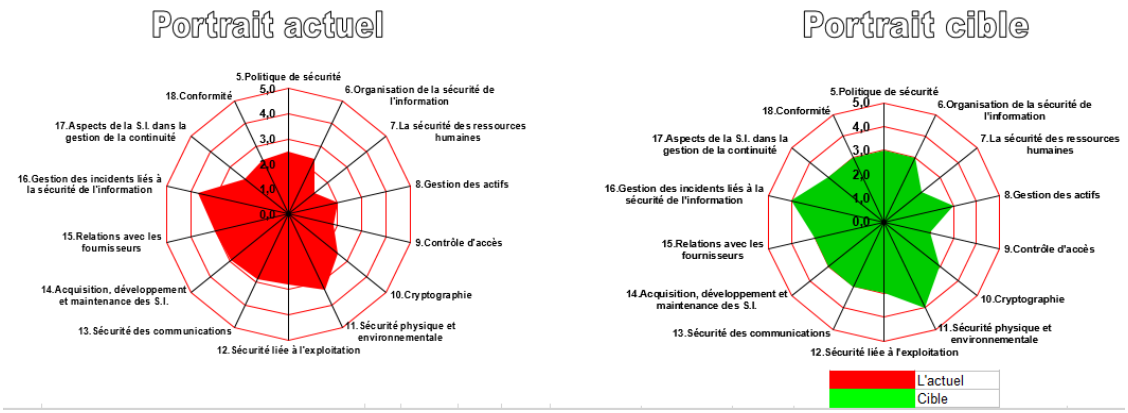
Guide d'utilisation de l'outil d'audit de sécurité

AUDITSec



Mai 2014

TABLE DES MATIÈRES

AVIS DE RESPONSABILITÉ

AUDITSec est un outil d'audit de sécurité conçu à l'intention des professionnels soucieux de la sécurité des technologies de l'information dans leur organisation. Cet outil vous sera fort utile pour réaliser vos exercices et vos travaux dans le cadre de ce cours, et vous voudrez sans doute aussi l'utiliser dans vos activités professionnelles. Vous devez toutefois savoir qu'il est d'une envergure limitée.

En effet, les informations contenues dans ce document reflètent une **orientation stratégique** quant aux 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 donc pas un engagement et nous ne pouvons garantir leur exactitude après la date de publication.

Ce document est fourni uniquement à des fins d'information et d'apprentissage. Faites-en un bon usage!

Mise en garde
Cet outil peut être utilisé comme outil d'aide à la décision, mais il ne remplace pas une analyse de risque. Il utilise simplement les 14 articles ou domaines de la sécurité, les 35 catégories de sécurité et les 114 mesures de la norme ISO 27002 :2013 pour répertorier les points forts et les points faibles de tout ou d'une partie du domaine visé.

OBJECTIF DE L'OUTIL D'AUDIT DE SÉCURITÉ AUDITSEC

L'outil d'audit de sécurité AUDITSec couvre 14 domaines de sécurité, appelés articles, tirés de la norme ISO 270022013[1] :

5. Politique de sécurité
6. Organisation de la sécurité de l'information
7. La sécurité des ressources humaines
8. La gestion des actifs
9. Le contrôle d'accès
10. La cryptographie
11. La sécurité physique et environnementale
12. La sécurité liée à l'exploitation
13. La sécurité des communications
14. L'acquisition, le développement et la maintenance des systèmes d'information
15. Les relations avec les fournisseurs
16. La gestion des incidents de sécurité de l'information
17. Les aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
18. La conformité

1. Voir *Norme internationale ISO/CEI 27002*, numéro de référence ISO/CEI 27002:2013, document PDF accessible à partir menu « Outils méthodologiques », en bas à gauche du site du cours.

Cet outil permet de mettre en évidence :

- la situation actuelle de l'entreprise : où elle se situe aujourd'hui;
- la situation actuelle du marché : pour établir une comparaison;
- l'objectif ou la cible de l'entreprise : où elle veut se situer;
- la trajectoire de croissance requise entre la situation actuelle et la situation ciblée.

L'outil d'audit répertorie les points forts, et surtout les points faibles (vulnérabilités), de tout ou d'une 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 fournit des présentations graphiques, sous la forme de rosaces, pour chacun des 14 articles ou domaines de la sécurité.

PRÉSENTATION DE L'OUTIL

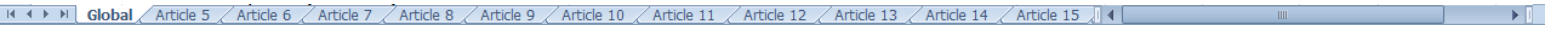
Cette section donne un aperçu général du contenu de l'outil AUDITSec, des façons de s'y déplacer et de ses principales fonctionnalités.

AUDITSec utilise un fichier Excel sans aucune macro et de simples calculs dans des champs protégés. Vous pouvez saisir des valeurs uniquement dans les champs permis.

Vue initiale à l'ouverture du fichier

Les 15 onglets

Le fichier Excel contient 15 onglets (accessibles au bas de l'écran) :



- Le premier onglet, « Global », est une sorte de tableau de bord qui regroupe les valeurs saisies dans chacun des onglets qui suivent. Il vous présente un portrait global de la situation (portrait actuel et portrait cible), une fois les valeurs entrées dans les onglets suivants.
- Les 14 onglets suivants, « Article 5 » à « Article 18 », représentent les 14 articles de la sécurité de la norme ISO 27002 :2013. Ces articles étant numérotés de 5 à 18 dans la norme, les onglets de l'outil respectent l'ordre et la numérotation des articles de la norme.

Astuce!
Nous vous suggérons d'ouvrir le fichier Excel de l'outil AUDITSec dès maintenant et de l'utiliser pour suivre la présentation de l'outil et les instructions au fur et à mesure de votre lecture.

Vous trouverez l'outil AUDITSec dans le menu « Outils méthodologiques », situé à gauche de l'écran principal. Téléchargez-le sur votre poste de travail et enregistrez-le sous un nouveau nom, en ajoutant par exemple « test » à la fin du nom du fichier. Cela vous permettra de conserver l'outil dans sa version originale et de l'utiliser pour réaliser les exercices de ce cours ou dans le cadre de vos activités professionnelles.

L'onglet « Global »

À l'ouverture du fichier, vous vous trouvez par défaut dans le premier onglet qui joue le rôle de tableau de bord de l'outil. Le contenu de chacune des colonnes est présenté plus loin, dans les instructions. Pour le moment, notez seulement les principaux éléments de cet onglet.

Les 14 articles

En vert, dans la colonne C, voyez les 14 articles ou domaines de la sécurité de la norme ISO 27002 :2013 :

C
ISO 27002:2013
14 articles, 35 catégories de sécurité, 114 mesures
5.Politique de sécurité
6.Organisation de la sécurité de l'information
7.La sécurité des ressources humaines
8.Gestion des actifs
9.Contrôle d'accès
10.Cryptographie
11.Sécurité physique et environnementale
12.Sécurité liée à l'exploitation
13.Sécurité des communications
14.Acquisition, développement et maintenance des S.I.
15.Relations avec les fournisseurs
16.Gestion des incidents liés à la sécurité de l'information
17.Aspects de la S.I. dans la gestion de la continuité
18.Conformité

Les 35 catégories de sécurité

Chaque article contient une ou plusieurs catégories de sécurité.

Articles	Nombre de catégories de sécurité
5. Politique de sécurité	1
6. Organisation de la sécurité de l'information	2
7. La sécurité des ressources humaines	3
8. Gestion des actifs	3
9. Contrôle d'accès	4
10. Cryptographie	1
11. Sécurité physique et environnementale	2

12. Sécurité liée à l'exploitation	7
13. Sécurité des communications	2
14. Acquisition, développement et maintenance des S.I.	3
15. Relations avec les fournisseurs	2
16. Gestion des incidents liés à la sécurité de l'information	1
17. Aspects de la S.I. dans la gestion de la continuité	2
18. Conformité	2
TOTAL :	35

Les informations relatives à chaque catégorie de sécurité sont données dans l'onglet de l'article concerné. Elles sont présentées plus loin dans ce document.

Les 114 mesures

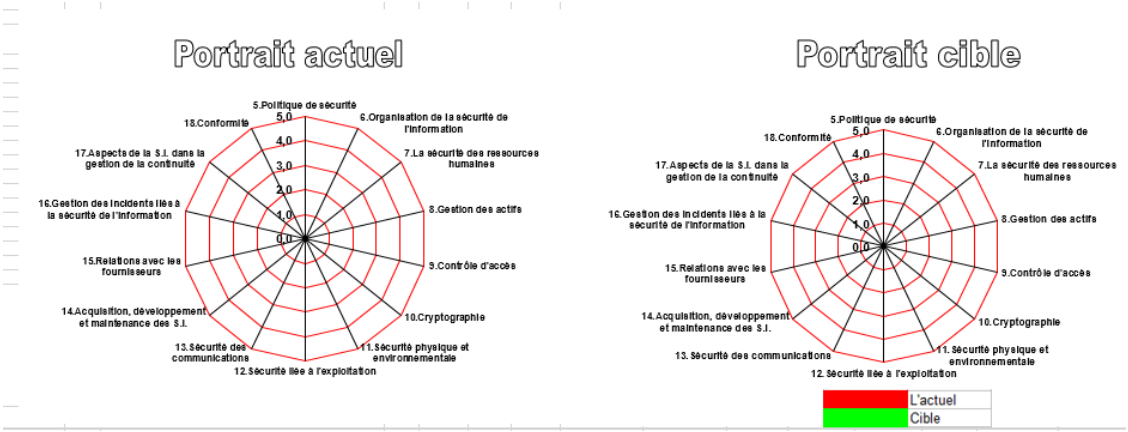
La colonne A vous indique le nombre de mesures applicables pour chaque article.

A	B	C
Mesures Applicables	Non applic.	**ISO 27002:2013 14 articles, 35 catégories de sécurité, 114 mesures**
2	0	5.Politique de sécurité
7	0	6.Organisation de la sécurité de l'information
6	0	7.La sécurité des ressources humaines
10	0	8.Gestion des actifs
14	0	9.Contrôle d'accès
2	0	10.Cryptographie
15	0	11.Sécurité physique et environnementale
14	0	12.Sécurité liée à l'exploitation
7	0	13.Sécurité des communications
13	0	14.Acquisition, développement et maintenance des S.I.
5	0	15.Relations avec les fournisseurs
7	0	16.Gestion des incidents liés à la sécurité de l'information
4	0	17.Aspects de la S.I. dans la gestion de la continuité
8	0	18.Conformité
114	**0**	

Les informations relatives à chaque mesure sont présentées dans l'onglet de l'article concerné.

Les rosaces

Faites défiler le contenu de l'onglet « Global » vers le bas à l'aide de la roulette de votre souris ou de la barre de défilement située à la droite de l'écran. Vous accéderez alors à deux rosaces dont l'utilité est expliquée plus loin.



Les niveaux du modèle d'évolution des capacités (cotation des mesures de sécurité)

Poursuivez votre défilement du contenu vers le bas pour voir la description des différents niveaux de l'échelle qui est utilisée pour mesurer l'atteinte de chaque objectif. Son utilisation est présentée plus loin.

Source: Capability Maturity Model	Cotation des mesures de sécurité
0 - Aucun	
Aucun processus/documentation en place	
1 - initial	
Le processus est caractérisé par la prédominance d'interventions ponctuelles, voire chaotiques. Il est très peu défini et la réussite dépend de l'effo	
2 - reproductible	
Une gestion élémentaire de la sécurité est définie pour assurer le suivi des coûts, des délais et de la fonctionnalité. L'expertise nécessaire au pro	
3 - défini	
Le processus de sécurité est documenté, normalisé et intégré dans le processus standard de l'organisation	
4 - maîtrisé	
Des mesures détaillées sont prises en ce qui concerne le déroulement du processus et la qualité générée. Le processus et le niveau de qualité s	
5 - optimisation	
Une amélioration continue du processus est mise en œuvre par une rétroaction quantitative émanant du processus lui-même et par l'application d'	

Contenu des onglets « Article 5 » à « Article 18 »

Chacun des 14 onglets suivants présente le même contenu. Pour vous permettre de vous familiariser avec ce contenu, prenons l'onglet « Article 7 » en exemple; vous n'avez qu'à cliquer dessus pour y accéder.

Les catégories de sécurité

En observant la droite de l'écran (colonnes I et J), on constate que l'article 7, « La sécurité des ressources humaines », contient trois catégories de sécurité :

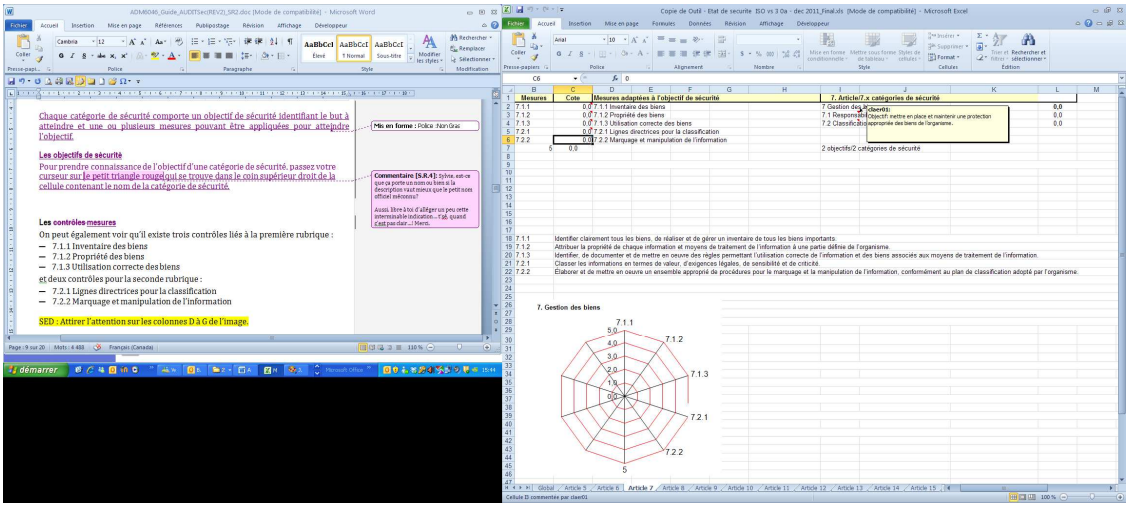
- 7.1 Avant l'embauche
- 7.2 Pendant la durée du contrat
- 7.3 Rupture, terme ou modification du contrat de travail

B	C	D	E	F	G	H	I	J	K
Mesures	**Cote**	**Mesures adaptées à l'objectif de sécurité**					**7. Article/7.x catégories de sécurité**		
7.1.1	0,0	7.1.1 Sélection des candidats					7 La sécurité des ressources humaines		
7.1.2	0,0	7.1.2 Termes et conditions d'embauche					7.1 Avant l'embauche		
7.2.1	0,0	7.2.1 Responsabilités de la direction					7.2 Pendant la durée du contrat		
7.2.2	0,0	7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information					7.3 Rupture, terme ou modification du contrat de travail		
7.2.3	0,0	7.2.3 Processus disciplinaire							
7.3.1	0,0	7.3.1 Achèvement ou modification des responsabilités associées au contrat de travail							
6	0,0						3 objectifs/3 catégories de sécurité		

Chaque catégorie de sécurité comporte un objectif de sécurité identifiant le but à atteindre et une ou plusieurs mesures pouvant être appliquées pour atteindre l'objectif.

Les objectifs de sécurité

L'objectif d'une catégorie de sécurité s'affiche lorsque vous passez votre curseur sur le petit triangle rouge situé dans la cellule où est nommée la catégorie de sécurité.



Les mesures

On peut également voir qu'il existe deux mesures liées à la première catégorie de sécurité :

- 7.1.1 Sélection des candidats
- 7.1.2 Termes et conditions d'embauche

trois mesures pour la seconde catégorie de sécurité :

- 7.2.1 Responsabilités de la direction
- 7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information
- 7.2.3 Processus disciplinaire

et enfin une mesure pour la troisième catégorie de sécurité :

- 7.3.1 Achèvement ou modification des responsabilités associées au contrat de travail

7.1.1	Il convient que des vérifications des informations concernant tous les candidats à l'embauche soient réalisées conformément aux lois, aux règlements et à l'éthique, et il convient qu'elles soient proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés.
7.1.2	Il convient que les accords contractuels conclus avec les salariés et les contractants déterminent leurs responsabilités et celles de l'organisation en matière de sécurité de l'information.
7.2.1	Il convient que la direction demande à tous les salariés et contractants d'appliquer les règles de sécurité conformément aux politiques et aux procédures en vigueur dans l'organisation.
7.2.2	Il convient que l'ensemble des salariés de l'organisation et, le cas échéant, les contractants suivent un apprentissage et des formations de sensibilisation adaptés et qu'ils reçoivent régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leurs fonctions.
7.2.3	Il convient qu'il existe un processus disciplinaire formel et connu de tous pour prendre des mesures à l'encontre des salariés ayant enfreint les règles liées à la sécurité de l'information.
7.3.1	Il convient de définir les responsabilités et les missions liées à la sécurité de l'information qui restent valables à l'issue de la rupture, du terme ou de la modification du contrat de travail, d'en informer le salarié ou le contractant et de veiller à leur application.

À chaque catégorie de sécurité sont associées une ou plusieurs mesures adaptées à l'objectif de sécurité.

Les mesures sont des moyens de gérer un risque, tels que les politiques, les procédures, les lignes directrices et les pratiques ou structures organisationnelles, et peuvent être de nature administrative, technique, gestionnaire ou juridique. Elles sont davantage détaillées plus bas dans la feuille Excel (lignes 18 à 22 dans l'exemple qui suit).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	P
	Mesures	**Cote**	**Mesures adaptées à l'objectif de sécurité**					**7. Article/7.x catégories de sécurité**						
	7.1.1	0,0	7.1.1 Sélection des candidats					7 La sécurité des ressources humaines			**0,0**			
	7.1.2	0,0	7.1.2 Termes et conditions d'embauche					7.1 Avant l'embauche			0,0			
	7.2.1	0,0	7.2.1 Responsabilités de la direction					7.2 Pendant la durée du contrat			0,0			
	7.2.2	0,0	7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information					7.3 Rupture, terme ou modification du contrat de travail			0,0			
	7.2.3	0,0	7.2.3 Processus disciplinaire											
	7.3.1	0,0	7.3.1 Achèvement ou modification des responsabilités associées au contrat de travail											
	6	0,0						3 objectifs/3 catégories de sécurité						

Mesures	7.1.1	Il convient que des vérifications des informations concernant tous les candidats à l'embauche soient réalisées conformément aux lois, aux règlements et à l'éthique, et il convient qu'elles soient proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés.
	7.1.2	Il convient que les accords contractuels conclus avec les salariés et les contractants déterminent leurs responsabilités et celles de l'organisation en matière de sécurité de l'information.
	7.2.1	Il convient que la direction demande à tous les salariés et contractants d'appliquer les règles de sécurité conformément aux politiques et aux procédures en vigueur dans l'organisation.
	7.2.2	Il convient que l'ensemble des salariés de l'organisation et, le cas échéant, les contractants suivent un apprentissage et des formations de sensibilisation adaptés et qu'ils reçoivent régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leurs fonctions.
	7.2.3	Il convient qu'il existe un processus disciplinaire formel et connu de tous pour prendre des mesures à l'encontre des salariés ayant enfreint les règles liées à la sécurité de l'information.
	7.3.1	Il convient de définir les responsabilités et les missions liées à la sécurité de l'information qui restent valables à l'issue de la rupture, du terme ou de la modification du contrat de travail, d'en informer le salarié ou le contractant et de veiller à leur application.

Ainsi, par exemple, pour réaliser la sécurité des ressources humaines, la mesure recommandée consiste à :

- 7.1.1 Convenir que des vérifications des informations concernant tous les candidats à l'embauche soient réalisées conformément aux lois, aux règlements et à l'éthique, et il convient qu'elles soient proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés.

De même, pour déterminer les accords contractuels, il faut :

- 7.1.2 Convenir que les accords contractuels conclus avec les salariés et les contractants déterminent leurs responsabilités et celles de l'organisation en matière de sécurité de l'information.

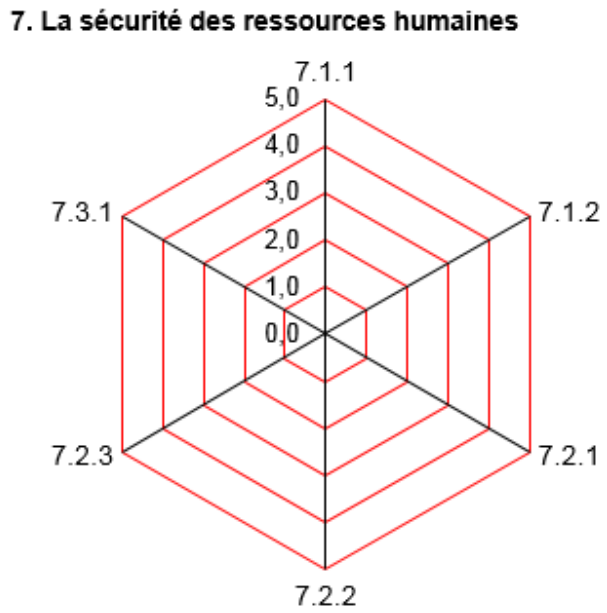
La description des mesures comprend également :

- des préconisations de mise en œuvre, qui proposent des informations détaillées pour mettre en œuvre la mesure et pour atteindre l'objectif de sécurité;
- des informations supplémentaires, qui présentent des compléments d'information à considérer, par exemple des éléments juridiques et des références à d'autres normes.

Par souci de concision, elles n'ont pas été incluses dans AUDITSec, mais vous les trouverez dans la norme ISO 27002 :2013, disponible à partir du menu « Outils méthodologiques » du site du cours.

La rosace

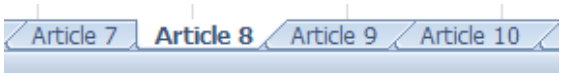
Au fur et à mesure que vous saisirez des valeurs dans la colonne C, « Cote », une rosace vous fournira le portrait actuel de l'état de la sécurité pour votre organisation pour l'article ou domaine de la sécurité visé. Vous aurez des explications plus détaillées à ce sujet dans la section « Instructions ».



Déplacements dans l'outil et autres fonctionnalités

Le déplacement d'un onglet à l'autre

Pour accéder à un onglet particulier, cliquez directement sur l'onglet voulu, par exemple sur « Article 8 » :

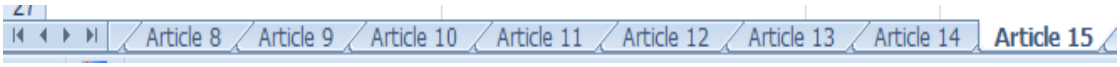


L'accès aux derniers onglets

Pour accéder aux derniers onglets qui ne sont pas visibles à l'ouverture du fichier, utilisez les flèches de déplacement tout à gauche du premier onglet :

Le retour aux premiers onglets

Pour revenir aux premiers onglets lorsqu'ils ne sont plus directement accessibles, utilisez ces mêmes flèches :

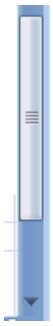


Le déplacement horizontal

Pour visualiser tout le contenu d'un onglet qui n'est pas visible à l'écran sur le plan horizontal, déplacez-vous à l'aide de la barre de défilement située à droite du dernier onglet :

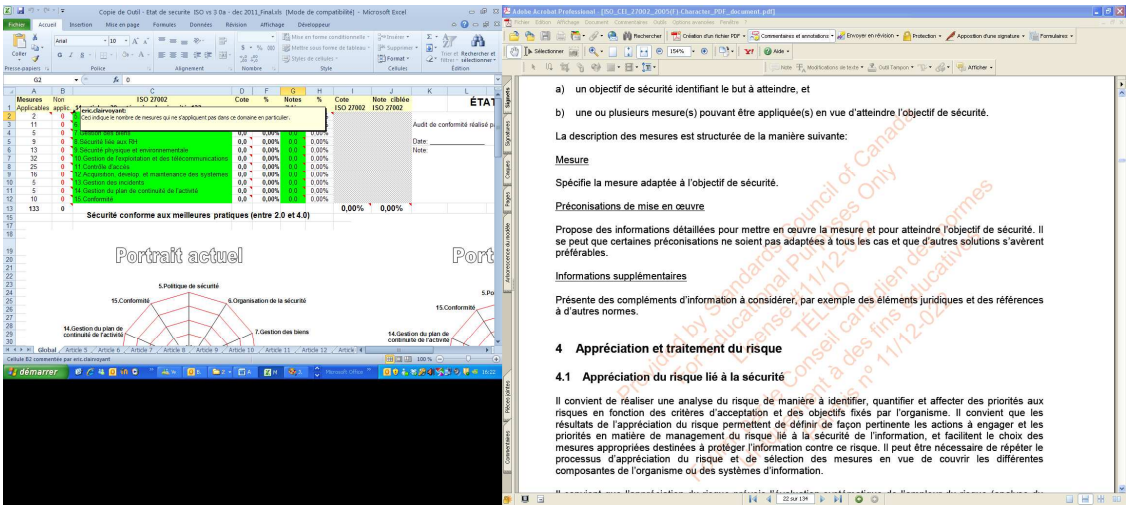
Le déplacement vertical

Pour visualiser tout le contenu d'un onglet qui n'est pas visible à l'écran sur le plan vertical, faites glisser la barre de défilement située à droite de l'écran :



L'information supplémentaire

Lorsque vous voyez un petit triangle rouge dans le coin supérieur droit d'une cellule, passez votre curseur dessus pour consulter l'information supplémentaire relative à cette cellule.



INSTRUCTIONS

Cette section vous explique comment utiliser l'outil AUDITSec pour réaliser un audit de sécurité.

Étape 1 : la saisie des valeurs pour les 14 articles ou domaines

- Vous devez d'abord cliquer sur l'un des 14 derniers onglets, au bas de l'écran, soit les articles numérotés de 5 à 18.

- Saisissez ensuite les valeurs qui correspondent à l'échelle de mesure qui suit, de 0 à 5, dans la colonne C de chacun des articles. Commencez à l'onglet « Article 5 »

et répétez l'exercice pour chacun des onglets suivants, soit pour chacun des articles ou domaines de la sécurité.

L'échelle de mesure

Les valeurs à saisir, de 0 à 5, proviennent du modèle d'évolution des capacités (CMM, pour *Capability Maturity Model*[2]). Ce modèle offre un cadre reconnu qui permet d'évaluer le degré de maturité des capacités. Il comprend une échelle à cinq niveaux auxquels s'ajoute le niveau 0.

Le niveau 0 (inexistant) : Il y a absence totale de processus identifiables. L'entreprise n'a même pas pris conscience qu'il s'agissait d'un problème à étudier.

Le niveau 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 de la gestion n'est pas organisée.

Le niveau 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 est laissée à l'individu. On se repose beaucoup sur les connaissances individuelles, d'où un risque d'erreurs.

Le niveau 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. Les procédures elles-mêmes ne sont pas sophistiquées, mais elles formalisent des pratiques existantes.

Le niveau 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.

Le niveau 5 (optimal) : Les processus ont atteint le niveau des bonnes pratiques à la suite d'une amélioration constante et en comparaison avec d'autres entreprises (modèles d'évolution des capacités). 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.

Acceptable ou non?

Les bonnes pratiques laissent croire que, pour chacun des 14 articles ou domaines, une valeur globale située entre 2 et 4 est acceptable.

— Au fur et à mesure que les valeurs sont saisies pour un article, une rosace se crée, fournissant une représentation visuelle de l'état actuel de la sécurité pour le domaine visé.

2. Voir « Capability Maturity Model Integration (CMMI) », *Software Engineering Institute /Carnegie Mellon*, [En ligne], [http://www.sei.cmu.edu/cmmi/].

— En parallèle, une rosace se met à jour dans l'onglet « Global » qui constitue le tableau de bord de tous les articles.

(Les rosaces sont expliquées plus loin dans ce document.)

IMPORTANT
Si une mesure ne s'applique pas à votre situation

Si une des mesures d'un article n'est pas pertinente à votre contexte, le champ doit demeurer vide.

Vous ne devez pas saisir la valeur 0 si une mesure ne s'applique pas étant donné que cela affectera le résultat final (la note 0 est considérée dans le calcul, abaissant ainsi les résultats obtenus, tandis qu'un champ vide n'entre pas dans le calcul).

Vous devez plutôt utiliser la touche **Suppr** ou **Del** du clavier. De cette façon, la mesure ne sera pas comptabilisée dans le calcul final.

Dans le tableau de bord, c'est-à-dire à l'onglet « Global », l'article sera en rouge, indiquant que certaines mesures ne sont pas applicables pour cet article.

Par exemple, dans l'image qui suit, on voit que, pour l'article 6 qui compte un total de neuf mesures applicables, deux mesures sont non applicables à la situation évaluée.

Mesures Applicables	Non applic.	ISO 27002:2013 14 articles, 35 catégories de sécurité, 114 mesures
2	0	5.Politique de sécurité
9	2	6.Organisation de la sécurité de l'information
5	0	7.La sécurité des ressources humaines

Astuce!

Pourquoi ne pas vérifier tout de suite ce qui vient de vous être expliqué?

Si ce n'est déjà fait, ouvrez l'outil AUDITSec, saisissez quelques valeurs dans un ou deux articles et voyez ce qui se produit. Jetez un coup d'œil à la rosace de chacun de ces articles, puis vérifiez le portrait global qui se dessine à l'onglet « Global ».

Étape 2 : le portrait global de la situation

— Une fois les valeurs saisies pour les mesures applicables de chacun des 14 articles, accédez à l'onglet « Global ».

— Vous obtiendrez alors le **portrait actuel** de votre organisation par rapport aux 14 articles ou domaines de la sécurité de la norme ISO 27002 :2013 et le **portrait cible** que vous déterminerez en fonction des objectifs que vous fixerez.

— Le contenu des différentes colonnes vous fournit des données chiffrées sur la situation actuelle et vous permet de saisir des données pour la situation cible, et ce, pour chacun des articles de la sécurité.

Le contenu des différentes colonnes de l'onglet « Global »

A	B	C	D	F	G	H	I	J
Mesures Applicables	Non applic	ISO 27002:2013 14 articles, 35 catégories de sécurité, 114 mesures	Cote	%	Notes ciblées	%	Cote ISO 27002:2013	Note ciblée ISO 27002:2013

La colonne A indique le nombre de mesures applicables pour chaque domaine visé en lien avec la norme ISO 27002 :2013.

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

La colonne C présente les titres des 14 articles ou domaines de la sécurité selon la norme ISO 27002 :2013.

La colonne D indique la valeur globale, ou cote, obtenue pour chaque article ou domaine. Ce calcul se fait automatiquement selon les valeurs saisies dans les autres onglets. Si jamais le symbole #DIV/0 apparaît, cela signifie que le calcul ne peut se faire parce qu'aucune mesure n'est sélectionnée; il n'y a donc aucune valeur 0 à 5 dans le domaine applicable. Par conséquent, ce code d'erreur est tout à fait pertinent.

(La colonne E n'est pas utilisée.)

La colonne F précise le pourcentage de conformité par rapport à l'ISO 27002 :2013, en fonction des valeurs saisies.

La colonne G est utilisée pour indiquer les cotes que vous souhaitez atteindre pour une certaine période. La valeur à saisir pour chaque note ciblée doit être un chiffre entier entre 1 et 5.

> Exemple : Si la colonne D présente une valeur de 2, alors à la colonne G, la valeur maximale suggérée devrait être de 3 et non de 4 ou 5. Il faut en effet se fixer des objectifs réalistes, car plus la valeur dans la colonne G sera élevée, plus les coûts d'implantation des mesures de sécurité le seront aussi.

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

La colonne I indique le pourcentage de l'état actuel de la sécurité en conformité avec la norme ISO 27002 :2013.

La colonne J donne la note ciblée (en pourcentage) pour la période.

- Utilisez la barre de défilement à droite de l'écran pour vous déplacer vers le bas et atteindre les deux rosaces qui viennent illustrer la situation globale actuelle et la situation cible.
- Utilisez la barre de défilement au bas de l'écran pour vous déplacer de gauche à droite dans le fichier.

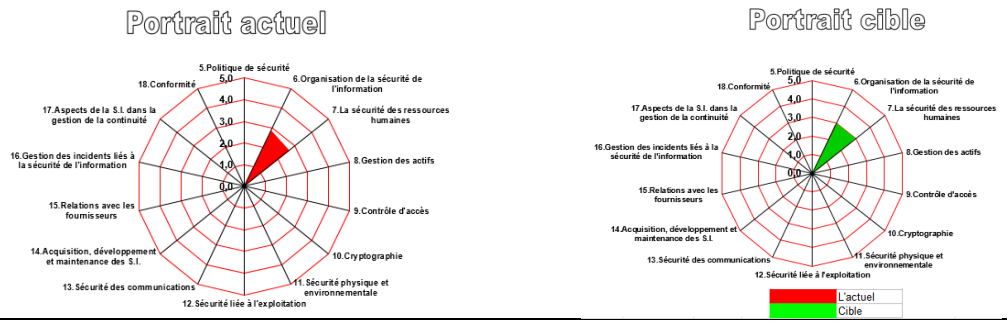
Les rosaces

Les rosaces sont constituées de courbes illustrant chaque article ou domaine de la sécurité. La rosace de gauche, « Portrait actuel », fait voir l'état actuel de la sécurité et celle de droite, « Portrait cible », montre l'état visé de la sécurité.

Le **portrait actuel** indique l'état de la sécurité au moment de la compilation des données, en fonction des valeurs que vous avez saisies pour chacune des mesures de chaque domaine.

Le **portrait cible** indique, en rouge, l'état actuel de la sécurité et, en vert, la cible que désire atteindre l'organisation en fonction des valeurs que vous aurez saisies comme objectifs dans la colonne G.

7	0	6.Organisation de la sécurité de l'information	2,9	57,14%	3,0	60,00%
6	0	7.La sécurité des ressources humaines	2,7	53,33%	3,0	60,00%



EXEMPLE D'UTILISATION D'AUDITSEC

Cette section présente un scénario type illustrant l'utilisation d'AUDITSec. Nous vous recommandons de suivre cet exemple avec l'outil et d'insérer les valeurs suggérées dans ce scénario afin de pouvoir en observer les effets directement dans l'outil.

Exemple de l'étape 1 : la saisie des valeurs pour les 14 articles ou domaines

On peut utiliser l'outil pour vérifier la sécurité pour un article particulier ou pour l'ensemble des articles. On choisit pour cet exemple de réaliser un audit pour l'article 7 de la norme ISO 27002 :2013, « La sécurité des ressources humaines », soit l'onglet « Article 7 ».

On note d'abord que cet article comporte trois catégories de sécurité (7.1 à 7.3) et six mesures (7.1.1 à 7.3.1).

On évalue ensuite le niveau de sécurité pour chacune des mesures en se référant à l'échelle de mesure.

La première mesure

La mesure 7.1.1, « Sélection des candidats », est ainsi décrite :

> *Il convient que des vérifications des informations concernant tous les candidats à l'embauche soient réalisées conformément aux lois, aux règlements et à l'éthique, et il convient qu'elles soient proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés.*

On se demande alors :

> Est-ce que la valeur pour la **colonne C**, « Cote », est 0, 1, 2, 3, 4 ou 5 selon l'échelle de valeurs du modèle d'évolution des capacités? Autrement dit, à quel niveau évaluons-nous la sécurité pour cette mesure dans notre organisation?

Pour cet exemple, supposons que le processus de sécurité est « documenté, normalisé et intégré dans le processus standard de l'organisation », c'est-à-dire qu'il correspond au niveau 3, « défini ». (Vous trouverez un rappel de la signification de chaque niveau en passant votre curseur sur le triangle rouge situé dans chaque cellule de la colonne C, « Cote ».) Saisissez la valeur 3 dans la colonne C, à la ligne de la mesure 7.1.1.

Passons à la mesure suivante.

La deuxième mesure

La mesure 7.1.2, « Termes et conditions d'embauche », est ainsi décrite :

> *Il convient que les accords contractuels conclus avec les salariés et les contractants déterminent leurs responsabilités et celles de l'organisation en matière de sécurité de l'information.*

Pour cet exemple, supposons qu'« une gestion élémentaire de la sécurité est définie pour assurer le suivi des accords contractuels » et que « l'expertise nécessaire au processus est en place », soit le niveau 2, « reproductible ». Saisissez la valeur 2 dans la colonne C, à la ligne de la mesure 7.1.2.

Passons à la mesure suivante.

La troisième mesure

Pour la mesure 7.2.1, « Responsabilités de la direction », supposons à nouveau que ce processus correspond au niveau 3, « défini ». Saisissez la valeur 3 dans la colonne C, à la ligne de la mesure 7.2.1.

Les mesures suivantes

Dans une situation réelle, vous poursuivriez de la même façon pour l'ensemble des mesures suivantes. Pour les fins de notre illustration, nous nous arrêtons ici.

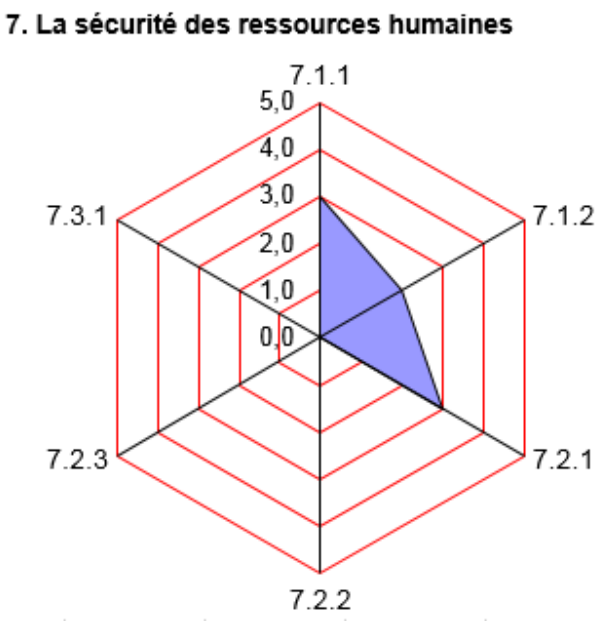
L'observation des résultats

Les premières lignes de la colonne C devraient ressembler à ceci :

B	C	D	I
Mesures	**Cote**	**Mesures adaptées à l'objectif de sécurité**	**7. Article/7.x catégories de sécurité**
7.1.1	3,0	7.1.1 Sélection des candidats	7 La sécurité des ressources humaines
7.1.2	2,0	7.1.2 Termes et conditions d'embauche	7.1 Avant l'embauche
7.2.1	3,0	7.2.1 Responsabilités de la direction	7.2 Pendant la durée du contrat
7.2.2	0,0	7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information	7.3 Rupture, terme ou modification du contrat de travail
7.2.3	0,0	7.2.3 Processus disciplinaire	
7.3.1	0,0	7.3.1 Achèvement ou modification des responsabilités associées au contrat de travail	
6	1,3		3 objectifs/3 catégories de sécurité

Observez, dans le bas de cette colonne, que pour cet exemple la cote finale obtenue pour l'article 7 est 1,3. (Il s'agit tout simplement de la moyenne des six cotes; comme nous avons laissé la valeur 0 pour les trois dernières mesures, cela explique que la cote soit si basse.)

Une rosace s'est également dessinée pour chaque article ou domaine que nous avons coté :



Exemple de l'étape 2 : le portrait global de la situation

Une fois que vous avez saisi toutes les valeurs pour chaque mesure applicable de chacun des 14 articles, le tableau de bord, c'est-à-dire l'onglet « Global », se met à jour.

Voici à quoi il ressemble dans notre exemple :

A	B	C	D	F	G	H	I	J
Mesures Applicables	Non applic.	**ISO 27002:2013** **14 articles, 35 catégories de sécurité, 114 mesures**	**Cote**	**%**	**Notes ciblées**	**%**	**Cote ISO 27002:2013**	**Note ciblée ISO 27002:2013**
2	0	5.Politique de sécurité	0,0	0,00%	0,0	0,00%		
7	0	6.Organisation de la sécurité de l'information	0,0	0,00%	0,0	0,00%		
6	0	7.La sécurité des ressources humaines	1,3	26,67%	0,0	0,00%		
10	0	8.Gestion des actifs	0,0	0,00%	0,0	0,00%		
14	0	9.Contrôle d'accès	0,0	0,00%	0,0	0,00%		
2	0	10.Cryptographie	0,0	0,00%	0,0	0,00%		
15	0	11.Sécurité physique et environnementale	0,0	0,00%	0,0	0,00%		
14	0	12.Sécurité liée à l'exploitation	0,0	0,00%	0,0	0,00%		
7	0	13.Sécurité des communications	0,0	0,00%	0,0	0,00%		
13	0	14.Acquisition, développement et maintenance des S.I.	0,0	0,00%	0,0	0,00%		
5	0	15.Relations avec les fournisseurs	0,0	0,00%	0,0	0,00%		
7	0	16.Gestion des incidents liés à la sécurité de l'information	0,0	0,00%	0,0	0,00%		
4	0	17.Aspects de la S.I. dans la gestion de la continuité	0,0	0,00%	0,0	0,00%		
8	0	18.Conformité	0,0	0,00%	0,0	0,00%		
114	**0**						**1,90%**	**0,00%**
		Sécurité conforme aux meilleures pratiques (entre 2.0 et 4.0)						

L'état actuel de la sécurité pour l'article 7

Comme on peut le constater en observant la colonne D, la valeur globale 1,3 est représentée ainsi que le pourcentage de conformité à l'ISO 27002 :2013, soit 26,67 %.

Dans cet exemple, étant donné que nous n'avons saisi des valeurs que pour un seul des 14 articles, la cote globale de conformité à la norme ISO 27002 :2013 est de 1,90 % (au bas de la colonne I).

La note ciblée ou la situation visée

Vous devez maintenant inscrire à la colonne G la note ciblée pour une période donnée, c'est-à-dire ce sur quoi vous souhaitez concentrer vos efforts pour une période qui peut être d'un an, par exemple.

Des objectifs à atteindre
Rappelons qu'une cote de sécurité souhaitable se situe entre 2 et 4. Utilisez l'outil et les bonnes pratiques qu'il contient (mesures, préconisations de mise en œuvre et autres informations supplémentaires incluses dans la norme ISO 27002 :2013) pour formuler des recommandations d'amélioration ou entreprendre des actions.

Nous indiquerions normalement une cote cible pour chacun des articles dans la colonne G, « notes ciblées ». Dans notre exemple, supposons que la valeur 2 est notre cible pour l'ensemble des mesures de l'article 7.

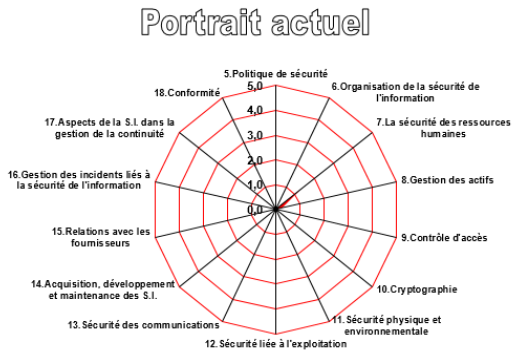
A	B	C	D	F	G	H	I	J
Mesures Applicable	Non applic	ISO 27002:2013 14 articles, 35 catégories de sécurité, 114	Cote	%	Notes ciblée	%	Cote ISO 27002:2013	Note ciblée ISO 27002:2013
2	0	5.Politique de sécurité	0,0	0,00%	0,0	0,00%		
7	0	6.Organisation de la sécurité de l'information	0,0	0,00%	0,0	0,00%		
6	0	7.La sécurité des ressources humaines	1,3	26,67%	2,0	40,00%		
10	0	8.Gestion des actifs	0,0	0,00%	0,0	0,00%		
14	0	9.Contrôle d'accès	0,0	0,00%	0,0	0,00%		
2	0	10.Cryptographie	0,0	0,00%	0,0	0,00%		
15	0	11.Sécurité physique et environnementale	0,0	0,00%	0,0	0,00%		
14	0	12.Sécurité liée à l'exploitation	0,0	0,00%	0,0	0,00%		
7	0	13.Sécurité des communications	0,0	0,00%	0,0	0,00%		
13	0	14.Acquisition, développement et maintenance des S.I.	0,0	0,00%	0,0	0,00%		
5	0	15.Relations avec les fournisseurs	0,0	0,00%	0,0	0,00%		
7	0	16.Gestion des incidents liés à la sécurité de l'informatio	0,0	0,00%	0,0	0,00%		
4	0	17.Aspects de la S.I. dans la gestion de la continuité	0,0	0,00%	0,0	0,00%		
8	0	18.Conformité	0,0	0,00%	0,0	0,00%		
114	0	Sécurité conforme aux meilleures pratiques (entre 2.0 et 4.0)					1,90%	2,86%

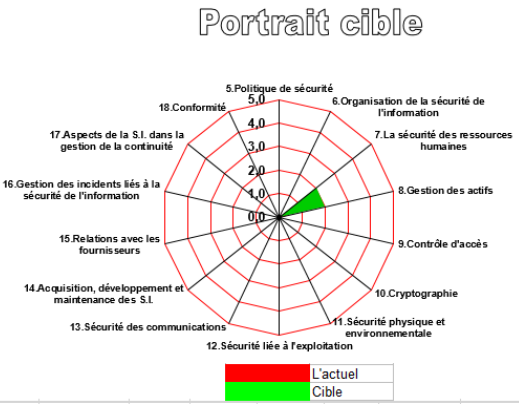
La note ciblée pour l'ensemble des articles

Cette cible de 2 pour l'ensemble des mesures de l'article 7 permettra d'atteindre une note ciblée ISO 27002 :2013 à 2,86 % (colonne J). Notez que si nous avions saisi des cotes cibles dans la colonne G, « notes ciblées », pour chacun des articles, cette note serait le résultat compilé (la moyenne) des notes ciblées pour l'ensemble des articles.

Le portrait actuel et le portrait cible

Vous pouvez maintenant voir les rosaces qui illustrent automatiquement, au fil des valeurs saisies, les deux situations : le portrait actuel de la sécurité (en rouge) et le portrait cible (en vert) qui vous indique où concentrer vos efforts de sécurité.





Éric Clairvoyant
Consultant en sécurité
ecclairvoyant@hotmail.com

Mai 2014