Cardynal
Installation et utilisation d'un site documentaire de SMSI

Date : 04/03/2022 Version : 1.1 Auteur : François KAAG

1 Objet

Ce document explique comment installer, puis utiliser un site permettant la documentation d'un Système de Management de la Sécurité de l'Information (SMSI) à partir du logiciel libre DokuWiki et d'extensions générales ou spécifiques.

2 Installation

L'installation de l'application DokuWiki est détaillée en https://www.dokuwiki.org/install

Les plugins suivants doivent ensuite être installés depuis le menu Administrer/Gestionnaire d'extensions de DokuWiki :

- Scrapbook (https://www.dokuwiki.org/plugin:scrapbook), pour la mise à disposition de modèles de pages. Scrapbook est disponible en installation automatique depuis l'onglet 'Rechercher et installer'
- Strata2 (https://github.com/fkaag71/dokuwiki-strata2). Pour cela, on doit télécharger le package sous la forme d'un ZIP, puis utiliser l'onglet 'Installation manuelle'.
  Strata2 a besoin pour fonctionner du package php-pdo-sqlite, s'il n'est pas installé on aura un message d'erreur '*strata storage failed to open data source'.*
- ISMSAddons (https://github.com/fkaag71/ismsaddons), également en installation manuelle.

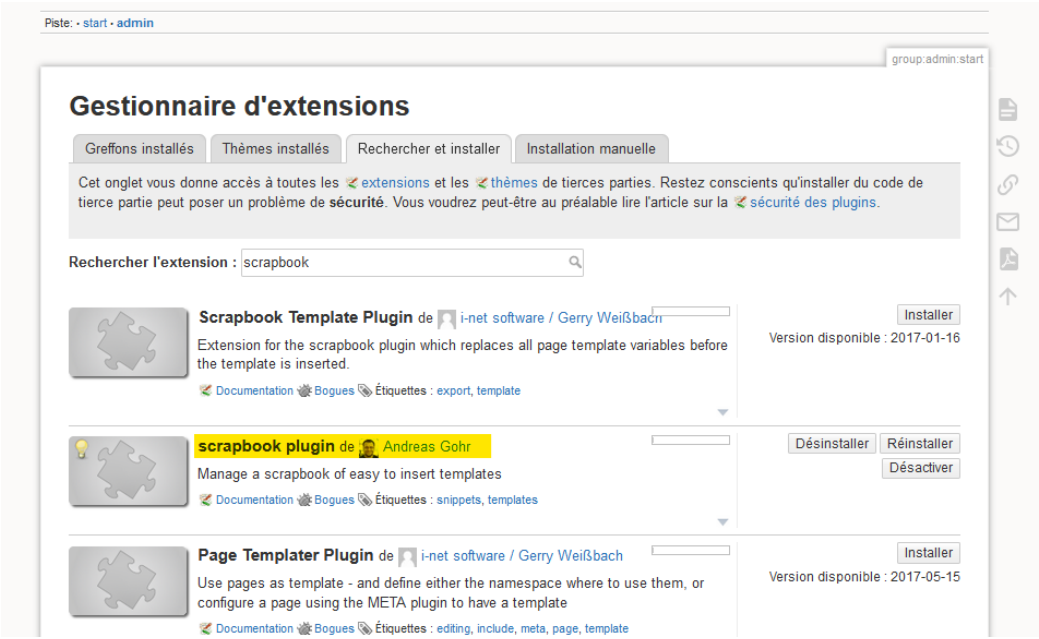


Figure 1-Gestionnaire d'extensions

D'autres plugins de commodité peuvent être chargés selon les besoins, tels que :

- Un plugin spécifique d'authentification, par exemple pour s'adosser à un SSO tiers.
- Move (https://www.dokuwiki.org/plugin:move) pour faciliter le renommage de pages.
- DW2PDF (https://www.dokuwiki.org/plugin:dw2pdf) pour des exports PDF.
- Publish (https://www.dokuwiki.org/plugin:publish) pour permettre de travailler en mode brouillon sur les pages avant de les publier.

3 Utilisation

3.1 Finalité

L'utilisation d'un Wiki pour le site documentaire permet d'y rassembler et de lier entre elles :

- Les politiques et procédures applicables par l'organisation
- L'analyse des risques
- Les enregistrements et preuves à l'appui de l'audit des mesures

Un jeu de pages types est disponible en https://github.com/fkaag71/smsi-example

3.2 Pages spéciales

Les extensions installées supportent l'analyse de risques et la création de tables de synthèse, telles que la déclaration d'applicabilité ou le plan de traitement des risques.

Pour cela, on s'appuie sur la constitution de pages spécifiques comportant des données structurées, des contenus générés à partir des données structurées et du texte libre.

Cinq types de pages sont ainsi définis, différenciés par la classe des données associées.

Classe	Données	Contenu généré	Texte libre
Risk	Label Critère Gravité Scénarios	Détail des scénarios liés	Atteinte Impacts possibles
Scn	Label V0 VC VF Source Vecteur Mode Mesures	Mesures effectives Mesures programmées Autres mesures possibles Risques liés	Description Exemples Justification des vraisemblances
Mes	Label Statut Justification	Scénarios liés Risques traités	Description Preuves
Evt	Label Date Actions	Détail des actions liées	Description
Act	Label Pilote Statut Avancement	Evénement source	Description Définition de l'avancement Critère de clôture Journal

Lors de la création d'une page, il suffit de sélectionner le modèle de page correspondant à l'un des types pour que sa structure soit préremplie. Il suffit alors de compléter les zones de données structurées (délimitées par les balises <data> </data>) et de textes libres.

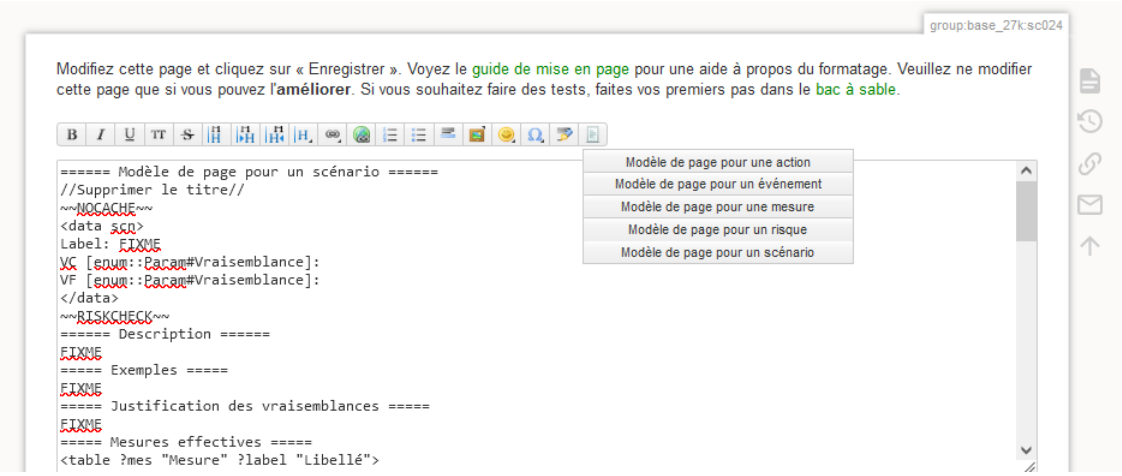


Figure 2-Création d'une page de scénario

Les données structurées peuvent ensuite être utilisées dans des requêtes permettant la génération de diverses tables, tant dans les pages concernées que dans d'autres pages. La syntaxe de ces requêtes est proche de SPARQL et décrite en https://github.com/fkaag71/dokuwiki-strata2/blob/main/manual.txt

Par exemple, la requête suivante permet d'obtenir la liste de toutes les pages de classe scn avec leurs attributs de caractérisation, sous la forme d'une table filtrable.

```
<table ?scn "Code" ?src "Source" ?vect "Vecteur" ?mode ?label>
?scn is a: scn
?scn label: ?label
optional {
?scn source: ?src
?scn vecteur: ?vect
?scn mode: ?mode
}
sort {
 ?scn(asc)
}
ui {
 filter: select
 Label {
   filter:text
 }
}
</table>
```

Ce qui donne le rendu suivant, utilisé pour la liste des scénarios :

Code	Source	Vecteur	Mode	Label
sc001	ANY	ORG	MOD	Attribution de droits applicatifs excessifs à un compte identifié
sc002	EXT-MOD-MLV	MAT_STOR	PTE	Perte ou vol de supports amovibles
sc003	EXT-MOD-MLV	RSX	MOD	Intrusion sur un applicatif depuis un lien externe
sc004	PER-ADMIN-MLD	LOG	MOD	Modification mal maîtrisée en exploitation
sc005	USG-MLD	LOG	USG	Des DSCP sont divulguées, altérées ou détruites intentionnellement par une personne habilitée.
sc006	PER-ADMIN-MLD	ORG	MOD	Maintien d'accès aux DSCP après un départ ou un changement de rôle

Figure 3 - Liste des scénarios

Dans le cas d'un SMSI fondé sur la norme ISO 27001, on créera une page pour chaque mesure énoncée dans l'annexe A, qu'elle soit prise en compte ou pas, afin de générer la Déclaration d'Applicabilité directement à partir du site.

Les captures suivantes présentent des exemples de pages conformes aux modèles fournis.

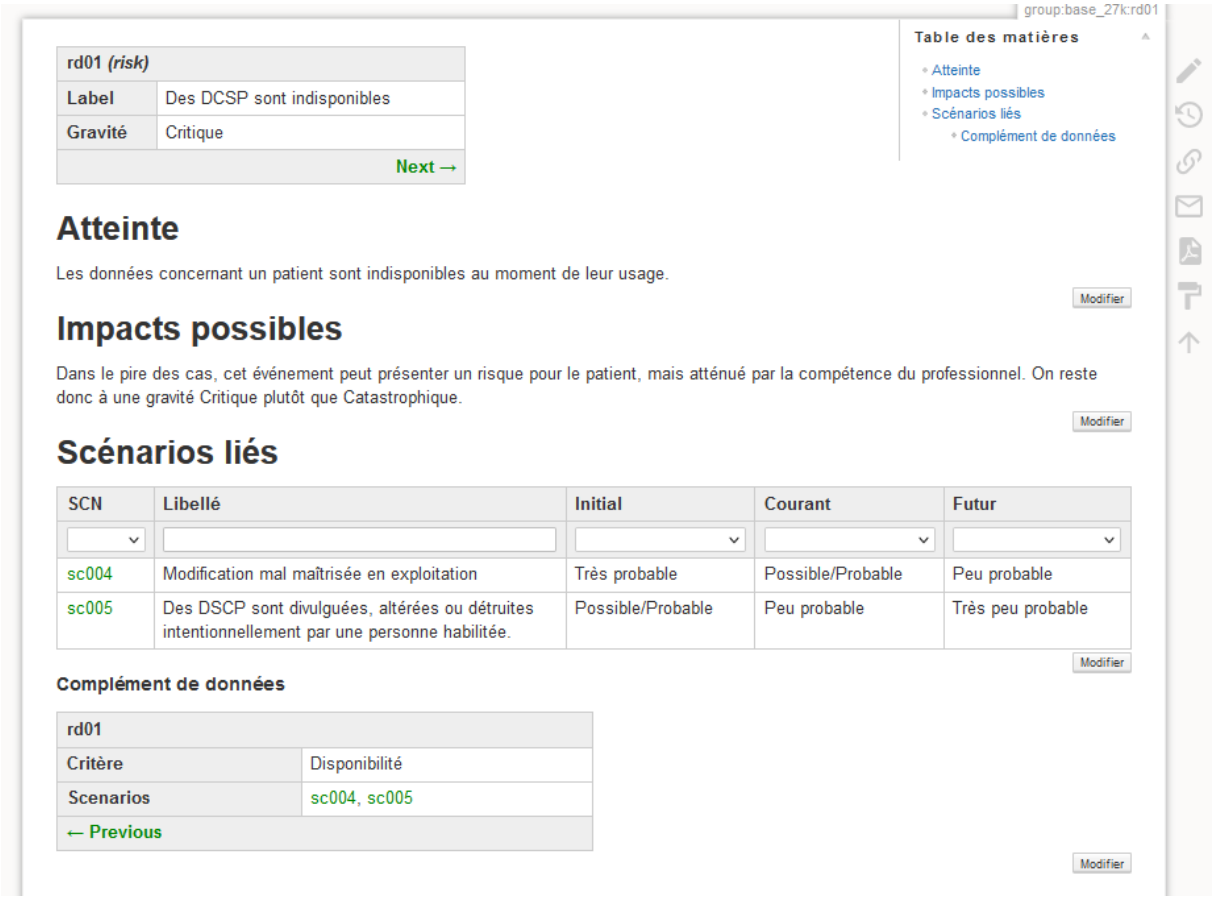
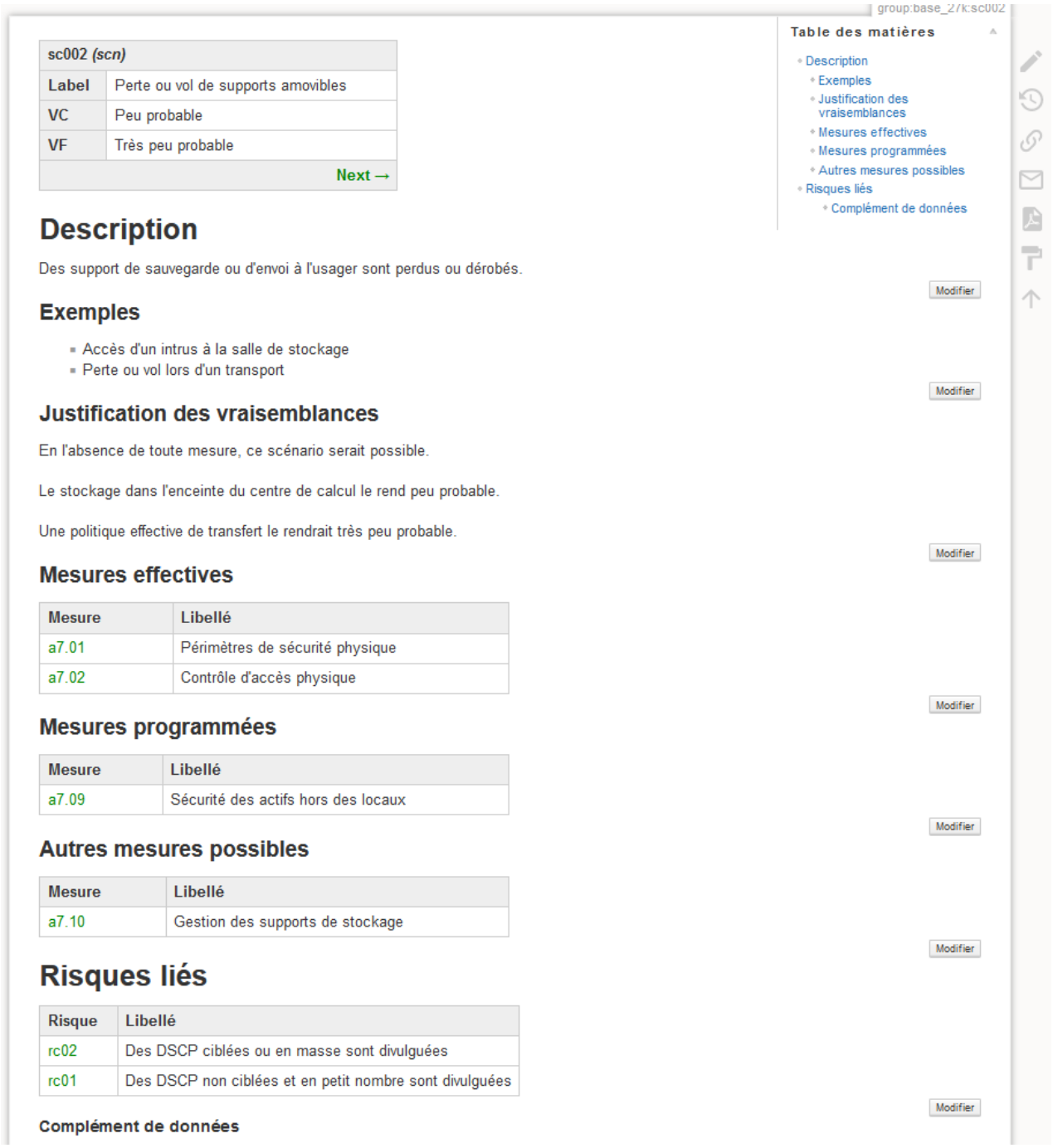


Figure 4 - Page de description d'un risque



sc002 *(scn)*	
Label	Perte ou vol de supports amovibles
VC	Peu probable
VF	Très peu probable

Next →

Table des matières
- Description
  - Exemples
  - Justification des vraisemblances
  - Mesures effectives
  - Mesures programmées
  - Autres mesures possibles
- Risques liés
  - Complément de données

Description

Des support de sauvegarde ou d'envoi à l'usager sont perdus ou dérobés.

Modifier

Exemples

- Accès d'un intrus à la salle de stockage
- Perte ou vol lors d'un transport

Modifier

Justification des vraisemblances

En l'absence de toute mesure, ce scénario serait possible.

Le stockage dans l'enceinte du centre de calcul le rend peu probable.

Une politique effective de transfert le rendrait très peu probable.

Modifier

Mesures effectives

Mesure	Libellé
a7.01	Périmètres de sécurité physique
a7.02	Contrôle d'accès physique

Modifier

Mesures programmées

Mesure	Libellé
a7.09	Sécurité des actifs hors des locaux

Modifier

Autres mesures possibles

Mesure	Libellé
a7.10	Gestion des supports de stockage

Modifier

Risques liés

Risque	Libellé
rc02	Des DSCP ciblées ou en masse sont divulguées
rc01	Des DSCP non ciblées et en petit nombre sont divulguées

Modifier

Complément de données

Figure 5 - Page de description d'un scénario

3.3 Paramétrage

Les données structurées utilisent des types qui doivent être définis dans une page intitulée Param, et comportant des codes ou échelles pour :

- La gravité des risques
- La vraisemblance initiale, courante ou future des scénarios
- Les niveaux de risque (calculés comme le produit d'une gravité et d'une vraisemblance maximale), ainsi que les couleurs associées.
- Les critères de sécurité de l'information

- Les modes, sources ou vecteurs de défaillance des scénarios
- Le statut des mesures. Ce paramètre est utilisé dans les modèles de pages et ne doit pas être modifié, les valeurs possibles sont :
    - E pour Effective
    - P pour Programmée
    - N pour Non prise en compte

Un exemple de page Param est présent dans le jeu de pages types.

3.4 Requêtes de présentation

Par ailleurs, l'extension ISMSAddons ajoute trois requêtes spécifiques qui permettent d'inclure des contenus de contrôle ou de synthèse :

```
~~RISKTABLE~~
```

Affiche une matrice des risques par vraisemblance et gravité, sur laquelle les risques sont portés selon leur niveau actuel (en bleu) ou futur (en vert).

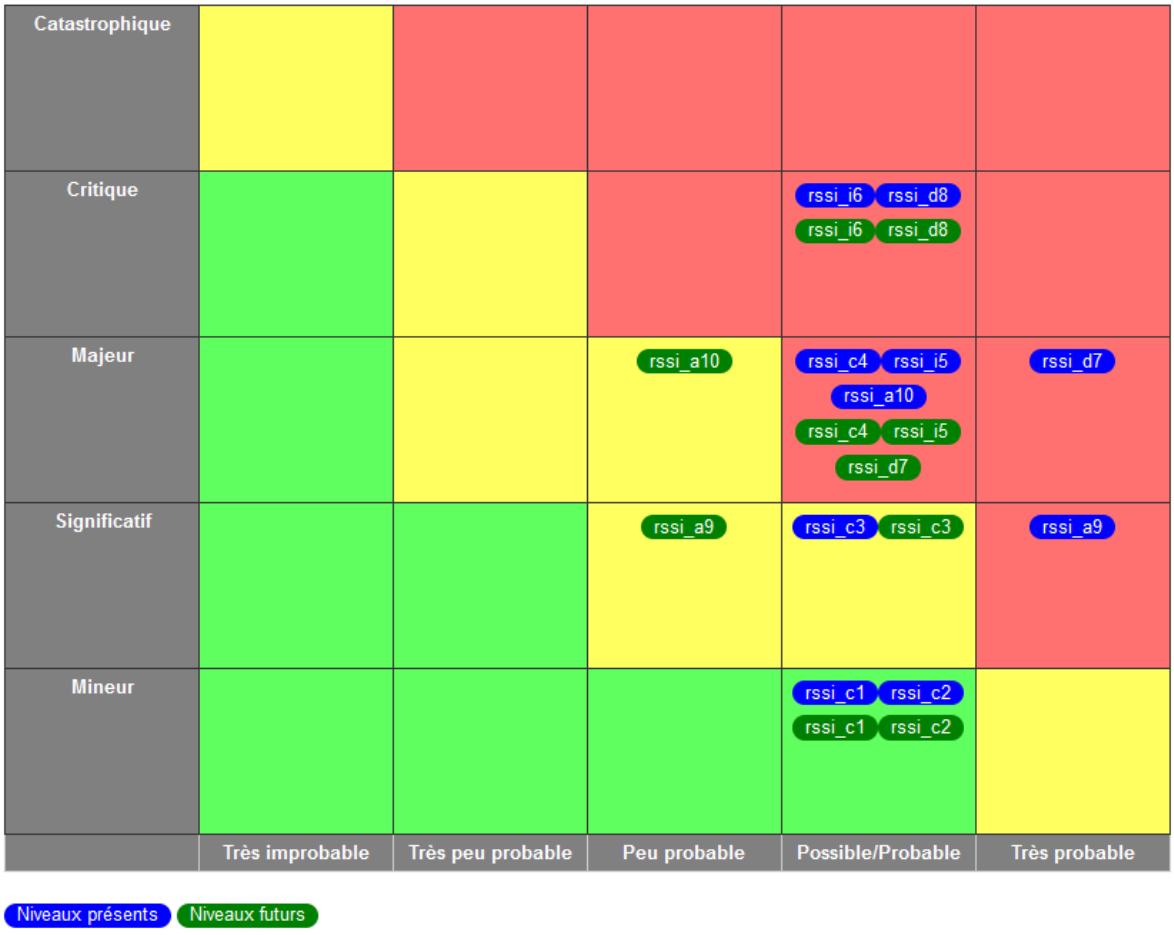


Figure 6 - Matrice des risques

~~RISKINDICATORS~~

Affiche une matrice des niveaux de risque résiduels par critère, pouvant alimenter le relevé des indicateurs de fonctionnement lors des revues.

	Disponibilité	Intégrité	Confidentialité
Nombre de risques	1	1	2
Niveau max courant	12	15	15
Niveau moyen courant	12	15	13.5
Niveau quadratique courant	12	15	13.6
Niveau max futur	8	10	10
Niveau moyen futur	8	10	9
Niveau quadratique futur	8	10	9.1

Figure 7 - Indicateurs de risque résiduel

~~RISKCHECK~~

Placé dans une page de scénario, affiche un bandeau d'alerte en cas d'incohérence entre les vraisemblances et les mesures prises :

- Vraisemblance courante (VC) supérieure à la vraisemblance initiale (V0
- Vraisemblance future (VF) supérieure à la vraisemblance courante (VC)
- VC inférieure à V0 alors qu'aucune mesure possible n'est effective.
- VF inférieure à VC alors qu'aucune mesure possible n'est programmée.

Placé dans une page de risque, affiche la liste des scénarios associés présentant une incohérence.

Dans toute autre page, affiche la liste de tous les scénarios présentant une incohérence.

4 Pages de l'exemple

Les pages fournies en https://github.com/fkaag71/smsi-example comportent :

- Dans l'espace scrapbook, les modèles de pages pour les risques, les scénarios, les mesures, les événements et les action.
- Dans l'espace man, diverses documentations sur l'utilisation de l'outil et la méthode d'analyse des risques.
- Dans l'espace demo
  - Une page de paramétrage de l'analyse des risques
  - Quelques pages de risques et de scénarios
  - Des pages pour toutes les mesures de l'annexe A de l'ISO 27001 (dans sa future organisation après la publication de la version approuvée en décembre de l'ISO 27002).
  - Des pages pour les synthèses calculées : matrice des risques, déclaration d'applicabilité, plan de traitement, listes des risques et des scénarios, indicateurs
  - Des squelettes de pages de cadrage et d'organisation du SMSI
  - Des pages de pointage des exigences 27001 et HDS

Après avoir été recopiées, les pages doivent être attribuées au compte utilisateur sous lequel s’exécute le serveur Web pour être modifiables.

La base de données de strata2 se peuple uniquement lorsque les pages contenant les données sont affichées une première fois, il faut les visiter une par une (par exemple depuis le plan du site) pour les voir apparaitre dans les listes dynamiques et les synthèses.