Pre-print en diffusion libre autorisée
Publication consultable ici : https://doi.org/10.1016/j.irbmnw.2018.08.001

Sécurité de l'information : Autodiagnostic selon l'ISO/CEI 27001

F. Dumont (Master qualité et performance dans les organisations), S. Jemai (Master qualité et performance dans les organisations), Z. Xu (Master qualité et performance dans les organisations), PM. Felan (Certification Professionnelle ABIH), G. Farges (Master qualité et performance dans les organisations)

Université de Technologie de Compiègne, CS 60319, 60203 Compiègne cedex, France

Auteurs correspondants : gilbert.farges@utc.fr - fdumont1993@hotmail.fr

1) La sécurité du système d'Information

Le Système d'Information (SI) peut être considéré comme un ensemble cohérent de ressources (personnel, logiciels, processus, données, matériels, équipements informatiques, de télécommunication …) permettant de recueillir, traiter, stocker et diffuser de l'information extra et intra-organisme. Cependant assez flou, ce système socio-technique possède sa propre interprétation selon chaque secteur d'activité, chaque entreprise, chaque service.

L'arrivée des Nouvelles Technologies de l'Information et de la Communication (NTIC) au cœur des organismes a bouleversé les systèmes d'information. La collecte, la mémorisation, le traitement et la diffusion de l'information se réalisent à l'aide des outils informatiques. À travers des supports numériques, il est désormais possible de stocker et conserver un nombre important de données dans un espace réduit, de les dupliquer et de les diffuser de manière très simple. Les organisations se voient désormais exposés à trois grands types de risques au niveau de leur SI :

- L'intégrité de l'information, garantissant l'exactitude des données,
- La confidentialité de l'information, garantissant que seules les personnes autorisées peuvent accéder à l'information,
- La disponibilité de l'information : garantissant que l'information est disponible pour une personne autorisée.

La non-prise en compte de ces critères peut provoquer d'importants dégâts sur le bon fonctionnement de l'organisme et lui porter préjudice ainsi qu'à ses parties prenantes. Des conséquences plus ou moins importantes peuvent alors résulter de ces menaces :

1. Sur Le plan financier, les dommages liés à une cyberattaque sont en moyenne de 300 000 € pour les entreprises de moins de 1 000 salariés et 1,3 million d'euros pour une entreprise de plus de 5 000 salariés [1].
2. Sur les données personnelles, en causant des torts à la vie privée d'une personne ou en diffusant des informations personnelles sur elle. Le nouveau règlement général sur la protection des données (RGPD) obligera les organisations européennes à notifier auprès des autorités compétentes, sous 72 heures, tout cas de risque réel d'atteinte à la protection de la vie privée. Sinon, l'organisation s'expose à des poursuites judiciaires ainsi qu'une amende allant jusqu'à 4% du chiffre d'affaire de celle-ci ou 20 millions d'euros [2].

3. Sur le bon fonctionnement de l'entreprise, il faut savoir qu'une entreprise met environ 9 semaines pour se remettre d'une cyberattaque [1].
4. En termes d'images, la désinformation, la diffamation, la mise en évidence de failles nuisent à l'image de l'entreprise. Certains cas restent fortement médiatisés comme le piratage de Sony Pictures Entertainment [3], les vols de données chez Yahoo, Myspace, Orange [4] ou plus récemment, la faille Meltdown dans les processeurs Intel [5] ...

Toutes ces conséquences et ces risques pour l'entreprise sont essentiellement générées par 3 facteurs :

1. Les causes humaines, divisées en trois catégories :
    - La maladresse humaine, 24% des pertes de données seraient dues aux employés [6],
    - L'inconscience du personnel, de nombreux utilisateurs méconnaissent les risques et introduisent des programmes malveillants au cœur du SI de leur entreprise. Selon une étude commandée par Blue Coat en 2014 [7], 51% des employés utilisent des appareils personnels au travail, 2 personnes sur 5 utilisent les réseaux sociaux pour des raisons personnelles au travail et 20% des sondés ouvrent des emails provenant de sources inconnues, pourtant 73% des interrogés ont conscience de la dangerosité de leur geste,
    - La malveillance, une personne ayant accès au réseau d'un organisme peut l'utiliser pour altérer son fonctionnement ou dérober des informations.
2. Les causes extérieures, pouvant provenir d'un sinistre (vol, incendie, dégâts des eaux) ou d'un problème électrique. La norme ISO/CEI 27001 sur les « Systèmes de management de la sécurité de l'information » apporte les bonnes pratiques en matière de management des systèmes, en évaluant les risques et en les prévenant [8],
3. Les causes techniques, celles-ci sont liées à la défaillance du matériel, son obsolescence ou à la mauvaise migration de données. Des failles de logiciels ainsi que des programmes malveillants peuvent aussi être identifiés.

Une étude indépendante menée pour Robert Half auprès de 100 Directeurs des Système d'Informations (DSI) français [9] montre que ceux-ci pensent que les principaux risques liés à la sécurité de l'information d'ici 5 ans seront la cybercriminalité à 63%, l'utilisation frauduleuse/compromission de l'intégrité de l'information à 52% et le manque de connaissances des salariés en matière de sécurité. Selon un sondage OpinionWay pour Symantec, 81% des entreprises françaises ont été visées par des cyberattaques en 2015. Cette même année, le coût des cyberattaques a été estimé à plus de 3,3 milliards d'euros pour les entreprises françaises [1].

La sécurité du système d'information d'un organisme est devenue un élément central pour le bon fonctionnement de celui-ci. Grâce aux Nouvelles Technologies de l'Information et de la Communication, les organismes produisent, exploitent et stockent de plus en plus de données. L'ensemble des informations est de plus en plus volumineux et rapide mais aussi de plus en plus vulnérable. Une mauvaise sécurisation du SI peut entrainer de graves conséquences au niveau du fonctionnement de l'entreprise. L'information est donc un actif qui, comme tous les autres actifs importants d'un organisme, doit être protégé de manière adéquate.

2) De la sécurité de l'information à la norme ISO/CEI 27001

Afin de garantir au mieux la sécurité de ses informations, un organisme peut mettre en place un ensemble de politiques et processus appelé Système de Management de la Sécurité de l'Information (SMSI), permettant de gérer et coordonner la manière dont la sécurité de l'information est mise en place. Cette approche systémique permet de définir et d'appliquer des mesures garantissant la confidentialité, l'intégrité et la disponibilité de l'information. Il est important de définir un périmètre sur ce genre de dispositif afin de garantir sa réussite. Le référentiel concernant le système de management de la sécurité de l'information le plus connu provient de l'organisation internationale de normalisation (ISO) et de la Commission Electrotechnique Internationale (CEI), qui ont mis en place la famille de normes et lignes directives ISO/CEI 270XX [10]. La norme ISO/CEI 27001:2013 expose les exigences relatives aux systèmes de management de la sécurité de l'information [8]. Elle tire ses origines de la norme britannique BS 7799-2:2002 « *Technologie de l'information – Guide pratique pour le management de la sécurité de l'information* », dont la première version a été publiée en 1999. En 2005, l'ISO l'adopte et l'améliore afin de mettre en place l'ISO/CEI 27001:2005 [11]. Devenue peu à peu un standard, cette norme a été révisée en 2013 et adopte désormais la structure High Level Structure (HLS) [12]. Celle-ci permet de satisfaire les exigences de deux ou plusieurs normes de systèmes de management simultanément en se rapprochant des autres normes de systèmes de management (ISO 9001, ISO 14001…). La norme ISO/CEI 27001 est actuellement en cours de révision depuis le mai 2017 [13].

Au niveau de sa forme, la norme ISO/CEI 27001:2013 comporte 10 chapitres, provenant de la structure HLS classique, et une annexe. Celle-ci est composée de 114 mesures de sécurité issues du document ISO/CEI 27002 « *Technologies de l'information -- Techniques de sécurité -- Code de bonne pratique pour le management de la sécurité de l'information* » [14] . La figure 1 synthétise la mise en place d'un SMSI selon la norme ISO/CEI 27001:2013 à travers une cartographie des processus [15].

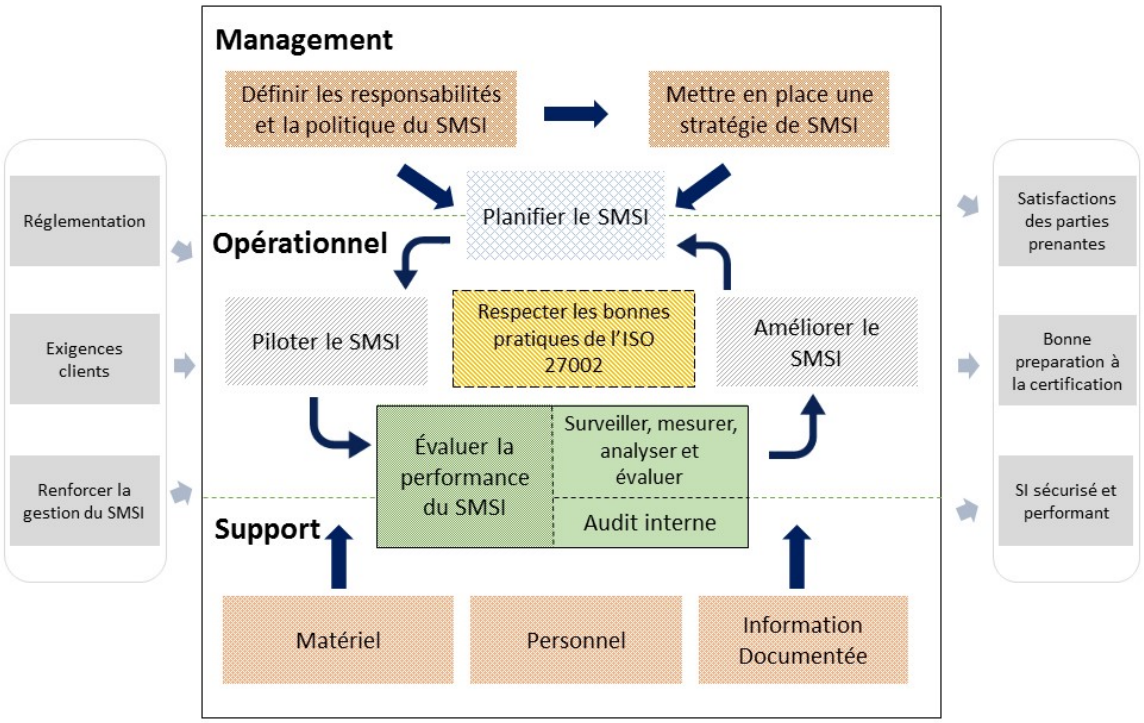

Figure 1 : Cartographie des processus de la norme ISO/CEI 27001 [15]

Selon une enquête de satisfaction des clients certifiés ISO/CEI 27001:2013 réalisée par l'organisme de normalisation British Standards Institution (BSI) [16], ceux-ci estiment que la certification :

- Augmente la confiance des parties prenantes et des clients en garantissant que leurs données sont protégées,
- Identifie et réduit les risques liés à la sécurité de l'information,
- Aide à protéger l'organisation,
- Aide à être conforme aux réglementations, RGPD par exemple [2],
- Améliore la compétitivité en prouvant la conformité et obtenant un statut de fournisseur privilégié,
- Réduit la probabilité d'erreurs liées aux technologies de l'information et de la communication.

La mise en œuvre des exigences de la norme ISO/CEI 27001:2013 permet de sécuriser le système d'information. Tous ces avantages classent l'ISO/CEI 27001 en 4ème position des normes les plus délivrées en 2016 avec un total de 33 290 organismes certifiés et une augmentation de 21% par rapport à 2015 [17]. Ces nombres montrent bien l'intérêt que portent les entreprises face aux problèmes liés à la sécurité de l'information. Cependant cet intérêt semble très disparate. Les pays possédant un nombre important d'entreprises dans les secteurs de l'information et de la technologie comme le Japon, l'Inde ou encore la Chine représentent une part importante des certifications dans ce classement. Ces pays, ainsi que le Royaume-Uni, représentent plus de 50% des certifications, avec une suprématie japonaise. Les pays Européens ne sont pas en reste avec une 5ème et 6ème place pour l'Allemagne et l'Italie. En 24ème position, la France reste loin derrière ses collègues avec moins de 300 organismes certifiés en 2016. La France n'est pas différente de ses voisins européens en termes de sécurité de l'information. Les entreprises françaises ont tendance à valider les bonnes pratiques de la norme sans aller jusqu'à la certification ou en certifiant uniquement un sous-périmètre de l'organisation [18]. Celles-ci prennent donc au sérieux ces problématiques liées à la sécurité de l'information et reconnaissent l'intérêt de la norme ISO/CEI 27001 [19]. Mettre en place une démarche de certification est un parcours long, coûteux et difficile, celle-ci nécessitant d'importantes ressources. Les entreprises françaises préfèrent donc utiliser la norme ISO/CEI 27001 comme un recueil de bonnes pratiques, contrairement au Royaume-Uni où la certification semble indispensable pour la signature de contrats [20]. Afin d'aider les organismes le désirant à se positionner face à cette norme et à estimer leur niveau de conformité, un outil d'autodiagnostic a été développé facilitant l'évaluation et la communication sur les résultats.

3) Un outil d'autodiagnostic pour se positionner

Afin de fournir une vision claire sur le système de management de la sécurité de l'information, l'outil d'autodiagnostic a été conçu à l'aide du logiciel Microsoft Excel©. Son but est d'assister les organismes dans l'évaluation de leurs pratiques en matière de sécurité de l'information. Il leur permet également de se positionner face aux exigences de la norme ISO/CEI 27001:2013. L'utilisateur peut ainsi préparer des plans d'action convenables avec les résultats des évaluations de son SMSI tout en identifiant les priorités à prendre compte.

L'outil d'autodiagnostic est disponible gratuitement sur internet [15]. Celui-ci est composé d'onglets contenant plusieurs éléments ; allant du mode d'emploi à la déclaration de conformité en passant par l'évaluation *(*Figure 2*)*.

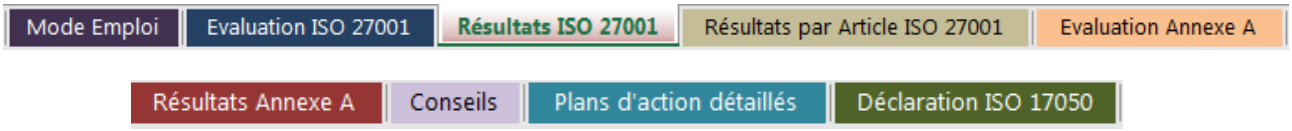

Figure 2 : Onglets de l'outil d'autodiagnostic sur l'ISO/CEI 27001:2013 [15]

{Mode d'Emploi} : cet onglet permet aux utilisateurs de comprendre le fonctionnement des différentes fenêtres et d'expliquer les critères pris en compte lors de l'évaluation. Il renseigne sur les niveaux de véracité [Faux, Plutôt Faux, Plutôt Vrai, Vrai] des critères d'évaluation et permet de pondérer ceux-ci selon le choix de l'utilisateur. Des niveaux de conformité paramétrables [Insuffisant, Informel, Convaincant, Conforme] peuvent aussi être définis par l'utilisateur afin de pouvoir communiquer sur les résultats (figure 3). Cet outil est adaptable à différentes situations et aux stratégies mises en place par les entreprises.

Niveaux de **VÉRACITÉ** quant à la **RÉALISATION** des actions associées aux exigences de la norme			**LIBELLÉS** des niveaux de **CONFORMITÉ** des **ARTICLES** de la norme			
Libellés explicites **des niveaux de VÉRACITÉ**	Choix de **VÉRACITÉ**	Taux de **VÉRACITÉ**	Taux moyen **Minimal**	Taux moyen **Maximal**	Niveaux de **CONFORMITÉ**	Libellés explicites **des niveaux de CONFORMITÉ**
Niveau 1 : L'action **n'est pas réalisée** ou alors de manière très aléatoire.	**Faux**	**0%**	**0%**	**9%**	**Insuffisant**	Conformité de niveau 1 : Il est nécessaire de **formaliser** les activités réalisées.
Niveau 2 : L'action est **réalisée quelques fois** de manière **informelle.**	**Plutôt Faux**	**30%**	**10%**	**49%**	**Informel**	Conformité de niveau 2 : Il est nécessaire de **pérenniser la bonne exécution** des activités.
Niveau 3 : L'action est **formalisée** et **réalisée.**	**Plutôt Vrai**	**70%**	**50%**	**89%**	**Convaincant**	Conformité de niveau 3 : Il est nécessaire de **tracer et d'améliorer** les activités.
Niveau 4 : L'action est **formalisée, réalisée, tracée** et **améliorée.**	**Vrai**	**100%**	**90%**	**100%**	**Conforme**	Conformité de niveau 4 : **BRAVO !** Maintenez et **communiquez vos résultats.**
NB : Vous pouvez modifier les **limites minimales** ci-dessus des intervalles de conformité						

Figure 3 : Paramétrage des critères d'évaluation de l'outil d'autodiagnostic par l'utilisateur [15]

Les onglets d'évaluation {Evaluation ISO 27001} et {Evaluation Annexe A} : Ceux-ci permettent de lister les différents critères de la norme ISO/CEI 27001:2013 et mesures de l'annexe A. Ces critères et mesures sont classés par articles et sous-articles selon le chapitre de la norme et de son annexe. Pour chaque valeur de véracité choisie, l'utilisateur peut visualiser dans la colonne de conformité un libellé expliquant les conditions nécessaires pour valider la conformité de l'action (figure 4). L'onglet d'évaluation de l'annexe A contient également les bonnes pratiques issues de la norme ISO 27002:2013 associées à chaque mesure de l'annexe.

Réf.	Critères d'exigence des articles de la norme	Evaluations	Taux %	Libellés des évaluations	Modes de preuve et commentaires
Art.4	**Contexte de l'organisme**	**Convaincant**	**86%**	**Conformité de niveau 3 : Il est nécessaire de tracer et d'améliorer les activités.**	
4.1	**Compréhension de l'organisme et de son contexte**	**Informel**	**43%**	**Conformité de niveau 2 : Il est nécessaire de pérenniser la bonne exécution des activités.**	
cr 1	Les enjeux internes et externes sont **déterminés** relativement à la **finalité** et l'orientation stratégique de l'organisme	Vrai	100%	Niveau 4 : L'action est formalisée, réalisée, tracée et améliorée.	La finalité et l'orientation stratégique de l'organisme sont explicitées dans la revue de direction de la norme ISO 27001
cr 2	Les **informations** relatives aux enjeux externes et internes sont **surveillées** et **revues** périodiquement	Choix de VÉRACITÉ		Libellé du critère quand il sera choisi	

Figure 4 : Exemple d'évaluation selon les critères associés aux exigences de l'article 5 de la norme ISO/CEI 27001:2013 [source : auteurs]

Les onglets de résultats {Résultats ISO 27001} et {Résultats Annexe A} : Ces fenêtres permettent de visualiser les performances des actions évaluées et leurs degrés de respect par rapport aux exigences de la norme. Afin de fournir une analyse efficace de ces résultats, des interfaces interactives et des diagrammes radar ont été intégrés dans ces fenêtres. Ceci permet une compréhension rapide et une assistance au niveau de la prise de décision. La Figure 5 et la Figure 6 présentent un exemple des résultats générés après une évaluation complète au niveau de l'article 4 et de ses sous-articles associés.

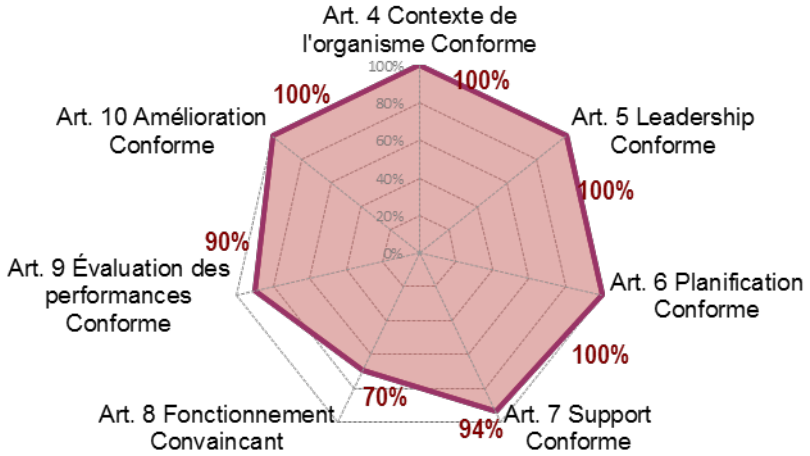

Figure 5: Diagramme radar des résultats de l'évaluation des critères de la norme ISO 27001 [source : auteurs]

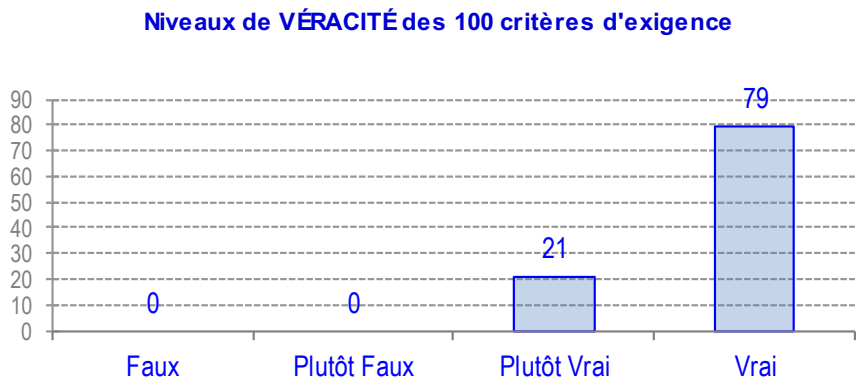

Figure 6 : Histogramme des résultats de l'évaluation des critères de la norme ISO 27001 en fonction des niveaux de véracité proposés [source : auteurs]

{Conseils} et {Plans d'Action Détaillés} : Dans le cadre de l'amélioration continue du système de sécurité de l'information, et après avoir effectué une analyse efficace des résultats générés, les utilisateurs peuvent noter les remarques et les mesures à prendre en compte. Ces onglets peuvent être utilisés au cours d'un audit interne pour aider à construire les plans d'actions convenables avec le SMSI testé.

{Déclaration de la Conformité} : A l'issu de l'évaluation, et au cas où la performance de l'organisme en termes de conformité soit au minimum convaincant, cet onglet propose une déclaration de conformité aux critères d'exigences associés à la norme ISO/CEI 27001: 2013 selon l'ISO 17050 « *Déclaration de conformité selon la norme NF EN ISO 17050 Partie 1 : Exigences générales* » & « *Déclaration de conformité selon l'ISO 17050 Partie 2 : Documentation d'appui (NF EN ISO/CEI 17050-2)* ». La norme ISO/CEI 17050 permet de déclarer ses activités conformes à un référentiel sans recourir à une certification délivrée par un tiers. Cette déclaration a l'avantage d'être gratuite et de pouvoir être réalisée de manière autonome. Celle-ci permet de communiquer en interne afin de valoriser les efforts et ainsi d'obtenir plus facilement l'adhésion et la motivation du personnel [21], [22].

Conclusion

Dans le cadre de la recherche d'une performance optimale et d'un contrôle efficace des processus de sécurisation des informations, les entreprises doivent évaluer régulièrement leurs pratiques concernant la sécurité de l'information. Dans ce cas, la norme ISO/CEI 27001:2013 demeure un support permettant de maintenir l'efficacité et la robustesse du Système de Management de la Sécurité de l'Information.

Un outil d'autodiagnostic, basé sur les exigences de cette norme, constitue une source d'aide gratuite et efficiente pour comprendre les processus de sécurité liés au SI et d'évaluer les actions « sécurité SI » d'une façon rapide, efficace et exploitable [15].

Adaptable et utilisable dans un grand nombre de situations, l'outil d'autodiagnostic est un support pertinent permettant une évaluation rapide et un ciblage des améliorations à apporter au système de management de la sécurité de l'information. Son utilisation apporte à l'organisme une visualisation globale de la sécurité de ses informations et peut offrir un gain de temps appréciable pour l'obtention de la certification ISO/CEI 27001:2013. L'aboutissement de cette démarche renforcera les performances de l'entreprise, sa résilience face aux menaces informatiques, ainsi que la confiance et la fidélité de ses clients.

Déclaration de liens d'intérêts

Les auteurs déclarent ne pas avoir de liens d'intérêts.

Références bibliographiques

[1] « Cybersécurité : la vigilance est de mise ! », *Groupe AFNOR*, 06_25-2018. [En ligne]. Disponible sur: http://www.afnor.org/actualites/cybersecurite-vigilance-de-mise/. [Consulté le: 08-oct-2017].

[2] Alan Calder, *RGPD UE: Guide de poche*. Ed IT Governance Ltd, 2017.

[3] Diane Jean, « Ce qu'il faut savoir sur le piratage géant de Sony Pictures », *Ed. Le Figaro, www.lefigaro.fr*, 18-déc-2014. [En ligne]. Disponible sur: http://www.lefigaro.fr/secteur/high-tech/2014/12/18/32001-20141218ARTFIG00176-ce-qu-il-faut-savoir-sur-le-piratage-colossal-de-sony-pictures.php. [Consulté le: 25-juin-2018].

[4] « Les principaux vols de données personnelles depuis 2013 », *Ed. Le Monde, www.lemonde.fr*, 23-sept-2016.

[En ligne]. Disponible sur: https://www.lemonde.fr/pixels/article/2016/09/23/les-principaux-vols-de-donnees-personnelles-depuis-2013_5002435_4408996.html. [Consulté le: 25-juin-2018].

[5] Martin Untersinger, « Meltdown et Spectre, les deux failles critiques découvertes dans la plupart des processeurs », *Ed. Le Monde, www.lemonde.fr*, 05-janv-2018. [En ligne]. Disponible sur: http://www.lemonde.fr/pixels/article/2018/01/05/meltdown-et-spectre-les-deux-failles-critiques-decouvertes-dans-la-plupart-des-processeurs_5237712_4408996.html. [Consulté le: 25-juin-2018].

[6] « Data Health Check 2015 - Survey Results », *Ed. Databarracks, www.databarracks.com*, 2015. [En ligne]. Disponible sur: http://datahealthcheck.databarracks.com/2015/#3. [Consulté le: 30-janv-2018].

[7] Florian Burnel, « Infographie : La vigilance des employés face aux cybermenaces », *ED. IT-Connect, www.it-connect.fr*, 20-mai-2015. [En ligne]. Disponible sur: https://www.it-connect.fr/infographie-la-vigilance-des-employes-face-aux-cybermenaces/. [Consulté le: 25-juin-2018].

[8] « NF ISO/CEI 27001 - Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences ». Editions Afnor, Paris, www.afnor.org, 27-déc-2013.

[9] « Cybersécurité : ce qu'en disent les DSI français », *Ed. Robert Half, www.roberthalf.fr*, 04-juill-2016. [En ligne]. Disponible sur: https://www.roberthalf.fr/presse/cybersecurite-ce-quen-disent-les-dsi-francais. [Consulté le: 25-juin-2018].

[10] G. Teneau et N. Dufour, « Normes ISO 2700x : vers la gouvernance de la sécurité des systèmes d'information », *Editions T.I., www.techniques-ingenieur.fr*, vol. Environnement-Sécurité, nº ref. G 9 060, 21 pages, avr. 2013.

[11] G. Teneau et N. Dufour, « ISO 27001 : management de la sécurité des systèmes d'information », *Editions T.I., www.techniques-ingenieur.fr*, vol. Environnement-Sécurité, nº ref. : G 9 062, 24 pages, oct. 2013.

[12] Stefan Tangen et Anne-Marie Warris, « Reconfiguration du management - Nouveau format pour les futures normes ISO », *Ed. Organisation internationale de normalisation, www.iso.org*, 18-juill-2012. [En ligne]. Disponible sur: http://www.iso.org/cms/render/live/fr/sites/isoorg/contents/news/2012/07/Ref1621.html. [Consulté le: 25-juin-2018].

[13] « Projet de révision de la norme NF EN ISO/CEI 27001-Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences ». Editions Afnor, Paris, www.afnor.org, 19-mai-2017.

[14] « NF ISO/CEI 27002 - Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour la gestion de la sécurité de l'information ». Editions Afnor, Paris, www.afnor.org, 18-janv-2014.

[15] F. Dumont, S. Jemaï, et Z. Xu, « Management de la sécurité de l'information : outils d'aide au déploiement de la norme ISO/CEI 27001 version 2013 », Université de Technologie de Compiègne, Master Qualité et Performance dans les Organisations (QPO), Mémoire d'Intelligence Méthodologique du projet d'intégration, http://www.utc.fr/master-qualite, puis « Travaux » « Qualité-Management » réf n°423, janv. 2018.

[16] « ISO/IEC 27001 Management de la Sécurité de l'Information », *Ed. BSI, www.bsigroup.com*. [En ligne]. Disponible sur: https://www.bsigroup.com/fr-FR/ISOIEC-27001-Securite-de-lInformation/. [Consulté le: 25-juin-2018].

[17] Laurent Charlet, « The ISO Survey 2016 », *Ed. Organisation internationale de normalisation, www.iso.org*, sept-2017. [En ligne]. Disponible sur: https://www.iso.org/the-iso-survey.html. [Consulté le: 25-juin-2018].

[18] Stéphane Bellec, « Sécurité : faut-il se certifier ISO 27001 ? », *Ed. BFM Business, bfmbusiness.bfmtv.com*, 12-juin-2008. [En ligne]. Disponible sur: http://bfmbusiness.bfmtv.com/01-business-forum/securite-faut-il-se-certifier-iso-27001-384687.html. [Consulté le: 25-juin-2018].

[19] « Cybersécurité : les peurs des entreprises françaises en 2018 », *Ed. Le Figaro, www.lefigaro.fr*, 29-déc-2017. [En ligne]. Disponible sur: http://www.lefigaro.fr/conjoncture/2017/12/29/20002-20171229ARTFIG00197-cybersecurite-les-peurs-des-entreprises-francaises-en-2018.php. [Consulté le: 25-juin-2018].

[20] Theodore-Michel Vrangos, « Les entreprises françaises boudent-elles la certification ISO 27001 ? », 20-juill-2009. [En ligne]. Disponible sur: http://www.journaldunet.com/solutions/expert/40822/les-entreprises-francaises-boudent-elles-la-certification-iso-27001.shtml. [Consulté le: 03-janv-2018].

[21] « NF EN ISO/CEI 17050-1 - Évaluation de la conformité - Déclaration de conformité du fournisseur - Partie 1 : exigences générales ». Editions Afnor, Paris, www.afnor.org, 01-sept-2011.

[22] « NF EN ISO/CEI 17050-2 - Évaluation de la conformité - Déclaration de conformité du fournisseur - Partie 2 : documentation d'appui ». Editions Afnor, Paris, www.afnor.org, 01-avr-2005.