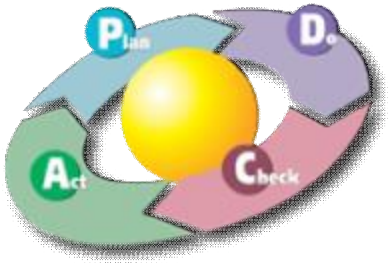


Guide d'utilisation de l'outil d'audit de sécurité

AUDITSec

Version 3.0

Mai 2011

Historique du document			
Version	Date	Auteur	Description
1.0	6 novembre 2010	Éric Clairvoyant http://ca.linkedin.com/pub/eric-clairvoyant/7/ba/227	Création du document
1.5	9 novembre 2010	Éric Clairvoyant http://ca.linkedin.com/pub/eric-clairvoyant/7/ba/227	Ajout explication de la couleur rouge lorsqu'un contrôle est manquant
1.6	mai 2011	Éric Clairvoyant http://ca.linkedin.com/pub/eric-clairvoyant/7/ba/227	Ajout d'un exemple concret à la fin du document

Table des matières

Avis de responsabilité

Cet outil de sécurité a été conçu à l'intention d'une personne soucieuse de la sécurité des Technologies de l'information dans son organisation et est d'envergure limitée.

Les informations contenues dans ce document reflètent une orientation stratégique sur les questions de sécurité abordées à la date de publication. En raison de l'évolution constante des conditions du marché auxquelles on doit s'adapter, elles ne représentent cependant pas un engagement et ne peut garantir l'exactitude de ces informations passé la date de publication.

Ce document est fourni à des fins d'information uniquement.

Objectif de l'outil de sécurité AUDITSec

En utilisant l'outil de sécurité AUDITSec pour chacun des 11 domaines de sécurité d'ISO 27002[1], le management peut mettre en évidence:

- l'état actuel de l'entreprise : où elle se situe aujourd'hui ;
- l'état actuel du marché : la comparaison ;

[1] http://www.27000.org/iso-27002.htm

- l'ambition de l'entreprise : où elle veut se situer ;
- la trajectoire de croissance requise entre les situations en cours et les situations cibles.

L'audit répertorie les points forts, et surtout les points faibles (vulnérabilités) de tout ou partie du domaine visé.

Pour exploiter facilement ces résultats dans les réunions de direction où ils seront présentés comme une aide à la décision pour des plans futurs, l'outil AUDITSec donne des présentations graphiques, ~~une~~ sous la forme d'une rosace, pour chacun des domaines.

Mise en garde

Cet outil ne remplace pas une analyse de risque. Il utilise les 11 domaines et les 133 mesures de contrôle d'ISO 27002.

Mode d'opération

AUDITSec utilise un fichier Excel© ~~avec~~ sans aucune macro, et de simples calculs dans des champs protégés. L'utilisateur entre des valeurs uniquement dans les champs permis.

Le fichier Excel contient 12 onglets représentant les 11 domaines de sécurité d'ISO 27002. Notez que les domaines portent les chiffres de 5 à 15 et que les onglets suivent l'ordre des domaines. Le 1er onglet est une sorte de tableau de bord regroupant les valeurs entrées dans chaque onglet.

Instructions

- Étape 1

Une fois entré dans le fichier, vous êtes invité à entrer ~~ses~~ des valeurs dans la colonne C en réponse au contrôle de chacun des domaines, en commençant à l'onglet DOMAINE 5 (bas de page). Il fait de même pour chaque onglet suivant. Il y ~~en~~ a 11 onglets en tout, représentant chacun des domaines

L'utilisateur doit entrer une valeur de 0 à 5 en se basant sur un des éléments de réponse ci-dessous. Il est à noter que ces valeurs proviennent du *Capability Maturity Model*[2] (*CMM*), en français un modèle de référence de maturité.

> 0 Inexistant : Absence totale de processus identifiables. L'entreprise n'a même pas pris conscience qu'il s'agissait d'un problème à étudier.

[2] http://www.sei.cmu.edu/cmmi/

1 Initial On constate que l'entreprise a pris conscience de l'existence du problème et de la nécessité de l'étudier. Il n'existe toutefois aucun processus standardisé, mais des démarches dans ce sens tendent à être entreprises individuellement ou cas par cas. L'approche globale du management n'est pas organisée.

2 Reproductible: Des processus se sont développés jusqu'au stade où des personnes différentes exécutant la même tâche utilisent des procédures similaires. Il n'y a pas de formation organisée ni de communication des procédures standard et la responsabilité et laissée à l'individu. On se repose beaucoup sur les connaissances individuelles, d'où un risque d'erreurs.

3 Défini : On a standardisé, documenté et communiqué des processus *via* des séances de formation. Ces processus doivent impérativement être suivis ; toutefois, des écarts seront probablement constatés. Concernant les procédures elles-mêmes, elles ne sont pas sophistiquées mais formalisent des pratiques existantes.

4 Géré : La direction contrôle et mesure la conformité aux procédures et agit lorsque certains processus semblent ne pas fonctionner correctement. Les processus sont en constante amélioration et correspondent à une bonne pratique. L'automatisation et les outils sont utilisés d'une manière limitée ou partielle.

5 Optimal : Les processus ont atteint le niveau des bonnes pratiques, suite à une amélioration constante et à la comparaison avec d'autres entreprises (Modèles de Maturité). L'informatique est utilisée comme moyen intégré d'automatiser le flux des tâches, offrant des outils qui permettent d'améliorer la qualité et l'efficacité et de rendre l'entreprise rapidement adaptable.

Afin, d'aider l'utilisateur, il y a une définition détaillée pour chaque mesure qui permettra d'avoir plus de détails afin de donner la meilleure réponse possible.

Les bonnes pratiques laissent croire qu'une valeur globale pour chacun des 11 domaines située entre 2 et 4 est acceptable

Important

Note (a) : Si le contrôle d'un domaine n'est pas pertinent dans votre contexte, le champ doit être vide, c'est-à-dire, il faut utiliser la touche Suppr ou Del du clavier. De cette façon, le contrôle ne sera pas comptabilisé dans le calcul final.

Note (b) : Dans le tableau de bord, le domaine sera en couleur rouge inversée indiquant que ce domaine n'a pas de contrôle applicable. Par exemple, le domaine 6 à un total de neuf (9) contrôles applicables. On peut y voir que deux (2) contrôles sont inapplicables.

Contrôles Applicables	Non applic.	ISO 27002 11 domaines, 39 objectifs, 133 contrôles
2	0	5.Politique de sécurité
9	2	6.Organisation de la sécurité

Au fur et à mesure que les valeurs sont entrées, une rosace se crée, donnant une photographie de l 'état actuel du point de vue de la sécurité pour le domaine visé. En parallèle, une rosace se met à jour dans l'onglet principal (Domaine 1 (Global)) qui représente le tableau de bord de tous les domaines.

- Étape 2

Une fois tous les onglets complétés, vous devez aller à l'onglet principal.

Tableau de bord – Domaine 1 Global

Quelques définitions :

A	B	C	D	F	G	H	I	J
Contrôles Applicables	Non applic.	ISO 27002 11 domaines, 39 objectifs, 133 contrôles	Cote	%	Notes ciblées	%	Cote ISO 27002	Note ciblée ISO 27002

La colonne A indique le nombre de contrôles applicables pour chaque domaine visé en lien avec ISO 27002.

La colonne B indique le nombre de contrôles qui ne s'appliquent pas dans un domaine en particulier. (Représente la valeur vide Suppr ou Del).

La colonne C ~~nomme~~ indique les titres pour les 11 domaines de sécurité selon la norme ISO 27002.

La colonne D donne la valeur globale pour ~~ce~~ chaque domaine. Ce calcul se fait automatiquement selon les valeurs entrées de 0 à 5. Si jamais le symbole suivant apparaît : #DIV/0, cela signifie que le calcul ne peut se faire parce qu'il n'y a aucun contrôle sélectionné, donc aucune valeur 0 à 5 dans le domaine applicable. En conséquence, ce code d'erreur est tout à fait pertinent.

La colonne F représente le pourcentage de conformité par rapport à l'ISO 27002.

Dans la colonne G, l'utilisateur est invité à entrer quelle cote désire comme objectif pour une certaine période. Cette note doit être un chiffre entier entre 1 et 5.

Exemple : Si la colonne D possède une valeur de 2 alors à la colonne G la valeur maximale suggérée serait de 3 et non supérieure à 3. Il faut en effet être réaliste car plus la valeur dans la colonne G est élevée, plus les coûts d'implantations des mesures de sécurité seront élevés par la même occasion.

La colonne H convertit en pourcentage la valeur entrée dans la colonne G et indique en % la valeur que désire obtenir l'organisation pour une période.

La colonne I donne le pourcentage de l'état actuel de la sécurité en conformité avec ISO 27002.

La colonne J donne le pourcentage cible visé pour la période.

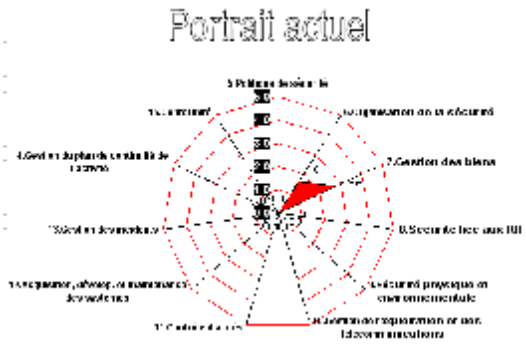
Les rosaces

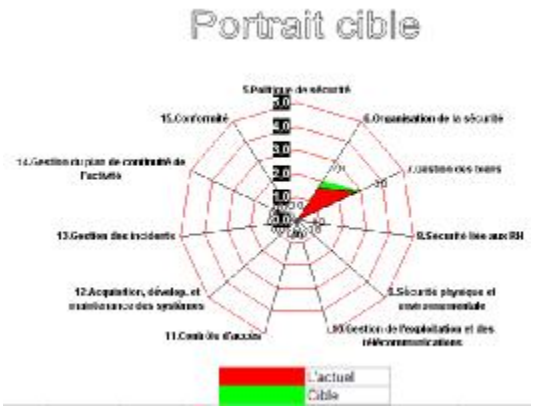
Les rosaces permettront de données des courbes pour chaque domaine visé.

Portrait actuel : indique l'état de la sécurité au moment de la compilation des données.

Portrait cible : indique en rouge l'état actuel de la sécurité plus, en vert la cible que désire atteindre l'organisation.

11	0	6.Organisation de la sécurité	1,6	32,73%	2,0	40,00%
5	0	7.Gestion des biens	2,8	56,00%	3,0	60,00%





Exemple – scénario

Voici un exemple type de l'utilisation d'AUDITSec.

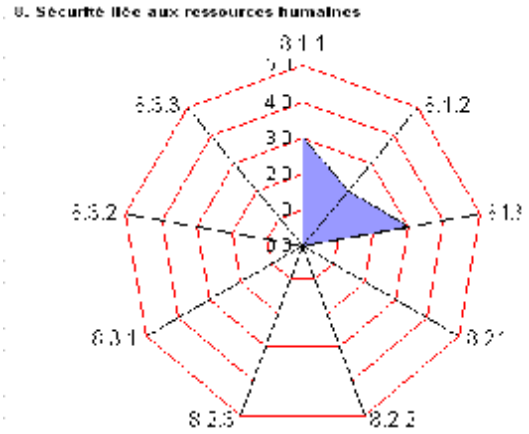
Étape 1

- Vous choisissez le domaine pour votre audit. On choisit pour cet exemple le domaine 8 (Sécurité liée aux ressources humaines), onglet no 8.
- Pour le contrôle 8.1.1 - Rôles et responsabilités, la validation ou mesure est la suivante :
  Définir et de documenter les rôles et responsabilités en matière de sécurité des salariés, contractants et utilisateurs tiers, conformément à la politique de sécurité de l'information de l'organisme. (source : ISO 27002)
  Est-ce que la valeur pour la colonne C est 0, 1, 2, 3, 4 ou 5? Pour cet exemple nous allons insérer la valeur 3 (Processus défini).
- Pour le contrôle 8.1.2- Sélection, la validation est la suivante:
  On insère la valeur de 2 (Reproductible mais intuitif)
- Pour le contrôle 8.1.3-Conditions d'embauche, la validation est la suivante :
  On insère la valeur de 3 (Processus défini).
- Vous procédez, ainsi de suite pour chaque contrôle subséquent.

Voyez ci-dessous le résultat.

B	C	D	E	F	G	H
Contrôle	**Cote**	**Contrôle**				
8.1.1	3,0	8.1.1 Rôles et responsabilités				
8.1.2	2,0	8.1.2 Sélection				
8.1.3	3,0	8.1.3 Conditions d'embauche				
8.2.1	0,0	8.2.1 Responsabilités de la direction				
8.2.2	0,0	8.2.2 Sensibilisation, qualification et formations en matière de sécurité de l'information				
8.2.3	0,0	8.2.3 Processus disciplinaire				
8.3.1	0,0	8.3.1 Responsabilités en fin de contrat				
8.3.2	0,0	8.3.2 Restitution des biens				
8.3.3	0,0	8.3.3 Retrait des droits d'accès				
9	0,9					

Dans cet exemple la cote finale pour le domaine 8 est 0,9. ~~Il y a~~ Une rosace apparaît pour chaque domaine.



Étape 2

Une fois que vous avez entré toutes les valeurs pour chaque contrôle, de chaque domaine, le tableau de bord (onglet domaine 1 global) se met à jour. Le voici :

A	B	C	D	F	G	H	I	J
Contrôles Applicables	Non applic.	**ISO 27002 11 domaines, 39 objectifs, 133 contrôles**	**Cote**	**%**	**Notes ciblées**	**%**	**Cote ISO 27002**	**Note ciblée ISO 27002**
2	0	5.Politique de sécurité	0,0	0,00%	0,0	0,00%		
11	0	6.Organisation de la sécurité	0,0	0,00%	0,0	0,00%		
5	0	7.Gestion des biens	0,0	0,00%	0,0	0,00%		
9	0	8.Sécurité liée aux RH	0,9	17,78%	0,0	0,00%		
13	0	9.Sécurité physique et environnementale	0,0	0,00%	0,0	0,00%		
32	0	10.Gestion de l'exploitation et des télécommunications	0,0	0,00%	0,0	0,00%		
25	0	11.Contrôle d'accès	0,0	0,00%	0,0	0,00%		
16	0	12.Acquisition, dévelop. et maintenance des systèmes	0,0	0,00%	0,0	0,00%		
5	0	13.Gestion des incidents	0,0	0,00%	0,0	0,00%		
5	0	14.Gestion du plan de continuité de l'activité	0,0	0,00%	0,0	0,00%		
10	0	15.Conformité	0,0	0,00%	0,0	0,00%		
133	**0**						**1,62%**	**0,00%**

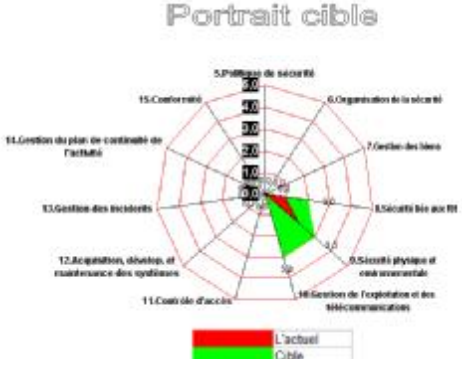
Comme on peut le constater à la colonne D, la valeur globale 0,9 ~~y~~ est représentée ainsi que le pourcentage 17,78. Dans cet exemple, pour ce domaine, la cote de conformité à ISO 27002 est de 1,62 %.

L'utilisateur doit maintenant inscrire à la colonne G, la note ciblée ~~qui~~ qu'il désire atteindre pour une période.

Dans notre exemple, la valeur 2 est note cible.

A	B	C	D	F	G	H	I	J
Contrôles Applicables	Non applic.	**ISO 27002 11 domaines, 39 objectifs, 133 contrôles**	**Cote**	**%**	**Notes ciblées**	**%**	**Cote ISO 27002**	**Note ciblée ISO 27002**
2	0	5.Politique de sécurité	0,0	0,00%	0,0	0,00%		
11	0	6.Organisation de la sécurité	0,0	0,00%	0,0	0,00%		
5	0	7.Gestion des biens	0,0	0,00%	0,0	0,00%		
9	0	8.Sécurité liée aux RH	0,9	17,78%	2,0	40,00%		
13	0	9.Sécurité physique et environnementale	0,0	0,00%	0,0	0,00%		
32	0	10.Gestion de l'exploitation et des télécommunications	0,0	0,00%	0,0	0,00%		
25	0	11.Contrôle d'accès	0,0	0,00%	0,0	0,00%		
16	0	12.Acquisition, dévelop. et maintenance des systèmes	0,0	0,00%	0,0	0,00%		
5	0	13.Gestion des incidents	0,0	0,00%	0,0	0,00%		
5	0	14.Gestion du plan de continuité de l'activité	0,0	0,00%	0,0	0,00%		
10	0	15.Conformité	0,0	0,00%	0,0	0,00%		
133	**0**						**1,62%**	**3,64%**

Cette cible à atteindre permettra d'atteindre une note ciblée ISO 27002 à 3,64%.
Et les rosaces ci-dessous traduisent automatiquement les deux situations (portraits).



Versi