Proposition de développement d'un outil de gestion interne du SMSI

Solumada vient de se lancer dans la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme ISO 27001. Que diriez-vous de développer une application interne simple et conviviale, conçue pour centraliser et rationaliser la gestion de la documentation, des responsabilités et des flux de travail du SMSI ?

1. Objectif

L'objectif principal est de créer une plateforme interne qui :

- Centralise les politiques, les procédures et les enregistrements du SMSI.
- Automatise les flux de travail de révision et d'approbation.
- Attribue la propriété et les responsabilités des documents.
- Envoie des notifications en temps opportun pour les révisions et les mises à jour des politiques.
- Maintient les pistes d'audit pour les modifications.
- Améliore la visibilité et la responsabilité du SMSI.

2. Principales caractéristiques

2.1 Gestion des documents et des politiques

- Référentiel central pour tous les documents du SMSI (politiques, SOP, directives, etc.)
- Catégorisation par type, département ou clause (par exemple, ISO 27001 A.5 – A.18)
- Contrôle de version avec historique des modifications
- Télécharger/afficher les autorisations par rôle

2.2 Système d'examen et de notification

- Cycles d'examen configurables (par exemple, annuels, biennaux)
- Rappels automatiques par courrier électronique aux propriétaires et aux réviseurs de documents
- Alertes d'escalade pour les évaluations en retard
- Aperçu du tableau de bord des avis en attente

2.3 Propriété et responsabilité

- Attribuer des propriétaires, des réviseurs et des approbateurs de documents

- Indicateurs d'état (par exemple, Brouillon, En cours de révision, Approuvé, Expiré)
- Registre des approbations avec horodatages

2.4 Journalisation des audits et de la conformité

- Suivre les modifications apportées aux documents, les journaux d'accès et les dates de révision
- Conserver un historique du cycle de vie du document prêt à être audité
- Exporter les journaux pour les preuves d'audit ISO 27001

2.5 Gestion des utilisateurs et des rôles

- Intégration avec l'authentification utilisateur existante (par exemple, SSO, “Active Directory”)
- Accès basé sur les rôles (administrateur, contributeur, réviseur, spectateur)
- Autorisations personnalisables par document ou par service

2.6 Il est important d'inclure ces fonctionnalités (cela serait un peu complexe, mais pourrait être envisagé à un stade ultérieur, ce n'est que mon avis)

- Intégration du registre des risques
- Module de gestion des incidents
- Module d'inventaire des actifs
- **Tableau de bord de conformité (par exemple, statut ISO 27001 clause par clause)**

3. Avantages

- Visibilité et contrôle accrus sur la documentation du SMSI
- Risque réduit de non-conformité en raison de politiques obsolètes
- Amélioration de l'efficacité grâce à l'automatisation
- Collaboration et responsabilisation renforcées
- Préparation aux audits et aux examens internes

CAS D'UTILISATION - Ce sont les principales fonctionnalités que l'application doit être capable d'exécuter

Cas d'utilisation 1 : Télécharger et catégoriser une nouvelle politique

- **Acteur :** Administrateur ou propriétaire de la politique ISMS
- **Description :** Télécharge une nouvelle politique de sécurité des informations, attribue une catégorie (par exemple, A.7 Sécurité des ressources humaines), définit la fréquence de révision et attribue des propriétaires/réviseurs.
- **But :** Assurez-vous que chaque politique est correctement classée et attribuée avec responsabilité et suivi du cycle de vie.

Cas d'utilisation 2 : Rappel de révision et flux de travail d'approbation

- **Acteur :** Réviseur/approbateur de documents
- **Description :** Recevez une notification automatique par e-mail lorsqu'une politique doit être révisée. Le réviseur se connecte, examine le document et l'approuve ou le signale pour mise à jour.
- **But :** Maintenir les documents à jour et répondre aux exigences de révision périodique selon la norme ISO 27001.

Cas d'utilisation 3 : Propriété des documents et journalisation des modifications

- **Acteur :** Tout utilisateur disposant de droits d'édition
- **Description :** Met à jour une politique ou un document. Le système enregistre automatiquement la modification, le numéro de version, l'horodatage et l'utilisateur ayant effectué la modification.
- **But :** Maintenez une piste d’audit sécurisée et un historique des versions.

Cas d'utilisation 4 : Politiques d'accès et de visualisation

- **Acteur :** Employé général ou spectateur
- **Description :** Accède à la plateforme ISMS pour afficher les versions actuelles approuvées des politiques pertinentes pour son département ou son rôle.
- **But :** Assurez-vous que les employés peuvent facilement accéder aux politiques de sécurité applicables.

Cas d'utilisation 5 : Présentation du tableau de bord de conformité

- **Acteur :** Responsable SMSI
- **Description :** Affiche le tableau de bord indiquant l'état de tous les documents ISMS : révisions dues, politiques expirées, couverture de conformité (par exemple, par la clause ISO 27001) et statut de propriété.

- **But :** Évaluez rapidement la santé globale et la conformité du SMSI.

USER STORIES - L'utilisateur doit être capable d'effectuer les tâches suivantes.

Histoire d'utilisateur 1

En tant que responsable SMSI :

Je souhaite recevoir des alertes lorsqu'une politique approche de sa date limite de révision afin de pouvoir garantir des mises à jour en temps opportun et éviter les écarts de conformité.

Histoire d'utilisateur 2

En tant que propriétaire d'une police d'assurance :

Je souhaite pouvoir télécharger de nouveaux documents et attribuer des réviseurs afin que les responsabilités soient clairement suivies dès le début.

Histoire d'utilisateur 3

En tant qu'employé général

Je souhaite rechercher et consulter les politiques pertinentes pour mon service afin de comprendre les attentes et les exigences en matière de sécurité de l'information.

Histoire d'utilisateur 4

En tant que réviseur

Je souhaite pouvoir commenter une politique pendant le processus de révision afin de pouvoir suggérer les améliorations nécessaires avant son approbation.

Histoire d'utilisateur 5

En tant qu'auditeur ou responsable de la conformité

Je souhaite voir l'historique des versions et la piste d'approbation de chaque politique pour pouvoir vérifier l'efficacité des pratiques de contrôle des documents.