ISO 27001:2013 - Certificat de Systèmes de management de la sécurité de l'information

Introduction

La présente Norme internationale a été élaborée pour fournir des exigences en vue de l'établissement, de la mise en œuvre, de la tenue à jour et de l'amélioration continue d'un système de management de la sécurité de l'information. L'adoption d'un système de management de la sécurité de l'information relève d'une décision stratégique de l'organisation. L'établissement et la mise en œuvre d'un système de management de la sécurité de l'information d'une organisation tiennent compte des besoins et des objectifs de l'organisation, des exigences de sécurité, des processus organisationnels mis en œuvre, ainsi que de la taille et de la structure de l'organisation. Tous ces facteurs d'influence sont appelés à évoluer dans le temps.

Le système de management de la sécurité de l'information préserve la confidentialité, l'intégrité et la disponibilité de l'information en appliquant un processus de gestion des risques et donne aux parties intéressées l'assurance que les risques sont gérés de manière adéquate.

Il est important que le système de management de la sécurité de l'information fasse partie intégrante des processus et de la structure de management d'ensemble de l'organisation et que la sécurité de l'information soit prise en compte dans la conception des processus, des systèmes d'information et des mesures. Il est prévu qu'un système de management de la sécurité de l'information évolue conformément aux besoins de l'organisation.

La présente Norme internationale peut être utilisée par les parties internes et externes pour évaluer la capacité de l'organisation à répondre à ses propres exigences en matière de sécurité de l'information.

L'ordre dans lequel les exigences sont présentées dans la présente Norme internationale ne reflète pas leur importance, ni l'ordre dans lequel elles doivent être mises en œuvre. Les éléments des listes sont énumérés uniquement à des fins de référence.

L'ISO/CEI 27000 décrit une vue d'ensemble et le vocabulaire des systèmes de management de la sécurité de l'information, en se référant à la famille des normes du système de management de la sécurité de l'information (incluant l'ISO/CEI 27003,[2] l'ISO/CEI 27004[3] et l'ISO/CEI 27005[4]) avec les termes et les définitions qui s'y rapportent.

Domaine d'application

La présente Norme internationale spécifie les exigences relatives à l'établissement, à la mise en œuvre, à la mise à jour et à l'amélioration continue d'un système de management de la sécurité de l'information dans le contexte d'une organisation. La présente Norme internationale comporte également des exigences sur l'appréciation et le traitement des risques de sécurité de l'information, adaptées aux besoins de l'organisation. Les exigences fixées dans la présente Norme internationale sont génériques et prévues pour s'appliquer à toute organisation, quels que soient son type, sa taille et sa nature. Il n'est pas admis qu'une organisation s'affranchisse de l'une des exigences spécifiées aux Articles 4 à 10 lorsqu'elle revendique la conformité à la présente Norme internationale.