

Certification ISO 27001

CONTEXTE

Depuis quelques années, le volume d'information ne cesse d'augmenter et les systèmes informatiques participent à cette accélération en apportant les bénéfices de la dématérialisation. Les entreprises sont aujourd'hui connectées en interne mais aussi dans le monde entier. De ce fait, leur système d'information est accessible de l'extérieur pour leurs fournisseurs, clients, partenaires et administrations. L'accessibilité par l'extérieur entraîne la vulnérabilité vis à vis d'attaques potentielles. Des menaces telles que les vols d'informations, l'usurpation d'identité, l'intrusion et l'utilisation de ressources systèmes ou encore la mise hors service des systèmes de ressources informatiques sont donc bien présents aujourd'hui. L'investissement dans des mesures de protection et de sécurité est donc indispensable et la mise en œuvre d'un plan de sécurité pour garantir la disponibilité, l'intégrité et la confidentialité de l'information s'impose à toutes les entreprises. Ces plans de fiabilité s'appliquent grâce à des normes telles que l'ISO 27001.

À QUI S'ADRESSE CETTE CERTIFICATION ?

La norme ISO 27001 peut être mise en œuvre autant dans le cadre d'un grand groupe que celui d'une PME (les TPE sont également concernés).

Pour une PME/PMI, ou un petit organisme, son utilisation supposera de gérer une check-list des thèmes de sécurité à traiter et des contrôles à mettre en œuvre afin de constituer une politique de sécurité. Notons que pour que l'approche soit pertinente, il faut commencer la démarche par une évaluation des risques principaux puis par leur gestion. L'intérêt de cette norme est multiple. On peut y voir un avantage commercial (appel d'offre exigeant un niveau de sécurité conforme aux normes) : grâce à cette norme, on instaure aussi un climat de confiance vis à vis de ses partenaires extérieurs, elle permet aussi d'évaluer la valeur de l'information transmise dans l'entreprise...

Enfin, l'intérêt principal est la fiabilité et la sécurité au sein de son système d'information. Plan de continuité d'activité, maîtrise des dépenses informatiques, responsabilisation des collaborateurs.

MISE EN ŒUVRE

L'ISO 27001 permet aux entreprises et aux administrations d'obtenir une certification qui atteste de la mise en place effective d'un système de management de la sécurité de l'information. Cette norme garantit aux parties prenantes (clients, actionnaires, partenaires, etc.) que la sécurité des systèmes d'information permet d'améliorer la confidentialité, l'intégrité et la disponibilité de l'information.