GUIDE DE MISE EN ŒUVRE DE LA NIS 2

Résumé

Introduction

La directive NIS 2 (Network and Information Security) représente une évolution majeure de la législation européenne en matière de cybersécurité, imposant des obligations spécifiques à un large éventail d'organisations considérées comme essentielles ou importantes pour le fonctionnement de la société et de l'économie. Sa mise en œuvre nécessite une approche méthodique pour assurer la conformité, réduire les cyber-risques et protéger les infrastructures critiques.

Ce guide a été créé pour aider les entreprises à s'adapter au NIS 2, en mettant l'accent sur les différences entre les organisations déjà certifiées ISO/IEC 27001 et celles qui ne le sont pas. L'objectif est de fournir un chemin clair et pratique pour chaque contexte.

Partie 1 : Société certifiée ISO 27001

Les organisations déjà certifiées ISO 27001 partent avec un avantage significatif, car de nombreuses pratiques requises par le NIS 2 sont alignées sur les exigences de la norme ISO/IEC 27001. Toutefois, une approche stratégique est nécessaire pour combler les lacunes et intégrer les obligations réglementaires supplémentaires.

Avantages initiaux pour les entreprises certifiées :

- Structure établie : la présence d'un système de gestion de la sécurité de l'information (SGSI) bien défini facilite l'adaptation aux exigences spécifiques du NIS 2.
- Conformité partielle : des processus tels que l'analyse des risques, la gestion des vulnérabilités et la surveillance continue sont déjà en place.
- Culture de la sécurité : la certification implique une sensibilisation interne accrue à la sécurité informatique.

Principales mesures d'adaptation :

1. Cartographie des exigences supplémentaires de la NIS 2 : identifier les différences par rapport aux exigences de la norme ISO 27001, telles que la gestion de la chaîne d'approvisionnement et l'établissement de rapports à l'intention des organismes compétents.
2. Engagement des parties prenantes : renforcer la collaboration avec les fournisseurs, les partenaires et les autorités afin de répondre aux exigences de la NIS 2 en matière d'établissement de rapports et de résilience.
3. Mise à jour de la documentation : intégrer les processus existants aux nouvelles exigences, telles que la gestion des crises et les plans d'intervention.
4. Test de conformité : comparer l'état actuel du SGSI avec le cadre NIS 2 afin d'identifier et de résoudre les éventuelles lacunes.