BENCHMARK OUTILS SMSI

Novembre 2012

CLUB 27001
Site internet : http://www.club-27001.fr
Adresse email: club-27001@club-27001.fr.

Questionnaire pour l'analyse technique des outils de management de la sécurité de l'information utilisables dans le cadre des normes ISO 2700X

Introduction

L'objectif de ce questionnaire d'analyse technique est de permettre aux RSSI ou Responsables SMSI de se poser les bonnes questions, afin de choisir un outil SMSI en fonction de leurs besoins et contraintes internes.

Le questionnaire est construit selon les exigences de la norme ISO 27001:2005, mais également selon des fonctionnalités identifiées comme nécessaires pour la construction et l'exploitation d'un Système de Management de la Sécurité de l'Information.

Contributeurs

Le Club 27001 remercie les personnes du comité technique du Groupe de Travail "benchmark outils SMSI" qui ont contribué à la formalisation de ce questionnaire technique :

Contributeur	Rôle dans le GT	Entité
Thomas Lebouc	Animateur du Groupe de Travail	THALES
Emmanuel Joulain	Animateur du Comité technique	THALES
Niki Ioannidou-Gambier	Contributeur	RICOH France
Guillaume Le Galliard	Contributeur	Logica Business Consulting
Florence Le Goff	Contributeur	SOLUCOM
Didier Renauld	Contributeur	MIAXYS
Martin Veron	Contributeur	ESR Consulting

Nous remercions également les personnes ayant participé à la relecture de ce questionnaire technique.

CLUB 27001

" Benchmark d'outils SMSI "

Questionnaire pour l'analyse technique des outils de management de la sécurité de l'information utilisables dans le cadre des normes ISO 2700X

Liste des thématiques adressées :

Couverture de la norme	Analyse de risques
	Audit & conformité
	Tableau de bord et indicateurs
	Processus / Workflow / Organisation
	Gestion documentaire
	Suivi des actions et des événements
Analyse de l'outil	Sécurité des SI
	Coût / complexité
	Ergonomie
	Environnement technique & Sécurité
	Adaptabilité / Interopérabilité
	Intégration autres référentiels
	Test / acquisition / exploitation

Notation utilisée :

1	Ne répond pas à l'exigence
2	Répond partiellement à l'exigence
3	Répond globalement à l'exigence
4	Répond parfaitement à l'exigence
n/a	Non applicable, exigence non testée

Thématiques	Questions	Commentaire / réponse	PDCA	Point de la norme ISO 27001							Notation
Analyse des risques	Existe-t-il un module d'analyse des risques et une description associée ? *Sur la base d'EBIOS, 27005, CRAMM etc.…*		**PLAN**	4.2.1.c	4.3.1.d	5.1.f					
	L'outil contient-il par défaut des bases de connaissances pour l'analyse des risques ? *Scénarios de risques, liste d'actifs, de menaces, de vulnérabilités, de mesures de sécurité…)*										
	Existe-t-il une fonctionnalité permettant de faire l'identification des risques ? *Saisir ou générer une liste de scénarios de risques*		**PLAN**	4.2.1.d							
	L'outil permet-il d'intégrer une liste d'actifs (primordiaux / supports), de menaces, et/ou de vulnérabilités ? *Saisir ou importer une liste existante*										
	Existe-t-il une fonctionnalité permettant de faire une évaluation des risques identifiés ? *Evaluation de l'impact, de la vraisemblance, de la gravité (croisement Impact & Vraisemblance) Calcul automatique ou manuel*		**PLAN**	4.2.1.e							
	Les critères et échelles de base de l'évaluation des risques sont-ils personnalisables ? *Critères DIC, niveau, Impact, potentialité, gravité ou autres*										
	L'outil permet-il de sélectionner les choix de traitement des risques évalués ? *Accepter / Partager / Réduire / Refuser*		**PLAN**	4.2.1.f							
	L'outil permet-il de définir ou sélectionner les objectifs de sécurité (thèmes ISO 27002) et des mesures de sécurité pour les rattacher aux risques ?		**PLAN**	4.2.1.g							
	L'outil permet-il d'intégrer des référentiels de mesures de sécurité ? *Saisir ou importer ISO 27002, NIST, RGS etc.*										
	L'outil permet-il d'établir le calcul du risque résiduel ? *Calcul automatique ou manuel*		**PLAN**	4.2.1.h							
	L'outil permet-il de générer un rapport d'analyse / appréciation des risques utilisable pour une présentation des résultats à la Direction Générale et obtenir son approbation pour mettre en œuvre et exploiter le SMSI ?		**PLAN**	4.2.1.i	7.2	4.3.1.e	5.1.b	7.2.e			

CLUB 27001

" Benchmark d'outils SMSI "

Thématiques	Questions	Commentaire / réponse	PDCA	Point de la norme ISO 27001							Notation
	L'outil permet-il d'établir / de générer une Déclaration d'Applicabilité (DdA) basée sur l'ISO 27002 ? *Listes des objectifs, sélection, justification d'exclusion*		**PLAN**	4.2.1.j	4.3.1.i						
	Est-il possible de générer un plan de traitement des risques ? *Plan d'action, planning, budget, priorité, responsable…*		**DO**	4.2.2.a	4.2.2.b	4.2.2.c	4.3.1.f				
	Est-il possible d'importer un plan de traitement des risques externe à l'outil ?										
	L'outil permet-il de garder un historique des précédentes analyses des risques? *(réexamen de l'AdR)*		**CHECK**	4.2.3.d							
Audit & conformité											
	L'outil permet-il d'identifier les points de contrôles du SMSI ? *Identification de contrôles sur des activités du SMSI, des politiques ou des mesures, procédure de réalisation et les objectifs et résultats attendus du contrôle*		**PLAN**	4.2.2.d	4.3.1.c	4.3.1.g					
	L'outil permet-il de planifier la réalisation de plan de contrôles ? *Fréquence de réalisation, affectation à un porteur, suivi des charges*		**PLAN**	5.1.e	4.2.3.a	4.2.3.b	4.2.3.c				
	L'outil permet-il de suivre la réalisation du plan de contrôles et des écarts constatés par rapport aux objectifs ? *Avancement du plan de contrôle, questionnaire des points de contrôles à réaliser, Fiche de résultats, valorisation d'un contrôle à l'aide d'indicateurs, définition de seuil...*		**CHECK**	4.2.3.a	4.2.3.b	4.2.3.c	7.2	7.2			
	Suite à la réalisation d'un contrôle, est-il possible de suivre le traitement des écarts constatés? *Liaison entre des non conformités et des plans d'actions ?*		**ACT**	4.2.4.b							
	L'outil permet-il de définir un programme d'audits internes du SMSI ? *Identification et priorisation de périmètre à auditer : activités du SMSI, des politiques ou des mesures, date de réalisation, affectation à un auditeur, suivi des charges.*		**PLAN**	6	6.a	6.b	4.2.3.e	5.1.e			
	L'outil permet-il d'intégrer et de mettre à disposition une procédure d'audit ? *Intégration d'une pièce jointe*		**PLAN**	4.3.1.g	6						
	L'outil permet-il de suivre la réalisation des audits internes et des résultats associés? *Avancement d'un audit interne, résultats (recommandations), évaluation de la conformité…*		**CHECK**	5.1.g	6.c	6.d	7.2.a	7.2.f	7.2.i		
	L'outil permet-il d'intégrer / importer des rapports d'audits ?										
	Est-il possible de définir et personnaliser les niveaux de criticité des écarts (remarque, mineur, majeur) ?										
	Suite à un audit, est-il possible de suivre le traitement des écarts constatés? *Liaison entre des non conformités et/ou recommandations à des plans d'actions*		**ACT**	6	4.2.4.b						
	L'outil permet-il de générer des rapports de conformité / efficacité utilisable pour les comité d'audit et la Revue de Direction du SMSI ? *Synthèse des résultats issus des méthodes d'évaluation (contrôles, audits…)*		**CHECK**	7.2.a	7.2.f	7.2.i					
	L'outil permet-il la gestion d'indicateurs et de tableaux de bord ?		**DO**	4.2.2.d	4.2.2.h						
	L'outil contient-il par défaut une liste d'indicateurs et tableaux de bord ?										
	Les indicateurs et tableaux de bord sont-ils personnalisables? *Utilisation de modèle de tableau de bord existant, échelle et représentation graphique ?*										
	L'outil fournit-il un tableau de bord de suivi des événements de sécurité, de l'efficacité des processus du SMSI , du plan d'action, et du niveau de risques, etc.?		**CHECK**	6.b							

CLUB 27001

" Benchmark d'outils SMSI "

Thématiques	Questions	Commentaire / réponse	PDCA	Point de la norme ISO 27001							Notation
Tableau de bord et indicateurs	L'outil fournit-il un tableau de bord de suivi du niveau de conformité par rapport à la norme, aux objectifs, à l'ISO 27001 et/ou DDA ?		**CHECK**	6.a							
	Permet-il l'automatisation de la collecte des indicateurs ? En particulier, peut-il être interconnecté avec d'autres outils externes (outil de gestion des incidents, outils de surveillance de la sécurité...) ? *Intégration avec les outils de gestion d'incidents, possibilité de définition d'un workflow de remontée d'indicateurs, relance automatique des responsables de la remontée d'indicateurs...*										
	L'outil permet-il de générer un rapport utilisable pour la Revue de Direction du SMSI ? *Vision consolidée de l'évolution des indicateurs (évènements de sécurité, mesures d'efficacité, conformité etc.)*		**ACT**	7.2.f	7.2.d						
	L'outil permet-il de garder un historique des précédents indicateurs ?										
	Existe-t-il une fonctionnalité permettant de planifier la collecte d'indicateurs ? *Worflow ou planning de collecte*										
Processus / Workflow / Organisation /											
	Est-il possible de définir la politique du SMSI dans l'outil ? *Cadrage de la politique dans l'outil ou attachement d'un document*		**PLAN**	4.1	4.2.1.a	4.3.1.a	4.3.1.b	5.1	5.1.a	5.1.b	
	Est-il possible de modéliser une cartographie des processus du SMSI et procédures associées ?		**PLAN**	4.2.1.b	4.3.1.c						
	Est-il possible de décrire l'organisation, les rôles et responsabilités autour du SMSI (RACI) ?		**PLAN**	5.2.1	4.2.2.g	5.1.c	5.1.e				
	Existe-t-il un moteur de workflow permettant de cadrer les échanges / actions / validation…?		**DO**	4.2.2.f							
	Existe-t-il un centre de notifications / gestion des tâches / opérations du SMSI ? *Permet-il de réaliser des rappels automatiques, des alertes*										
	Existe-t-il une fonctionnalité de gestion des formations (planning / compétences) ? *Rattachement des preuves de formations ou feuille de présence*		**DO**	4.2.2.e	5.2.2.a	5.2.2.b	5.2.2.c	5.2.2.d	5.2.2	5.1.d	
	Existe-t-il une fonctionnalité de gestion de la communication / sensibilisation ? *Intranet de communication / module de questionnaire en ligne*		**DO**	4.2.2.e	5.2.2						
	L'outil permet-il l'échange d'information avec les parties intéressés du SMSI (clients, partenaires, acteurs du SMSI) ? *Remontée d'information, questionnaire, intranet / extranet de communication*		**CHECK**	7.2.b	4.2.4.c						
	Existe-t-il une fonctionnalité de gestion de préparation et gestion de la revue de Direction ? *Planning des revues, check-list des données entrantes et données sortantes*		**ACT**	7.1	7.2	7.3	4.2.3.f	5.1.h			
Gestion documentaire											
	Existe-t-il une fonctionnalité de gestion documentaire ? *Centralisation et mise à disposition de la documentation du SMSI*		**DO**	4.3.1	4.3.2.d	4.3.2.h					
	Existe-t-il un workflow associé à la gestion documentaire (approbation, vérification….) ?		**DO**	4.3.2.a							
	Est-il possible de gérer le cycle de revue des documents ? *Alerte de mise à jour en cas de fin de vie*		**DO**	4.3.2.b	4.3.2.i						

CLUB 27001

" Benchmark d'outils SMSI "

Thématiques	Questions	Commentaire / réponse	PDCA	Point de la norme ISO 27001							Notation
	Est-il possible de gérer l'identification (nom de code / origine document) et le versionning des documents ?		**DO**	4.3.2.c	4.3.2.e	4.3.2.g	4.3.2.j				
	Existe-t-il une gestion des droits d'accès à la documentation en fonction des habilitations ?		**DO**	4.3.2.f							
	Est-il possible de lier un enregistrement à un processus ou une action du SMSI ? *CR de revue de Direction, preuve de l'implication de la Direction, preuve d'une formation, rapport d'audit etc.*		**DO**	4.3.3	4.3.1.h						
Suivi des actions / évènements	Existe t-il un module permettant de créer et centraliser les événements liés au SMSI ? *Problèmes, demande d'amélioration, audit externe, analyse des risques, résultat d'audit, retour de parties intéressées, décision de la Direction*		**DO**	8.1	4.2.3.g	4.2.3.h					
	Est-il possible d'identifier / taguer la source de l'événement ? R*evue de direction, revue de processus, audit internet et externe…) dans le module afin de pouvoir les trier par la suite*		**DO**	8.2.a	8.2.b	8.3.a					
	Est-il possible de lier l'événement à un processus ou une mesure de sécurité du SMSI ?		**DO**	8.2.a	8.2.b	8.3.a					
	Est-il possible d'instruire le choix de prendre en compte ou non une action pour que l'événement ne se reproduise ou éviter son apparition (accepté, refusé,) et identifier la personne responsable ?		**DO**	8.2.c	8.3.b						
	Est-il possible de lier une action (dont préventive ou corrective ou d'amélioration) à un événement validé ?		**DO**	8.2.d	8.3.c	4.2.4.b	7.2.c				
	Est-il possible d'inclure l'action identifiée dans le plan d'action en gardant la source (incident, revue de direction, revue de processus, audit…) et son type (préventive ou corrective ou d'amélioration) ?		**DO**	8.2.d	8.3.c	8.3 g	7.2.d				
	Est-il possible de lier une action d'amélioration présente dans le plan d'action à des risques identifiés afin de recalculer le risque résiduel ?		**DO**	4.2.4.d	8.3	8.2					
	Est-il possible de lier à l'action une preuve de la mise en place (PV de recette - validation dans l'outil…) ? *(Pièce jointe…)*		**DO**	8.2.e	8.3.d						
	Est-il possible d'inclure une étape de vérification des actions terminées ? *Description des contrôles à réaliser, l'évaluation de l'efficacité de l'action, leur fréquence, leur responsable ou lien vers la fonctionnalité de gestion des contrôles*		**CHECK**	8.2.f	8.3.e						
	Est-il possible de suivre l'avancement des actions d'amélioration dans le plan d'action ?		**CHECK**	4.2.4.a							
	L'outil permet-il de générer un rapport utilisable pour la Revue de Direction du SMSI ? *Vision consolidée de la gestion des événements, l'avancement…*		**ACT**	7.2.d							

Thématiques	Questions	Réponses	PDCA	Point de la norme ISO 27001	Notation
Sécurité des SI	L'outil propose t-il des fonctionnalités utiles au responsable aux acteurs de la Sécurité (RSSI, responsable sécurité physique, gestion des déclarations CNIL) ? R*eporting opérationnel (malware, gestion des correctifs, audits des journaux d'évènements etc.)*				n/a

CLUB 27001

" Benchmark d'outils SMSI "

Thématiques	Questions	Commentaire / réponse	PDCA	Point de la norme ISO 27001	Notation
Coût / complexité	*Les éléments de coût d'acquisition et de maintenance (reprendre estimation questionnaire préliminaire), de temps d'administration, d'exploitation, la taille minimal du projet, etc. seront évaluées par les analystes, mais aucune note ne sera communiquée dans le rapport. Ces informations permettront de compléter le commentaire.*				n/a
Ergonomie					
	L'outil est-il globalement attrayant (incitant l'utilisation, etc.) ?				
	L'utilisateur peut-il accéder au contenu souhaité en un nombre limité de clic ?				
	Existe-t-il un moteur de recherche efficace ?				
	L'outil vous parait-il simple d'utilisation sans formation ? *User-friendly, lisible*				
	L'outil permet-il d'une part d'éviter ou de réduire les erreurs de manipulation, d'autre part de les détecter lorsqu'elles surviennent ? *Pop up d'alerte, demande de confirmation*				
	Les utilisateurs ont-il les moyens pour personnaliser leur interface ? *Personnalisation des menus, des couleurs, logo*				
	L'ensemble des éléments de l'interface de l'outil permet-il la réduction de la charge liée au SMSI ?				
	L'interface d'administration de cet outil vous semble-t-elle simple ? *User-friendly, lisible*				
Environnement technique & Sécurité					
	Quelles plateformes sont supportées par l'outil (OS, matériels, serveur d'application)?				n/a
	Sur quel type d'architecture l'outil est-il basé: Autonome (mono utilisateur) ou Client Serveur (multi utilisateurs) ?				n/a
	En cas d'architecture client/serveur: Est-ce un client "lourd", un client "léger", ou les 2 ?				n/a
	En quel langage l'outil est-il développé: JAVA/C++/PHP/RUBIS/Autre (préciser)?				n/a
	L'outil dispose-t-il d'un référentiel dédié, et si oui de quel type ? *Base SQL, Annuaire LDAP*				n/a
	L'outil supporte-t-il des extensions (plugins) et si oui dans quels langages?				n/a
	Quels moyens d'authentification sont proposés ? L*ogin / mot de passe, politique de mots de passe*				
	Est-il possible de créer sa propre gestion des habilitations et profils associés (utilisateur, administrateur, auditeur…) ? *Accès qu'à certaines fonctionnalités en fonction du profil*				
	Est-il possible de configurer une procédure de sauvegarde des données de l'outil ?				
	Comment les données (référentiels, rapports, etc.) sont-elles protégées ? *Intégrité/confidentialité des données stockées dans l'outil*				

CLUB 27001

" Benchmark d'outils SMSI "

Thématiques	Questions	Commentaire / réponse	PDCA	Point de la norme ISO 27001	Notation
	Les accès et actions sur l'outil sont-ils tracés ?				
	Quels modes d'hébergement sont proposés? *Sur site, ASP, les deux*				n/a
	Localisations & langues du support technique ?				n/a
Adaptabilité / Interopérabilité					
	Est-il possible de redimensionner à tout moment le périmètre du SMSI ? *Ajout d'un site physique, modification de l'organisation, modification du SI etc.*				
	Quels sont les formats d'import / export de l'outil ? *XML, CSV, pdf, document de bureautique*				n/a
	Est-il possible d'interfacer l'outil avec une solution de PKI ou annuaire d'authentification ? *Gestion des accès, profils et habilitations*				
	Est-il possible d'interfacer l'outil avec un logiciel de gestion de calendrier ? *Alerte, planification des réunions*				
	Est-il possible d'interfacer l'outil avec un outil de courrier électronique ?				
	Est-il possible d'interfacer l'outil avec un outil de gestion de workflow ?				
	Est-il possible d'interfacer l'outil avec une solution externe de gestion documentaire ?				
	Est-il possible d'interfacer l'outil avec des outils de système de management en place ? *Système de management de la qualité, sécurité, environnement*				
Intégration autres référentiels					
	Une bibliothèque de référentiels / lois / règlements est-elle disponible pour l'outil ? S*OX, Bâle 2, RGS, Solvency, COBIT*				
	L'outil prend-il en compte automatiquement la publication des nouveaux référentiels et les mises à jour ?				
	Est-il possible de créer et personnaliser son propre référentiel ? *PSSI, Charte, exigences contractuelles*				
	L'outil permet-il de garder un historique des versions des exigences d'un référentiel et les liens avec les contrôles ou mesures de sécurité associés ?				
	Est-il possible de mutualiser certaines activités du SMSI avec d'autres systèmes de management ? R*evue de Direction, audit, risques, demandes des parties intéressées, fiches d'amélioration, documentation*				
Test / acquisition / exploitation					
	Les modalités de tests sont-elles facilités ? P*lateforme de test disponible, limitation en termes de fonctionnalité, données inclues*				
	La solution est-elle proposée sous la forme de modules ou de package global ?				
	Est-il possible d'acquérir l'outil de manière progressive ? A*cquisition de modules complémentaires en fonction des besoins*				
	Existe-t-il un programme de formation (utilisateur / administrateur fonctionnel et technique) à l'outil ?				