

**ÉCART ANALYSE – Système De gestion du sécurité du information ISO 27001:2022**

- Remarque :**
- 1) là numérotage utilisé sous l'en-tête 'Clause' Et s'occupe de du ISO 27001:2022 ;
  - 2) insérer Le opportun indicateurs (tu vois pied De page) dans Colonnes 'Politique' Et 'Autre document';
  - 3) insérer dans le colonne 'Référence Document' Le référence identifiant de l'autre Document';
  - 4) dans le colonne 'Commentaire', au-delà au commentaires généraux, enregistrer est le commentaires sur l'état Ce le Actions demandes ;
  - 5) **Le texte dans bleu montrer le changements Et le ajouts introduit avec l'édition 2022 de la Normes .**

Prénom Et placer de l'organisation	
Manuel Extension SMSI ou équivalent	
Problème Non.	
Date De libérer	

Clause	Politique	Autre Document	Référence de document	Commentaire
<b>4 Contexte de l'organisation</b>				
<b>4.1 Comprendre l'organisation Et Le son contexte</b>				
L'organisation a déterminé questions externe Et interne Ce Je suis pertinent PourLe son portée Et Ce ils influencent là son capacité De atteindre le résultats attendu de la son système De gestion du sécurité du information? <b>NOTE: Là détermination De ces problèmes Oui rapports au définition de la contexte externe Et interne de l'organisation considéré dans le clause 5.4.1 du ISO 31000:2018.</b>				
<b>4.2 Comprendre le besoins Et le attentes du déclencher intéressé</b>				
L'organisation a déterminé:				
pour) sujets intéressé pertinent Pour Le système De gestion du sécurité du information; Et				
b) le exigences De tel déclencher intéressé pertinent Pour là sécurité du information?				
<b>c) qui De ces exigences sera satisfait par Le système De gestion du sécurité du information?</b>				

4.3 Détermination de la portée de la système De gestion du sécurité du information				
L'organisation a déterminé le limites Et l'applicabilité de la système De gestion du sécurité du information Pour établir Le viseur?				
Dans le déterminer ce portée, l'organisation a considéré:				
pour) questions éd externe interne de référencé point 4.1 ;				
b) le exigences De qui au indiquer 4.2 ; Et				

Clause	Politique	Autre Document	Référence de document	Commentaire
c) interfaces et dépendances entre les activités réalisées par l'organisation Et ceux effectué depuis autres organisations ?				
Le viseur Et disponible comme, comment information documenté?				
<b>4.4 Système De gestion du sécurité du information</b>				
L'organisation a établi, mis en œuvre, entretenu Et amélioré en permanence le système de gestion de la sécurité de information, <b>inclus le processus nécessaire Et là leur interactions</b> , enconformité avec le exigences du norme ISO 27001 ?				
<b>5 Direction</b>				
<b>5.1 Direction Et je m'engage</b>				
Le haut gestion a établi direction Et je m'engage respect au système de gestion de la sécurité de information:				
a) s'assurer que la politique et les objectifs de sécurité de l'informationsécurité de l'information sont établies et sont compatibles avec les direction stratégique de l'organisation ;				
b) garantie l'intégration de la exigences de la système De gestion dusécurité du information dans le processus de l'organisation ;				
c) garantie là disponibilité du ressources nécessaire au système De gestion sécurité des informations ;				
d) communiquer l'importance De un gestion efficace du sécurité du information Et du conformité au exigences de la système De gestion sécurité des informations ;				
Et) garantie Ce Le système De gestion du sécurité du information atteindre le résultats attendu;				
F) à diriger Et soutenir le gens Pour contribuer à l'efficacitéde la système De gestion du sécurité du information;				
g) promouvoir Le amélioration continu; Et				

**GAP ANALYSIS – Sistema di gestione della sicurezza delle informazioni ISO 27001:2022**

<p>h) soutenir autres les rôles exécutif pertinent Pour démontrer là leur direction comme, comment Oui appliquer à leur domaines De responsabilité?</p> <p><b>NOTE Le référence au "entreprise" dans ce document peut être interprété danssens côté Pour indiquer ceux activité Ce Je suis fondamental Pour Le fins d'exister de l'organisation.</b></p>				
<b>5.2 Politique</b>				
<p>Le haut la direction a établi une politique de sécurité d'informations qui :</p>				
<p>pour) Et adéquat au portée de l'organisation ;</p>				

Clause	Politique	Autre Document	Référence de document	Commentaire
b) comprend buts De sécurité du information (voir 6.2) ou fournit Le Carré Pour là définition de la buts De sécurité du information;				
c) inclure un je m'engage pour satisfaire le exigences applicables concernant ausécurité du information; Et				
d) comprend un je m'engage au amélioration continu de la système Degestion du sécurité du information?				
Là politique De sécurité du information Et:				
Et) disponible comme, comment information documenté;				
f) communiqué à l'intérieur de de l'organisation ; Et				
g) pour disposition du déclencher intéressé, pour deuxième de la cas?				
<b>5.3 Les rôles organisationnel, responsabilité Et autorité</b>				
La haute direction s'est assurée que les responsabilités et l'autorité pour les rôles pertinentes pour la sécurité de l'information sont attribuées et communiquées <b>à l'intérieur de de l'organisation ?</b>				
Le haut direction a attribué là responsabilité Et l'autorité Pour:				
pour) garantie Ce Le système De gestion du sécurité du information est conforme au exigences du norme ISO 27001 ; Et				
b) rendre compte à la haute direction sur les performances du système De gestion du sécurité du information?				
NOTE Le haut direction peut aussi assigner responsabilité Et autorité Pour là déclaration de performance de la système De gestion de sécurité du information à l'intérieur de de l'organisation.				
<b>6 Planification</b>				
<b>6.1 Actions Pour affronter des risques Et opportunité</b>				
<b>6.1.1 Général</b>				
Lors de la planification du système de gestion de la sécurité information, l'organisation a examiné les questions visées au point				