

Responsable sécurité : à votre norme, prêt, partez !

Management de la sécurité de l'information, implémentation ISO 27001, par Alexandre Fernandez-Toro; éditions Eyrolles; 256 pages; 39 €.

Si la sécurité englobe un grand nombre d'aspects techniques, elle est avant tout stratégique et politique. C'est en amont, avant la mise en œuvre, que tout se joue. La norme ISO 27001, devenue une référence, évite aux responsables de la sécurité des systèmes d'information (RSSI) de se retrouver devant le fait accompli : une installation complètement remise en question car inadaptée ou ne correspondant tout simplement pas aux besoins ou aux exigences de fonctionnement de l'entreprise. Définie sur le modèle de qualité PDCA (Plan, Do, Check & Act), cette norme pose les bases et fixe les exigences dans un document de 34 pages. A partir de ce matériau brut, Alexandre Fernandez-Toro propose un ouvrage didactique qui aide à mieux comprendre en fournissant une grille de lecture. Il rappelle le contexte historique de la norme et, surtout, décrypte les différentes clauses qui la composent. Ce qui intéressera ceux qui souhaitent obtenir la certification ISO 27001. Pour l'auteur, la norme fait peur. Lui-même auditeur de certification et formateur depuis quatre ans sur le sujet, il se veut rassurant, et notamment sur la phase de préparation de l'audit qu'il décrit comme « *encore trop souvent mal vécue* ». ■

