :

- plateforme d'hébergement de services (web, partage de fichiers, messagerie …) ;
- plateforme IGC dédiée à l'accès aux services hébergés.

pourquoi avoir utilisé l'outil :

- outil diffusable librement côté client et côté Orange ;
- utilisation du référentiel EBIOS 2010 ;
- simplification de la prise en compte des remarques du client ;
- simplification des mises à jour des analyses de risques.

un contexte réel plus complexe

l'outil a été évalué sur les exemples fournis :

- étude Archimède (4 BE / 37 BS);
- accès distant (2 BE / 5 BS) ;
- cloud computing (3 BE / 5 BS).

le contexte réel des études s'est avéré largement plus complexe :

- plateforme de services (15 BE / 20 BS) ;
- IGC (16 BE / 21 BS).

des difficultés ont été rapidement rencontrées

plusieurs types de difficultés rencontrées :

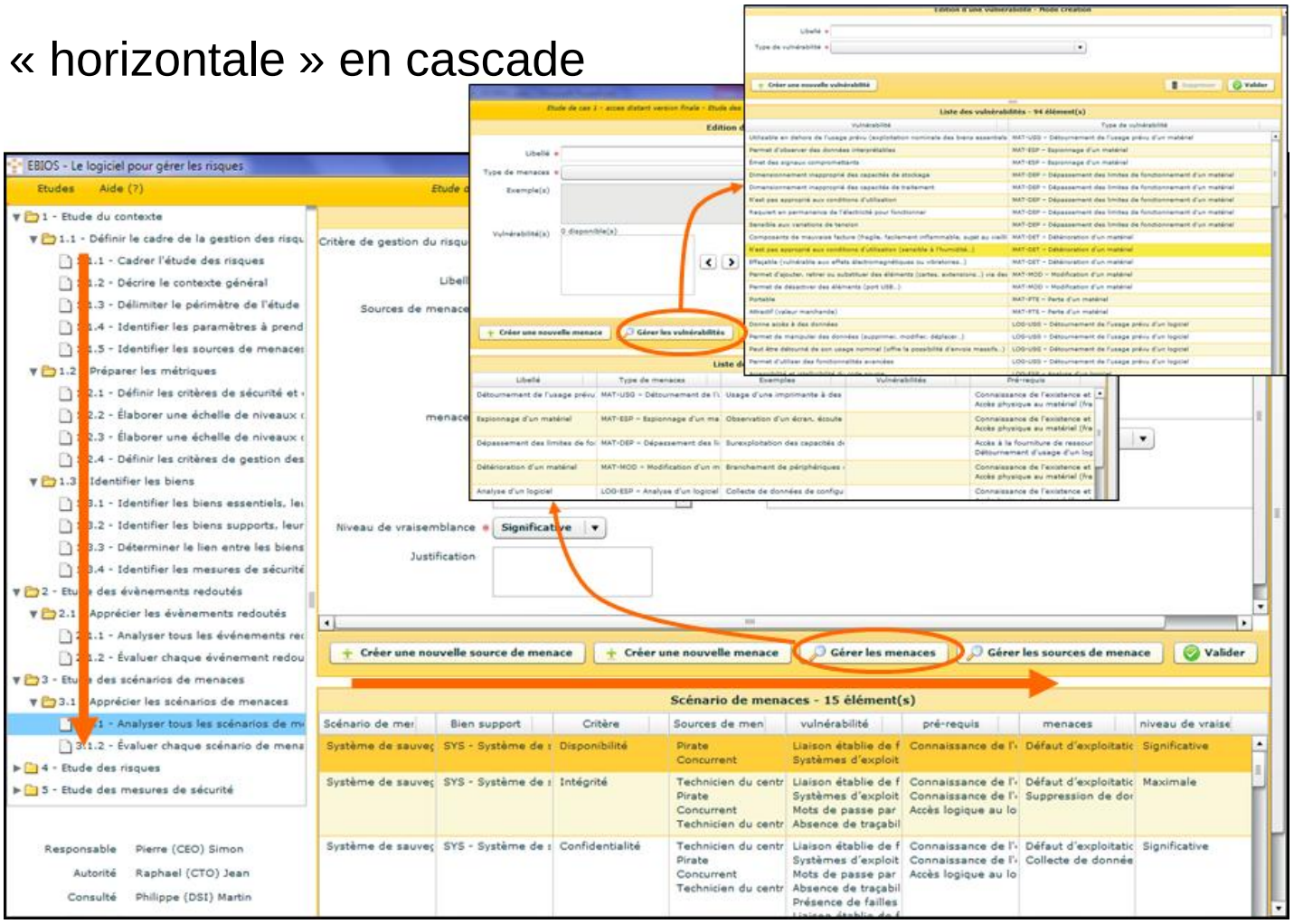
- une ergonomie perfectible de l'interface couplée à des dysfonctionnements ;
- une présentation des risques qui rend difficile l'identification de leur traitement ;
- les exports proposés par l'outil ne répondent pas aux attentes :
  - les données saisies dans l'outil ne sont pas toujours exportées.
  - le format des données exportées n'est pas lisible.
- une mise à jour de l'analyse du contexte conduisant à une perte des évaluations des risques ;

l’ergonomie
perfectible et couplée à
des dysfonctionnements

une navigation pas toujours intuitive

Une désorientation dans les écrans en cours de saisie

- Navigation « verticale »
- Navigation « horizontale » en cascade

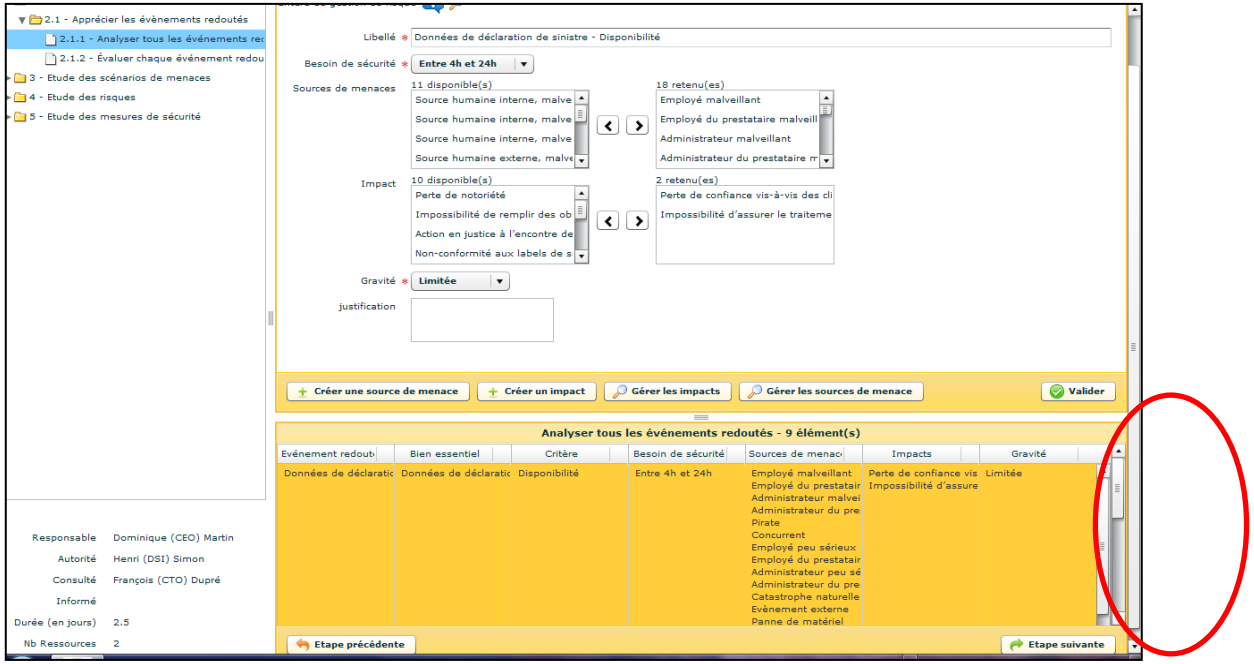


diffusion libre

une profusion d’ascenseurs

nécessite une vigilance de tous les instants

- cascade jusqu’à 3 niveaux d’ascenseurs
- des listes qui reviennent à la première ligne
- saut de plusieurs lignes simultanées non visible via l’ascenseur
- affichage incomplet des lignes

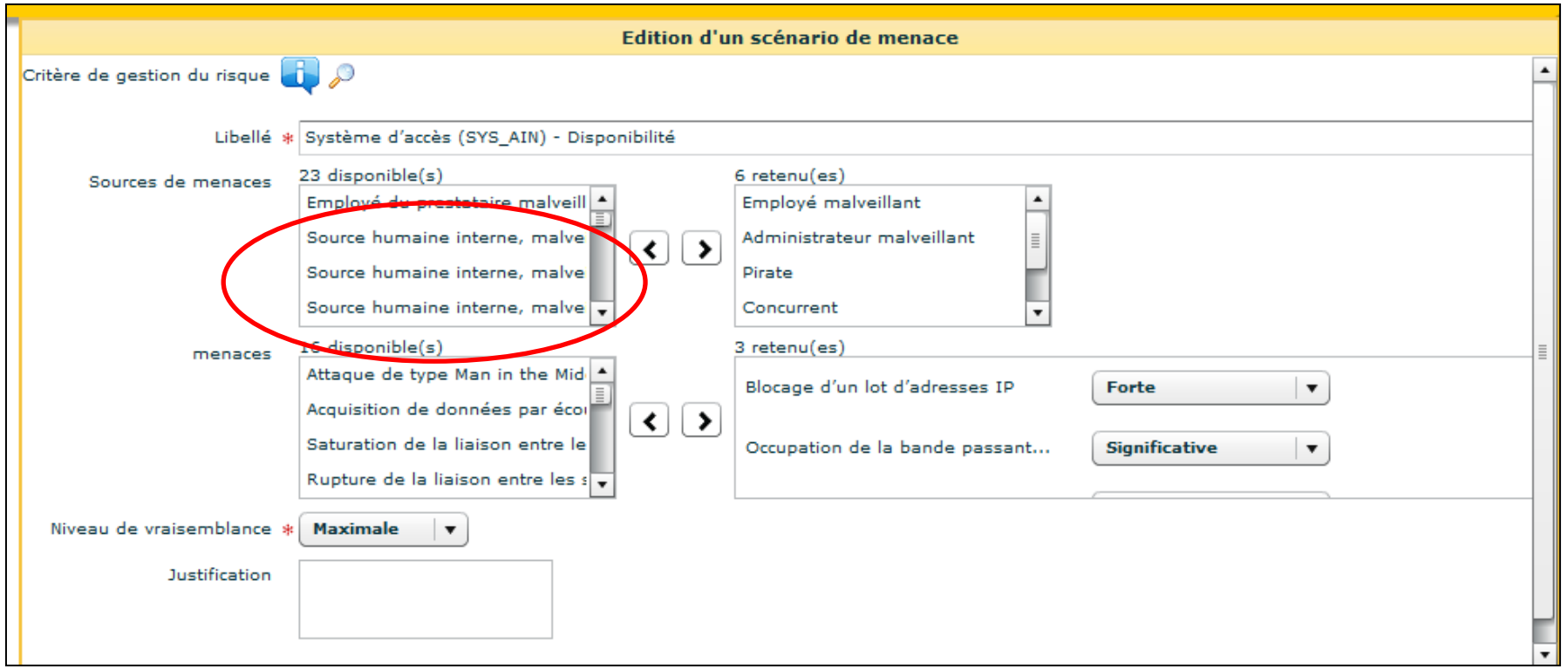


diffusion libre

des zones d'affichage trop petites

pour en lire le contenu

- attente des info-bulles



et plusieurs autres difficultés …

- regroupement hiérarchique des biens supports
- besoin d'utiliser les flèches à la place des ascenseurs
- redimensionnement des colonnes non conservé
- écran figé et curseur d'attente
- …

une interface rapidement contournée

Afin de contourner les difficultés, nous avons alimenté le fichier EBIOS grâce à :

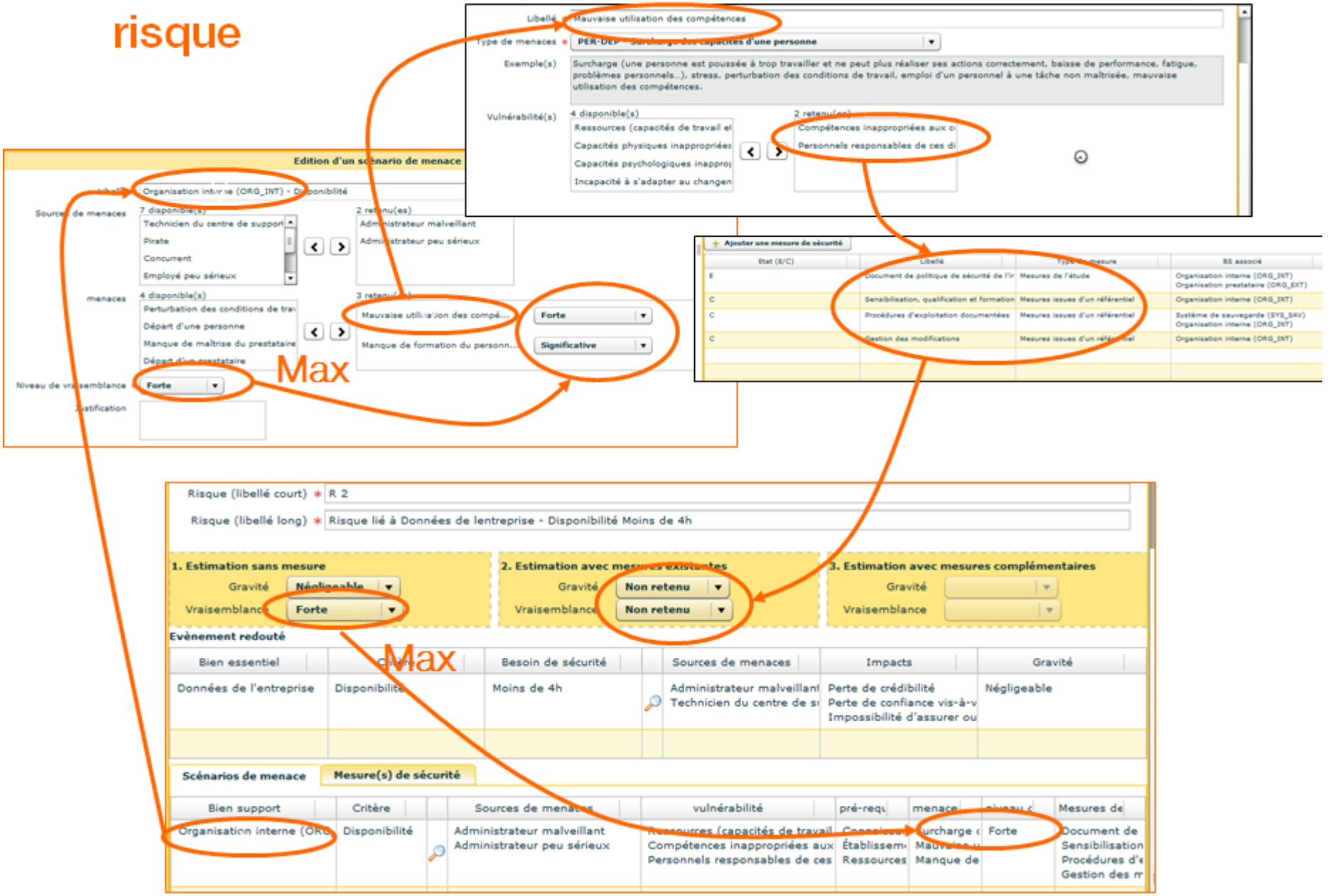
- **Microsoft Access.**

- Le fichier EBIOS est au format SQLlite
- Le fichier EBIOS a été accédé via un ODBC

une présentation des risques

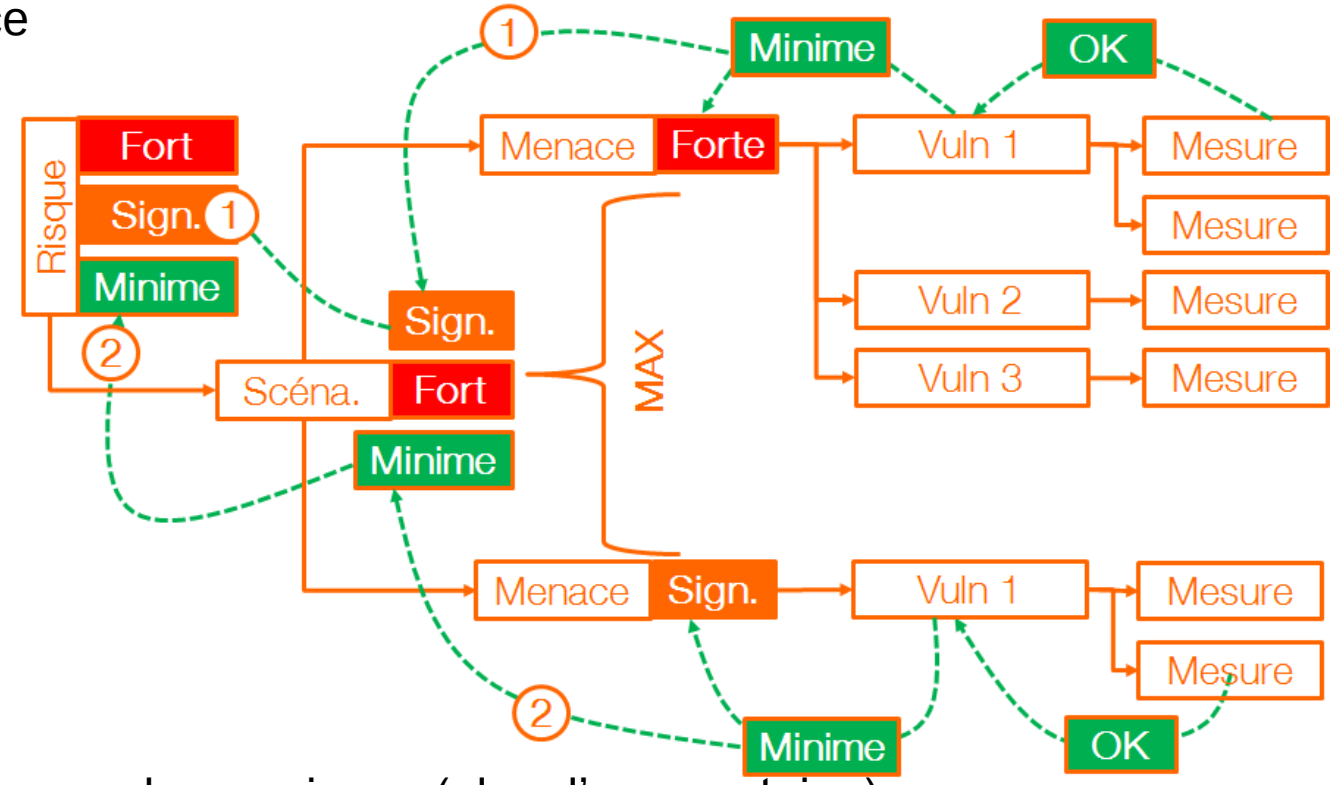
qui rend difficile l'identification
de leur traitement

risque


Libellé * Mauvaise utilisation des compétences
Type de menaces * PER-DEP - Surcharge des capacités d'une personne
Exemple(s) Surcharge (une personne est poussée à trop travailler et ne peut plus réaliser ses actions correctement, baisse de performance, fatigue, problèmes personnels...), stress, perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée, mauvaise utilisation des compétences.
Vulnérabilité(s)
4 disponible(s)
Ressources (capacités de travail et
Capacités physiques inappropriées
Capacités psychologiques inappro
Incapacité à s'adapter au changen
2 retenu(es)
Compétences inappropriées aux c
Personnels responsables de ces di
Edition d'un scénario de menace
Organisation interne (ORG_INT) - Disponibilité
Sources de menaces
7 disponible(s)
Technicien du centre de support
Pirate
Concurrent
Employé peu sérieux
2 retenu(es)
Administrateur malveillant
Administrateur peu sérieux
menaces
4 disponible(s)
Perturbation des conditions de trav
Départ d'une personne
Manque de maîtrise du prestataire
Départ d'un prestataire
3 retenu(es)
Mauvaise utilisation des compé...
Forte
Manque de formation du personn...
Significative
Max
Niveau de vraisemblance
Forte
Justification
Ajouter une mesure de sécurité
Etat (E/C)
Libellé
Type de mesure
BS associé
E
Document de politique de sécurité de l'ir
Mesures de l'étude
Organisation interne (ORG_INT)
Organisation prestataire (ORG_EXT)
C
Sensibilisation, qualification et formation
Mesures issues d'un référentiel
Organisation interne (ORG_INT)
C
Procédures d'exploitation documentées
Mesures issues d'un référentiel
Système de sauvegarde (SYS_SAV)
Organisation interne (ORG_INT)
C
Gestion des modifications
Mesures issues d'un référentiel
Organisation interne (ORG_INT)
Risque (libellé court) * R 2
Risque (libellé long) * Risque lié à Données de lentreprise - Disponibilité Moins de 4h
1. Estimation sans mesure
Gravité
Négligeable
Vraisemblance
Forte
2. Estimation avec mesures existantes
Gravité
Non retenu
Vraisemblance
Non retenu
3. Estimation avec mesures complémentaires
Gravité
Vraisemblance
Max
Evènement redouté
Bien essentiel
Besoin de sécurité
Sources de menaces
Impacts
Gravité
Données de l'entreprise
Disponibilité
Moins de 4h
Administrateur malveillant
Technicien du centre de s
Perte de crédibilité
Perte de confiance vis-à-v
Impossibilité d'assurer ou
Négligeable
Scénarios de menace
Mesure(s) de sécurité
Bien support
Critère
Sources de menaces
vulnérabilité
pré-requ
menace
Mesures de
Organisation interne (ORG
Disponibilité
Administrateur malveillant
Administrateur peu sérieux
Compétences inappropriées aux
Personnels responsables de ces
Établissem
Ressources
Manque de
Forte
Document de
Sensibilisation
Procédures d'
Gestion des m

une opération complexe à renouveler pour :

- chaque menace de manière récursive
- et d'autant plus qu'une même mesure doit être ré-évaluée pour chaque menace



- et ceci pour chaque risque (plus d'une centaine)
- et une fois de plus pour les mesures complémentaires et risques résiduels

un manque de caractérisation du risque présenté

pour choisir le traitement approprié

- absence du libellé du risque
- absence de l'impact du risque

Choisir les options de traitement des risques

Critère de gestion du risque

Risque	Gravité	Vraisemblance	Objectifs de sécurité	Commentaire
R 0	Négligeable	Minime	Prendre	
R 1	Négligeable	Significative	Réduire	
R 2	Négligeable	Forte	Réduire	
R 3	Importante	Minime	Prendre	
R 4	Importante	Minime	Prendre	
R 5	Importante	Significative	Transférer	
R 6	Critique	Forte	Réduire	

une intégrité du traitement contournée

Afin de contourner les difficultés pour assurer l'intégrité et l'exhaustivité des traitements des vulnérabilités, nous avons contrôlé le fichier EBIOS grâce à :

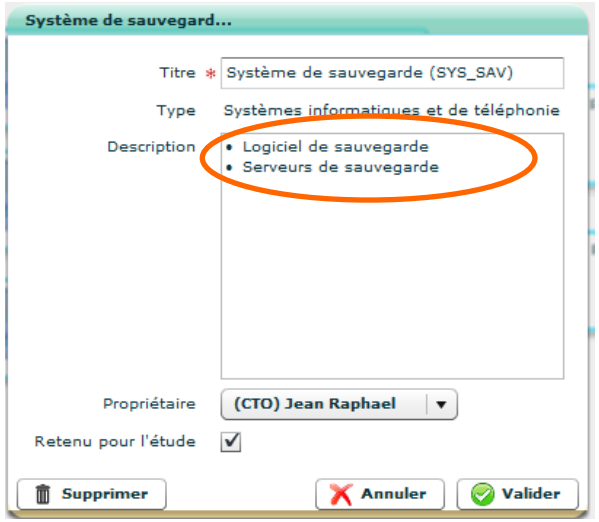
- **Microsoft Access.**

- Le fichier EBIOS est au format SQLlite
- Le fichier EBIOS a été accédé via un ODBC

les exports proposés
ne répondent pas aux attentes (FEROS)

les données saisies dans l'outil ne sont pas toujours exportées

Saisie



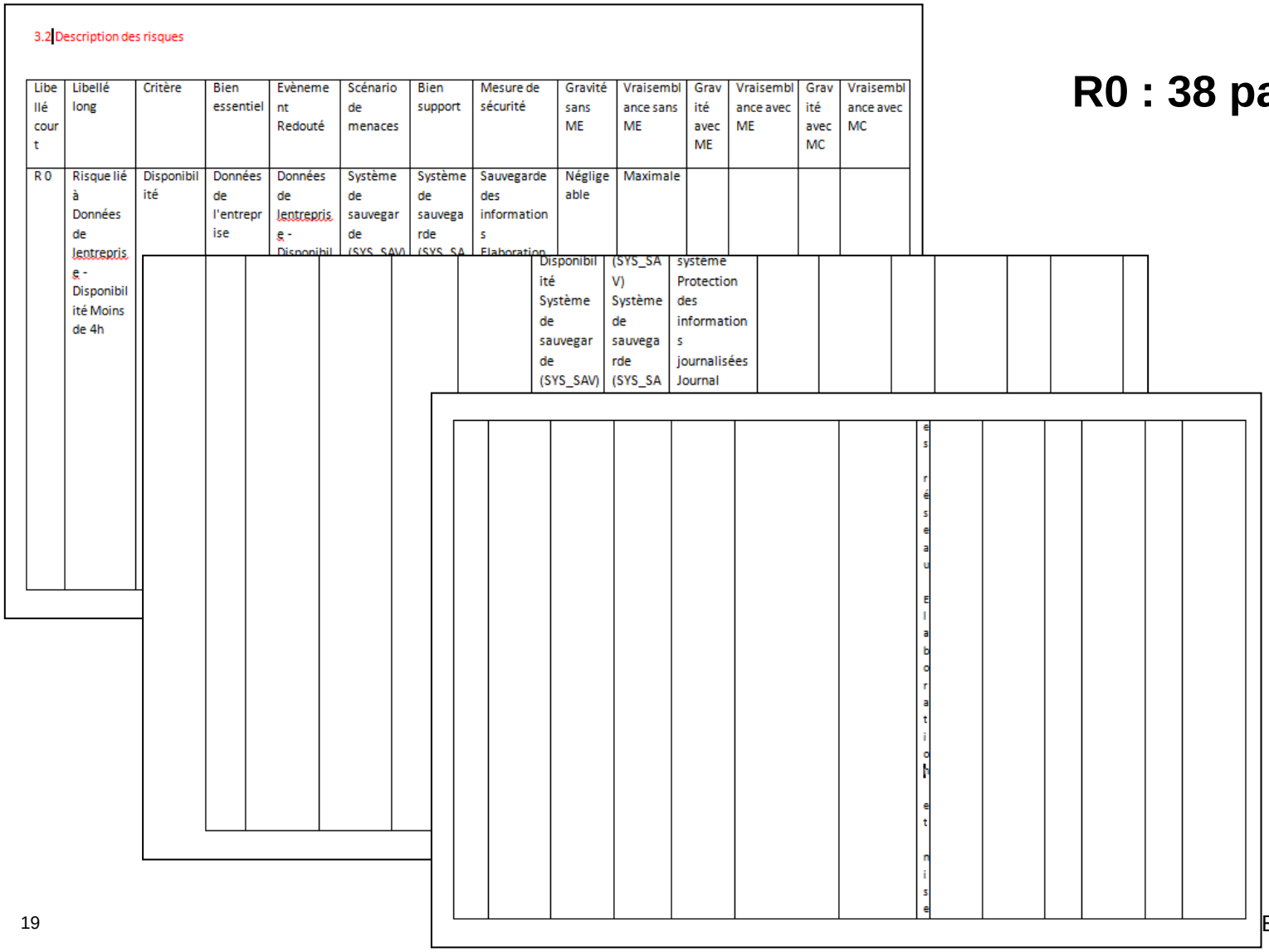
Export WORD

Bien support	Propriétaire
Système de sauvegarde (SYS_SAV)	(CTO) Jean Raphael
Système d'accès (SYS_ACC)	(CTO) Jean Raphael
Système du prestataire (SYS_EXT)	(CTO) Jean Raphael
Organisation interne (ORG_INT)	(CTO) Jean Raphael
Organisation prestataire (ORG_EXT)	(CTO) Jean Raphael

Export EXCEL

Libellé	Propriétaire
Systèmes informatiques et de téléphonie - Système de sauvegarde (SYS_SAV)	(CTO) Jean Raphael
Systèmes informatiques et de téléphonie - Système d'accès (SYS_ACC)	(CTO) Jean Raphael
Systèmes informatiques et de téléphonie - Système du prestataire (SYS_EXT)	(CTO) Jean Raphael
Personnes - Organisation interne (ORG_INT)	(CTO) Jean Raphael
Personnes - Organisation prestataire (ORG_EXT)	(CTO) Jean Raphael

le format des données exportées n'est pas lisible



3.2 Description des risques

Libellé court	Libellé long	Critère	Bien essentiel	Evènement Redouté	Scénario de menaces	Bien support	Mesure de sécurité	Gravité sans ME	Vraisemblance sans ME	Gravité avec ME	Vraisemblance avec ME	Gravité avec MC	Vraisemblance avec MC
R 0	Risque lié à Données de lentreprise - Disponibilité Moins de 4h	Disponibilité	Données de l'entreprise	Données de lentreprise - Disponibil	Système de sauvegarde (SYS_SAV)	Système de sauvegarde (SYS_SA	Sauvegarde des informations Elaboration	Négligeable	Maximale				

Disponibilité Système de sauvegarde (SYS_SAV) | (SYS_SAV) Système de sauvegarde (SYS_SA | système Protection des informations journalisées Journal

réseau Elaboration et

R0 : 38 pages

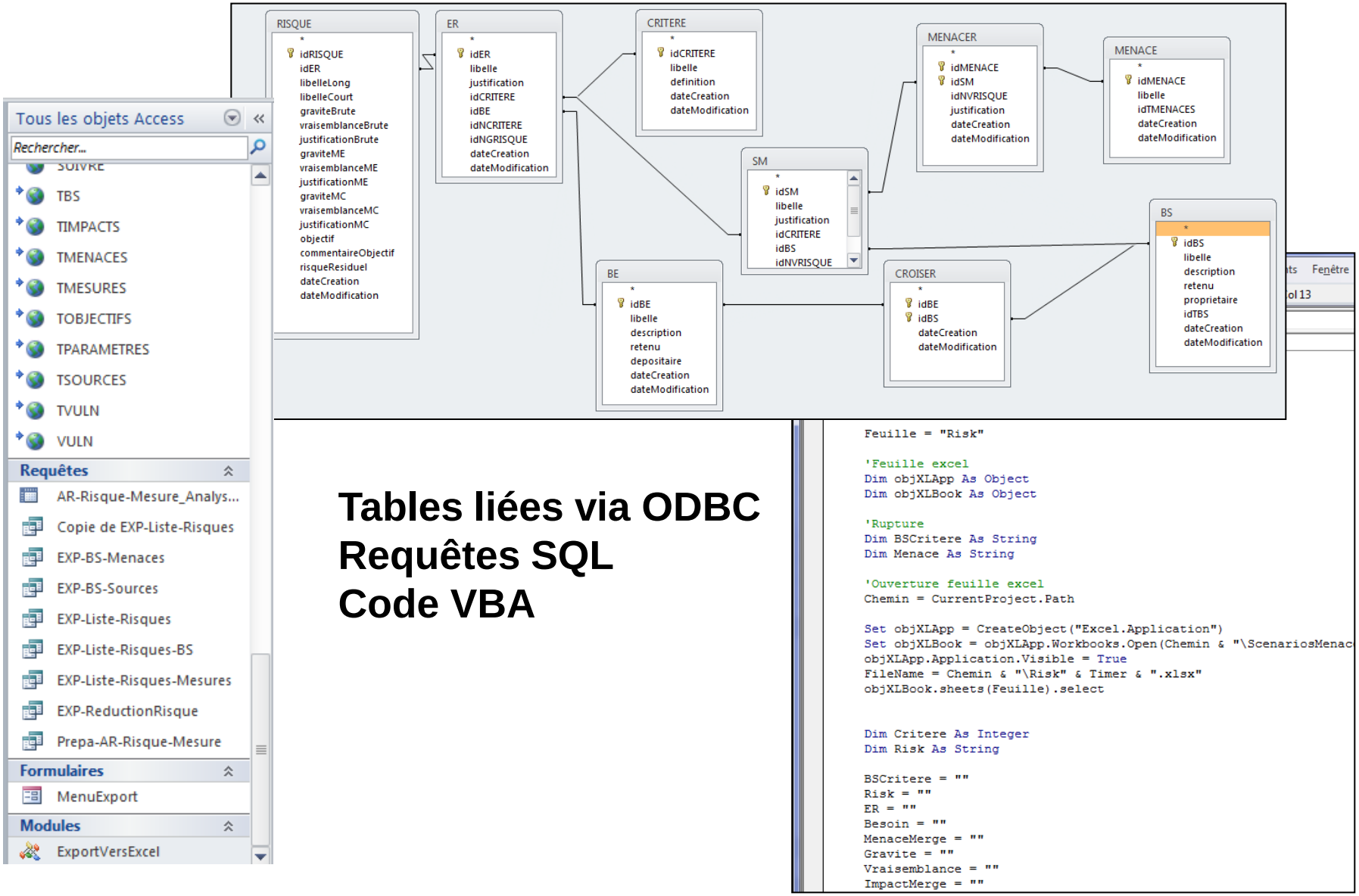
des difficultés d'export contournées

Pour pallier aux difficultés d'export des données, nous avons contrôlé le fichier EBIOS grâce à :

- **Microsoft Access ;**
- **Microsoft Excel.**

- Le fichier EBIOS est au format SQLlite
- Le fichier EBIOS a été accédé via un ODBC

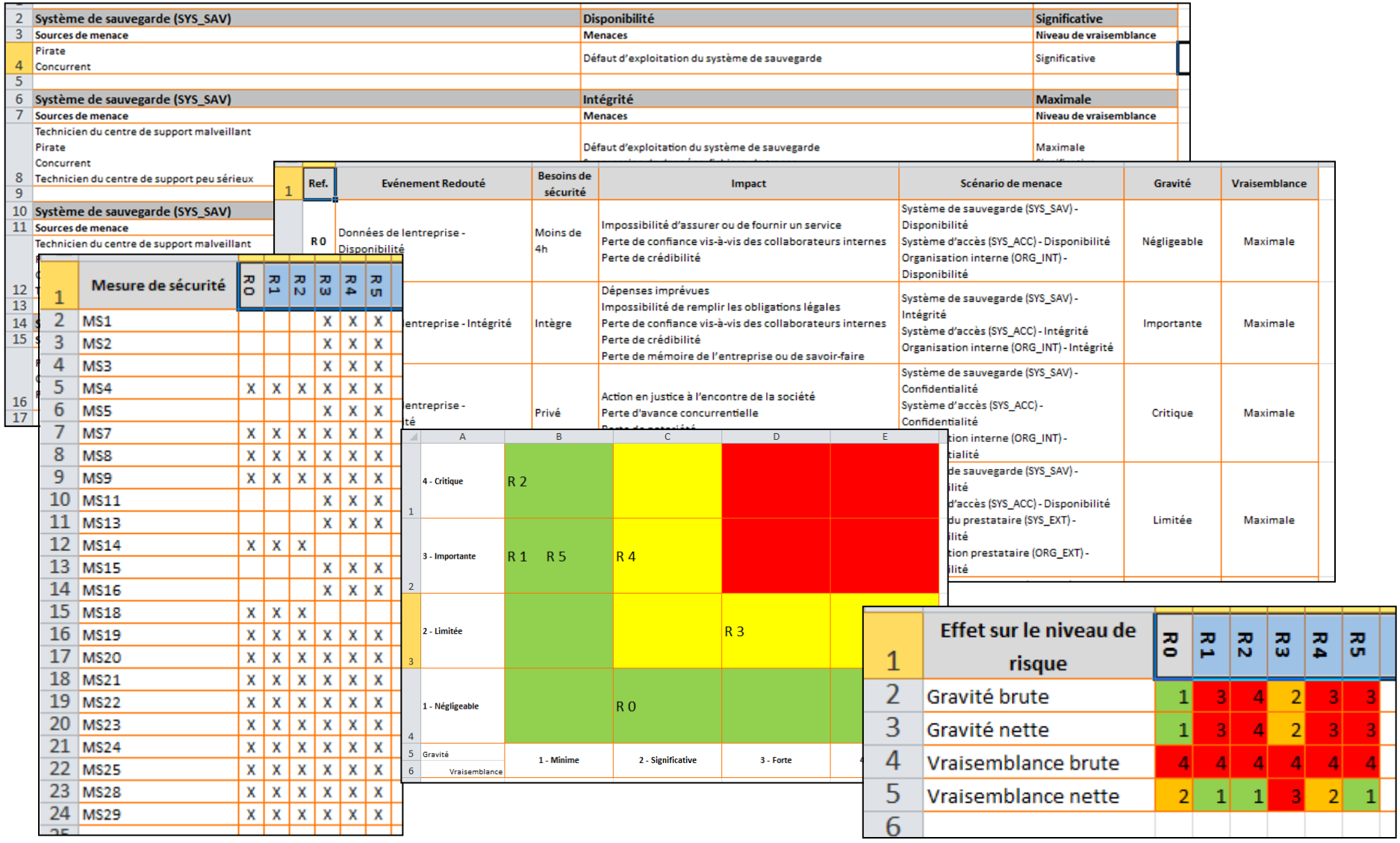
Utilisation de Microsoft Access



Tables liées via ODBC
Requêtes SQL
Code VBA

```
Feuille = "Risk"

'Feuille excel
Dim objXLApp As Object
Dim objXLBook As Object

'Rupture
Dim BSCritere As String
Dim Menace As String

'Ouverture feuille excel
Chemin = CurrentProject.Path

Set objXLApp = CreateObject("Excel.Application")
Set objXLBook = objXLApp.Workbooks.Open(Chemin & "\ScenariosMenac
objXLApp.Application.Visible = True
FileName = Chemin & "\Risk" & Timer & ".xlsx"
objXLBook.sheets(Feuille).select


Dim Critere As Integer
Dim Risk As String

BSCritere = ""
Risk = ""
ER = ""
Besoin = ""
MenaceMerge = ""
Gravite = ""
Vraisemblance = ""
ImpactMerge = ""
```

Utilisation de Microsoft Access



2	Système de sauvegarde (SYS_SAV)	Disponibilité	Significative
3	Sources de menace	Menaces	Niveau de vraisemblance
4	Pirate Concurrent	Défaut d'exploitation du système de sauvegarde	Significative
5			
6	Système de sauvegarde (SYS_SAV)	Intégrité	Maximale
7	Sources de menace	Menaces	Niveau de vraisemblance
8	Technicien du centre de support malveillant Pirate Concurrent Technicien du centre de support peu sérieux	Défaut d'exploitation du système de sauvegarde	Maximale
9			
10	Système de sauvegarde (SYS_SAV)		
11	Sources de menace		
12	Technicien du centre de support malveillant		
13			
14			
15			
16			
17			

1	Ref.	Evénement Redouté	Besoins de sécurité	Impact	Scénario de menace	Gravité	Vraisemblance
	R 0	Données de l'entreprise - Disponibilité	Moins de 4h	Impossibilité d'assurer ou de fournir un service Perte de confiance vis-à-vis des collaborateurs internes Perte de crédibilité	Système de sauvegarde (SYS_SAV) - Disponibilité Système d'accès (SYS_ACC) - Disponibilité Organisation interne (ORG_INT) - Disponibilité	Négligeable	Maximale
		entreprise - Intégrité	Intègre	Dépenses imprévues Impossibilité de remplir les obligations légales Perte de confiance vis-à-vis des collaborateurs internes Perte de crédibilité Perte de mémoire de l'entreprise ou de savoir-faire	Système de sauvegarde (SYS_SAV) - Intégrité Système d'accès (SYS_ACC) - Intégrité Organisation interne (ORG_INT) - Intégrité	Importante	Maximale
		entreprise - té	Privé	Action en justice à l'encontre de la société Perte d'avance concurrentielle	Système de sauvegarde (SYS_SAV) - Confidentialité Système d'accès (SYS_ACC) - Confidentialité tion interne (ORG_INT) - tialité	Critique	Maximale
					de sauvegarde (SYS_SAV) - ilité d'accès (SYS_ACC) - Disponibilité du prestataire (SYS_EXT) - ilité tion prestataire (ORG_EXT) - ilité	Limitée	Maximale

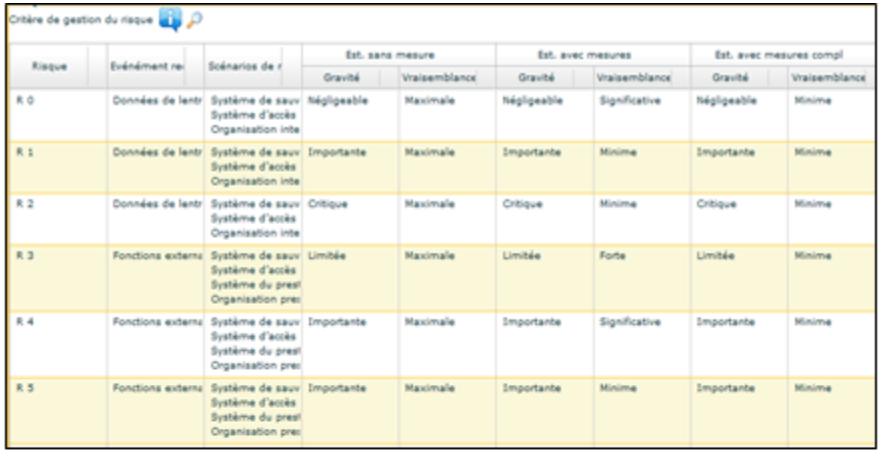
1	Mesure de sécurité	R0	R1	R2	R3	R4	R5
2	MS1				X	X	X
3	MS2				X	X	X
4	MS3				X	X	X
5	MS4	X	X	X	X	X	X
6	MS5				X	X	X
7	MS7	X	X	X	X	X	X
8	MS8	X	X	X	X	X	X
9	MS9	X	X	X	X	X	X
10	MS11				X	X	X
11	MS13				X	X	X
12	MS14	X	X	X			
13	MS15				X	X	X
14	MS16				X	X	X
15	MS18	X	X	X			
16	MS19	X	X	X	X	X	X
17	MS20	X	X	X	X	X	X
18	MS21	X	X	X	X	X	X
19	MS22	X	X	X	X	X	X
20	MS23	X	X	X	X	X	X
21	MS24	X	X	X	X	X	X
22	MS25	X	X	X	X	X	X
23	MS28	X	X	X	X	X	X
24	MS29	X	X	X	X	X	X

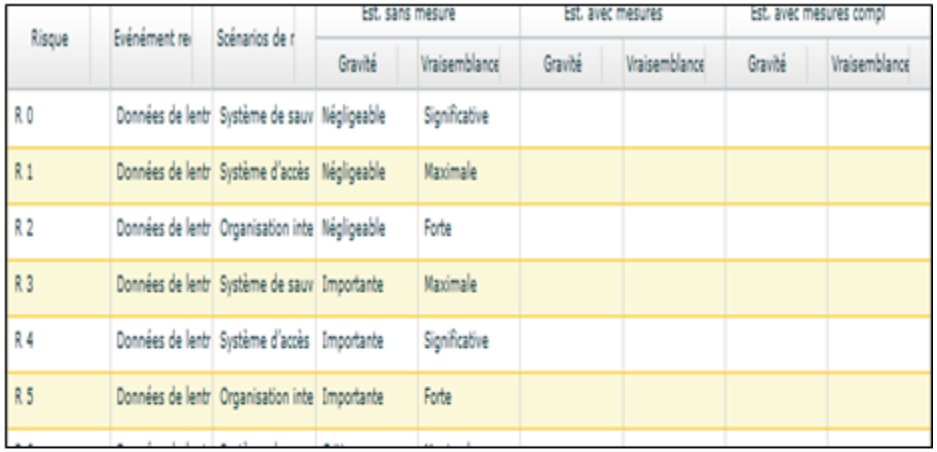
	A	B	C	D	E
1	4 - Critique	R 2			
2	3 - Importante	R 1 R 5	R 4		
3	2 - Limitée			R 3	
4	1 - Négligeable		R 0		
5	Gravité	1 - Minime	2 - Significative	3 - Forte	
6	Vraisemblance				

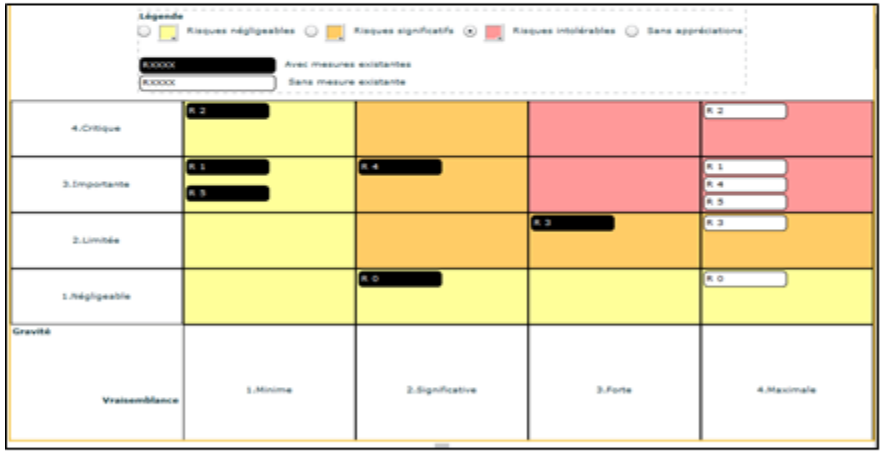
1	Effet sur le niveau de risque	R0	R1	R2	R3	R4	R5
2	Gravité brute	1	3	4	2	3	3
3	Gravité nette	1	3	4	2	3	3
4	Vraisemblance brute	4	4	4	4	4	4
5	Vraisemblance nette	2	1	1	3	2	1
6							

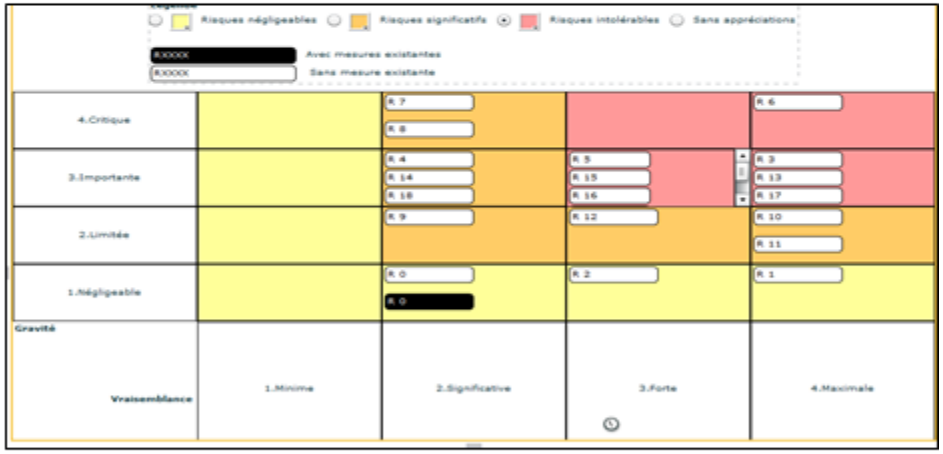
actualisations des
analyses de risques

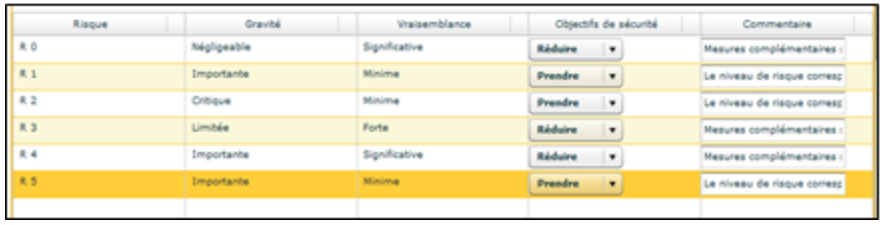
actualisation de risques











Chapitre 4 « Etude des risques »
Chapitre 5 « Etude des mesures de sécurité »
A refaire

diffusion libre

une ré-évaluation des risques inévitable

Pour pallier à ce comportement, nous avons ressaisi les évaluations des mesures de sécurité à partir :

- **de la version précédente imprimée**

notre conclusion

l'utilisation de l'outil EBIOS 2010 en situation réelle

propose :

- une ergonomie déroutante couplée à des dysfonctionnements ;
- un traitement des risques et des mesures fastidieux ;
- des exports non exploitables ;
- une grande difficulté à maintenir une analyse de risques;

pour lesquels il est nécessaire de faire appel à des outils complémentaires :

- Microsoft Access;
  - Reverse engineering sur modèle de données, requêtes SQL, code VBA
- Microsoft Excel.

l'outil EBIOS 2010 dans sa version actuelle

Dans sa version actuelle, l'outil EBIOS 2010 ne répond pas aux attentes :

- **un support simple de la méthodologie EBIOS ;**
- **un gain de temps.**

Nous pensons que les défauts de l'outil peuvent atteindre à l'application de la méthodologie.

des améliorations attendues

Ce retour d'expérience d'utilisation en **situation réelle** de l'outil EBIOS montre que des évolutions sont nécessaires telles que :

- l'ergonomie ;
- les exports des données ;
- la re-génération des risques.

Pour tout complément d'information sur les difficultés rencontrées, vous pouvez nous contacter à :

Alain.Marcay@orange.com

questions ?

merci

Orange Consulting porte l'offre de conseil du Groupe France Télécom vers les entreprises, administrations et collectivités territoriales.