Chapitre 3
La norme ISO 27001

1. Contextualisation de la norme

La norme ISO 27001 est, à l'instar des standards ISO 9001 (qualité) et ISO 14001 (environnement), une norme de gouvernance. La gouvernance étant définie comme le processus qui consiste à contrôler l'utilisation des actifs et ressources pour accomplir la mission de l'organisation. La norme ISO 27001 est dévolue à la sécurité de l'information, et a donc pour objectif d'améliorer la gestion des actifs et des ressources en termes de cybersécurité. Il convient de prendre en considération au premier chef cette essence managériale, et comprendre de prime abord que, loin d'être réservée aux seuls spécialistes de la cybersécurité, elle est destinée plus largement à un public ayant à mettre en place et opérer un système de gouvernance. Dans bien des organisations, des responsables qualité au fait de l'ISO 9001 ont mis en place avec succès une gouvernance sécurité, quand l'appropriation de la norme par des spécialistes techniques de la sécurité s'est avérée plus délicate. Et c'est bien naturel, puisque toutes ces normes de gouvernance présentent un modèle similaire, et spécifient les mêmes règles.

La norme ISO 27001 n'est donc pas réservée à une minorité d'élus spécialistes de la technologie ; elle n'est pas non plus exclusivement réservée à de grands groupes, et bien des PME ont été certifiées ces dernières années, ou ont mis en place avec succès ce modèle de gouvernance. Nous reviendrons sur le côté flexible du standard, sur les possibilités d'amélioration continue qu'il offre et qui le rend adaptable aux budgets plus restreints de structures moins bien dotées.

La norme ISO 27001 fait partie d'un ensemble normatif regroupé sous le sigle ISO 2700X. C'est la seule norme de cet ensemble qui donne lieu à certification, c'est-à-dire que des organismes accrédités peuvent certifier la conformité d'un organisme au standard.

La norme 27001 s'inscrit dans un corpus documentaire plus global, qui comprend essentiellement les éléments suivants :

– ISO 27002 : code de bonnes pratiques pour le management de la sécurité de l'information; il constitue une liste de mesures qu'il est recommandé de prendre en compte pour réduire les risques ou améliorer son niveau de sécurité. Ces mesures constituent l'annexe A de la norme ISO 27001.
– ISO 27003 : guide pour mettre en place la norme ISO 27001.
– ISO 27004 : guide pour la définition d'indicateurs visant à contrôler la pertinence et l'efficacité des mesures mises en place.
– ISO 27005 : guide relatif à la gestion des risques.

2. Rappel historique sur sa construction

Sans être un amateur inconditionnel du duc de Bern, il est des cas où un peu d'histoire permet de donner un éclairage neuf à une situation présente ; et c'est effectivement le cas pour la norme ISO 27001.

La norme ISO 27001 est en fait de naissance britannique, et existait avant son adoption à l'ISO au tournant du siècle en tant que standard BS (*British Standard Organisation*) sous la référence 7799-1 (7799-2 pour ce qui devait devenir ISO 27002). Est-ce cette naissance britannique qui a conduit les Français à adopter une position très réservée à l'égard de ce qui devait devenir le seul standard de sécurité réellement utilisé par le monde ? Peut-être est-ce effectivement lié à une inimitié remontant à Jeanne d'Arc… Peut-être et plus vraisemblablement est-ce lié au côté, non pas libertaire, mais respectueux de la liberté d'entreprendre que peuvent parfois avoir nos voisins d'Outre-Manche et qui nous fait souvent défaut ? Peut-être ce standard est-il beaucoup trop pragmatiquement anglais et heurte le goût français du dogmatisme ?

Le standard est respectueux de la liberté d'entreprendre. Dans la mesure où le système de management est en phase avec les objectifs stratégiques fixés par la direction, où il est conforme aux exigences réglementaires et au cadre contractuel que l'entreprise s'est fixé, il est possible d'agir en toute liberté. On est effectivement loin d'une école de pensée française friande de règles, qui génèrent autant d'exceptions, règles que nous subissons depuis l'école primaire.

Le standard est pragmatique, il définit la démarche à suivre et ne contraint pas le chemin. Il n'impose pas non plus le périmètre à traiter. Une analyse de risques doit être effectuée, le standard ne définit pas de méthode, juste une démarche. Une fois les risques identifiés, l'entreprise est libre de ses choix de traitement dans la mesure où les objectifs, la réglementation et les exigences contractuelles sont respectés. On est loin du dogme, il n'existe pas de vérité absolue, juste des objectifs à atteindre, des risques qui limitent l'atteinte de ces objectifs, et des mesures que l'on peut mettre en place ou non, en fonction de ses moyens, de sa maturité, dans la mesure où l'on tend vers une situation maîtrisée dans un futur raisonnable.

Du pragmatisme, peu de règles, et peu d'enthousiasme de la France, qui connaît un retard assez important dans l'adoption du standard par ses entreprises. Retard qui tend petit à petit à se résorber, mais reste très important au regard des Japonais férus de normes, ou de nations anglophones ayant compris très rapidement les avantages économiques d'une certification.

3. Domaine adressé

La norme 27001 est donc avant tout une norme de gouvernance, appliquée à la sécurité de l'information. Elle permet de définir un Système de Management de la Sécurité de l'Information (SMSI). Il convient alors de définir le sens donné à « sécurité de l'information » : la sécurité de l'information est un processus visant à protéger des données contre l'accès, l'utilisation, la diffusion, la destruction, la modification non autorisée ou l'indisponibilité. Le point important à retenir dans cette définition, en dehors de l'introduction des concepts de confidentialité d'intégrité et de disponibilité qui seront développés ultérieurement, est la composante protection des données : le système de management vise à protéger les données qui le nécessitent, quel que soit leur support (papier, clé USB, espace mémoire, bande de sauvegarde…), qu'elles soient échangées ou stockées… Il convient également de noter qu'il n'y a pas de restriction envisagée quant à la notion de protection : le système de management fera ainsi appel à des mesures physiques (accès aux locaux, caméra…), techniques (sécurité des postes de travail, sécurité des réseaux, des systèmes…), des mesures organisationnelles (recrutement, sensibilisation…) ou des mesures procédurales (définition de politiques, de procédures…).

Cela signifie implicitement, mais il est bon de le souligner, que la mise en place du système de management de la sécurité de l'information va bien au-delà des seules directions informatiques et implique également la direction logistique, la direction des ressources humaines, la direction juridique, etc.

La norme adresse donc la gouvernance de la sécurité de l'information. Mais à qui est-elle destinée ? Si l'on se reporte à la définition première, à toute entreprise concernée par la protection de ses données contre l'accès, l'utilisation, la diffusion, la destruction, la modification non autorisée ou l'indisponibilité. Ce qui concerne, somme toute, l'ensemble des entreprises de la planète. Quelle entreprise pourrait ne pas se soucier d'une perte de son fichier client, d'une indisponibilité de son système de production, d'une modification des données de facturation ou de paie ? Ou de maltraiter les données personnelles qui lui sont confiées ? Il convient de raison garder et d'adopter un peu de pragmatisme. Chaque entreprise devrait se poser les questions suivantes : est-ce que je traite des données sensibles ? Est-ce que ces données sont sensibles au point que leur perte, leur altération, leur indisponibilité auraient un impact conséquent sur ma structure ? Et cet impact est-il conséquent au point que le coût de ma gouvernance sécurité est justifié ? La logique est un peu la même que pour la sécurisation de son appartement. Vais-je investir dans un système d'alarme très sophistiqué si je n'ai pour toute richesse qu'un grille-pain et une télévision ? La réponse est non, évidemment. Sauf si l'on tient résolument à son grille-pain.

À cela s'ajoute le constat suivant, qui a toute son importance : la norme laisse à l'entreprise le choix de son domaine d'application, c'est-à-dire du périmètre sur lequel porte le système de management. En d'autres termes, il est possible, et même tout à fait souhaitable, de circonscrire la portée du système de management aux seuls processus comportant des données vraiment stratégiques pour l'entreprise : l'offre SaaS pour un éditeur logiciel, l'hébergement pour un datacenter, l'activité d'audit pour une société de service… Pour reprendre le parallèle avec la sécurisation de l'appartement, la norme vous invite à choisir la pièce à sécuriser, parce que c'est celle où vous exposez vos tableaux, celle où vous recevez vos invités, votre cave si vous êtes porté sur la bouteille, non, si vous êtes un œnologue averti. L'investissement peut donc être contrôlé et progressif, au sens où il est possible de commencer par un périmètre limité, et de l'étendre par la suite.

L'adoption de la norme peut avoir également d'autres causes que la seule amélioration de la maturité sécurité : obligations contractuelles, avantages concurrentiels, accès à de nouveaux marchés… qui sont abordés dans la prochaine section.

4. Usage actuel de la norme

Dans ses grandes lignes, la norme ISO 27001 incite une organisation à définir un plan d'action afin de se mettre en conformité vis-à-vis des exigences réglementaires et de ses engagements contractuels, et d'atteindre les objectifs de sécurité qu'elle s'est fixée en réduisant les risques par la mise en place de mesures. Elle demande également de contrôler l'efficacité de ces mesures au travers d'indicateurs. Elle demande enfin et surtout de mettre en place ce plan d'action, et d'améliorer les éléments qui demeurent perfectibles au regard des audits, des indicateurs et plus généralement des opportunités constatées. Il s'en suit que la norme invite à améliorer progressivement sa maturité sécurité, en harmonie avec les moyens humains et financiers de l'entreprise. Elle est en cela pragmatique : on constate en effet trop d'organisations qui, confrontées à un référentiel sécurité trop contraignant, abandonnent tout simplement l'exercice ; un peu comme on ne retourne pas dans un club de sport qui vous propose un entraînement inadapté à vos capacités du moment. La norme a cette vertu de se montrer accessible à tous, et de permettre un développement harmonieux et progressif de la maturité sécurité.

Deuxième atout conséquent de la norme : sa cohérence avec les autres standards de gouvernance que sont l'ISO 27001 et l'ISO 14001, et plus généralement les pratiques de management de toute entreprise. Cette cohérence ancre la communication avec le Directeur Informatique ou le Directeur Général en terrain connu. Quel RSSI (responsable de la sécurité du système d'information) n'a pas connu de grands moments de solitude en présentant un budget non argumenté, et pour tout dire peu compréhensible, à sa direction ? Comment justifier une ligne de 30000 euros d'équipements de sécurisation réseau, une autre à 20000 euros pour la sécurisation des postes de travail… ?

La norme permet de placer la relation dans une situation familière à la direction, et ce faisant rend la discussion plus aisée : la direction a fixé des objectifs stratégiques, le RSSI a décliné ces objectifs stratégiques en objectifs de sécurité ; il a analysé les exigences réglementaires, contractuelles, mesuré les risques de ne pas atteindre ses objectifs et propose des mesures, des coûts, un planning, afin d'atteindre lesdits objectifs. Il a priorisé ces mesures et a défini des éléments de contrôle de l'efficacité de celles-ci. Il peut donc en justifier les coûts : telle mesure coûte tant, permet d'atteindre 40 % de mon objectif, sera en place dans huit mois, et nous serons ainsi en phase avec tel engagement contractuel. Il peut également, au travers des indicateurs, reporter à sa direction de l'avancement du chantier correspondant, et montrer l'efficacité de la mesure planifiée au travers d'indicateurs soigneusement choisis. La direction, en retour, peut suivre l'intérêt de son investissement et la cohérence des dépenses effectuées.

4.1 Obtenir la certification ISO 27001

Au-delà de l'amélioration de la maturité sécurité, l'objectif fixé par la direction peut être d'obtenir la certification ISO 27001 sur un périmètre donné. Les motivations incitant une entreprise à aller jusqu'à la certification sont développées dans les paragraphes suivants. Tentons dans un premier temps d'effectuer un point sur le nombre de certifications, même si cela n'est pas chose aisée.

La France atteint en 2018 la vingt-quatrième place mondiale, avec un nombre d'entreprises certifiées peu ou prou au niveau de la Belgique. Le Japon occupe la pôle position mondiale, les pays européens étant somme toute bien représentés puisque l'Allemagne et l'Italie sont dans le top 6.

Notons qu'en 2019, 60 000 sites sont certifiés dans le monde, chiffre à rapprocher de 1 200 000 sites certifiés ISO 9001. On voit que l'écart est encore conséquent quant à l'appropriation des standards par les entreprises. Cependant, les mêmes sources notent une progression sur l'année de 19 % dans le monde, et font même état de 63 % en France.