Chapitre 3
Les normes ISO résilience-compatibles

1. Introduction

Dans le chapitre précédent, les principaux référentiels et guides de cyber-sécurité utiles pour appréhender et mettre en œuvre la cyber-sécurité/cyber-résilience en entreprise ont été présentés. Ce chapitre s'attache désormais au passage en revue d'un certain nombre (non exhaustif) de normes ISO/CEI indispensables dans une démarche de mise en place d'une politique de cyber-résilience : 27001, 27002, 27005, 27017, 27018, 22301, 20000 et 27701.

2. Les documents normatifs de la famille ISO/CEI

2.1 Normes relatives au management de la sécurité de l'information

2.1.1 ISO/CEI 27001 - Système de management de la sécurité de l'information

Cette norme certifiante est sans aucun doute le pilier de la conformité en matière de gestion de sécurité informatique au sein d'une organisation.

Initialement publiée en 2005 et révisée en 2013 (ISO/CEI 27001:2013), cette norme porte sur la mise en œuvre d'un système de management de la sécurité de l'information (SMSI). Elle est disponible (en version payante) sur le site de l'AFNOR.

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."

Remarque

https://www.boutique.afnor.org/norme/nf-en-iso-iec-27001/technologies-de-l-information-techniques-de-securite-systemes-de-management-de-la-securite-de-l-information-exigences/article/922720/fa187277

Contenu de la norme

Le corpus documentaire est constitué de deux parties :

Articles de 4 à 10

Il s'agit d'exigences relatives aux domaines suivants :

– Contexte de l'organisation
– Leadership
– Planification
– Support
– Fonctionnement
– Évaluation des performances
– Amélioration

Remarque

Dans ces articles, lorsqu'une information précise le terme "documenté", cela signifie qu'il faut produire un document dans un système de gestion documentaire. Il sera demandé comme preuve dans le cadre de l'audit initial. Par exemple, dans la 4.3 - Détermination du domaine d'application du système de management de la sécurité de l'information, il est spécifié : "Le domaine d'application doit être disponible sous forme d'information documentée."

Annexe A

Liste des objectifs et mesures de référence. Il existe 114 exigences (de A.5 à A.18) à respecter scrupuleusement pour obtenir la certification.

Cette annexe se présente de la façon suivante :

Id du thème : thème		
Sous-Id du thème : sous-thème		
Objectif		
Numéro de l'exigence	Description de l'exigence	Mesure à mettre en œuvre

Exemple avec le premier thème de l'annexe A :
Politique de sécurité de l'information

A.5 Politique de sécurité de l'information		
A.5.1 Orientations de la direction en matière de sécurité de l'information		
Objectif : apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.		
A.5.1.1	Politique de sécurité de l'information	Un ensemble de politiques de sécurité de l'information doit être défini, approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés.
A.5.1.2	Revue des politiques de sécurité de l'information	Les politiques de sécurité de l'information doivent être revues à intervalles programmés ou en cas de changements majeurs pour garantir leur pertinence, leur adéquation et leur effectivité dans le temps.

Source : norme ISO/CEI 27001:2013 - Annexe A

Recette d'une gestion de projet réussie

Afin de réussir un projet de certification ISO 27001, plusieurs ingrédients sont indispensables :

- Sponsoring fort de la direction générale avec une lettre de mission claire sur les objectifs à atteindre.
- Définition précise du périmètre (scope) de la certification à venir.
- Choisir le plus tôt possible son organisme certificateur et se renseigner sur le profil des auditeurs.
- Mise en place de formation de sensibilisation à la 27001 auprès d'un ensemble représentatif de Directions métier. Une durée de 2 jours avec une alternance de cours et mises en situation semble une bonne formule.

– Mise en place d'une équipe réduite pilotée par un chef de projet dédié. Cette équipe va interagir avec le commanditaire (la direction générale) et les équipes métier (DSI, RH, Production, Administration des ventes…).
– Élaboration d'un budget primitif (coût de l'équipe projet, coût de la certification, coût de prestations diverses et coût en jours/homme du travail à fournir par les directions métier, coûts des audits internes/externes). Ce dernier point étant le plus délicat à chiffrer. Mais une bonne base de travail consiste à proposer une estimation macro de 5 j/ho par exigences, ce qui représente environ 2,5 ETP.
– Assistance auprès d'une société de consulting extérieure à l'organisation.
– Établissement d'une roadmap trimestrielle pour pouvoir assurer un suivi temporel rapproché.

Remarque

Attention, un bon budget doit prendre en compte une période de trois ans, durée de la validité de la certification. Un audit de renouvellement a lieu chaque année.

Constitution de l'équipe projet

Il existe deux écoles sur le leadership de cette équipe : soit il est porté par le RSSI (responsable de la sécurité des systèmes d'information), soit il est porté par le responsable qualité.

Probablement que le curseur doit se situer au centre et que la meilleure des stratégies consiste à confier les clés de ce projet à un comité de pilotage SSI constitué d'un chef de projet dédié, du responsable qualité, du RSSI et d'un directeur métier. Le RSSI porte la partie *Lead Implementer* (certification homme) et le responsable qualité porte la partie *Lead Auditor* (certification homme).

Remarque

Un projet de certification s'inscrit dans la durée : il faut un minimum d'une année de mise en production d'un SMSI avant de pouvoir prétendre à une certification réussie.

Procédure de certification

La certification se déroule en plusieurs phases.

T0 - 6 mois : gap analysis : il s'agit d'une étape d'audit préalable qui peut être réalisée par une société extérieure. Cette étape sert avant tout à faire le point et à se rassurer sur la feuille de route établie. Tous les documents exigibles doivent être passés en revue ainsi que toutes les exigences. En général, il faut entre 2 et 4 jours pour faire ce gap.

T0 : audit initial

T0 + 1 an : audit de surveillance

T0 + 2 ans : audit de surveillance

T0 + 3 ans : audit de renouvellement

Et ainsi de suite par période de 3 ans.

Chaque audit produit un rapport d'audit comprenant des non-conformités (majeures ou mineures) et des opportunités d'amélioration. Une non-conformité majeure ne permet pas d'obtenir la certification. Les non-conformités mineures doivent être levées par la proposition d'un plan d'action de remédiation pour que la certification soit prononcée.

Remarque

Tous les hébergeurs de données de santé à caractère personnel (HDS) sont soumis à la certification HDS qui impose, en prérequis, de disposer d'une certification ISO 27001 sur le périmètre concerné.

La version ISO/IEC 27001:2022

Une nouvelle version de la norme a été publiée en octobre 2022.

Les principales modifications sont les suivantes :

– Titre de la norme :

La première modification porte sur le titre même de ladite norme : Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information. Il est donc à noter l'introduction de deux thématiques nouvelles par rapport à 2013 : celle de la cybersécurité et celle de la protection de la vie privée.

– Chapitres 4 à 10 :

Chapitre concerné	Nouveauté
4.2 Compréhension des besoins et attentes des parties intéressées	c) Les interfaces et les dépendances existant entre les activités réalisées par l'organisation et celles réalisées par d'autres organisations.
6.2 Objectifs de sécurité de l'information et plans pour les atteindre	Les objectifs de sécurité de l'information doivent : d) être surveillés
8.1 Planification et contrôle opérationnel	L'organisation doit planifier, mettre en œuvre et contrôler les processus nécessaires pour satisfaire aux exigences et réaliser les actions déterminées dans l'article 6, en : – établissant des critères pour ces processus ; – mettant en œuvre le contrôle de ces processus conformément aux critères.
9.1 Surveillance, mesures, analyse et évaluation	L'organisation doit évaluer les performances de sécurité de l'information, ainsi que l'efficacité du système de management de la sécurité de l'information.

Chapitre concerné	Nouveauté
9.2 Programme d'audit interne	Des informations documentées doivent être disponibles comme preuve de la mise en œuvre du ou des programmes d'audit et des résultats d'audit.
9.3 Revue de direction	c) Les modifications des besoins et attentes des parties intéressées, pertinentes pour le système de management de la sécurité de l'information.

Très peu de modifications ont donc été apportées sur la partie « haute » de la norme.

– Annexe A :

Afin de bien comprendre cette annexe A, il convient de se référer à la nouvelle norme ISO 27002 :2022 (article 5 à 8). L'annexe A a ainsi été modifiée en conséquence ; elle est classée selon quatre catégories d'exigences :

– Organisationnelle
– Personnelle
– Physique
– Technologique

ISO 27001:2022
A5 Mesures de sécurité 37 exigences
A6 Mesures de sécurité applicables aux personnes 8 exigences
A7 Mesures de sécurité physique 14 exigences
A8 Mesures de sécurité technologiques 34 exigences
93 exigences