Retour d'expérience sur l'obtention d'une certification ISO 27001

Cyberiane Conseil *est une* ***société indépendante*** *dédiée aux* ***enjeux en cybersécurité*** *intervenant sur Nantes et sa région ou en distanciel*

Cyberiane Conseil

Pourquoi mettre en place un SMSI certifié ?

1	**Renforcer la posture de cybersécurité**	*Réduction des risques de cyberattaque*
2	**Structurer la gouvernance de la sécurité**	*Responsabilités clairement définies*
3	**Impliquer durablement la Direction**	*Temps d'écoute régulier avec la direction*
4	**Anticiper les exigences réglementaires (dont NIS2)**	*Première étape de mise en conformité*
5	**Inspirer confiance aux parties prenantes**	*Meilleure crédibilité auprès des clients* *Réponse facilitée pour les appels d'offre*
6	**Professionnaliser et rendre l'organisation plus résiliente**	*Moins d'interruption liés aux incidents* *Meilleure culture cyber*

Cyberiane Conseil *est une* ***société indépendante*** *dédiée aux* ***enjeux en cybersécurité*** *intervenant sur Nantes et sa région ou en distanciel*

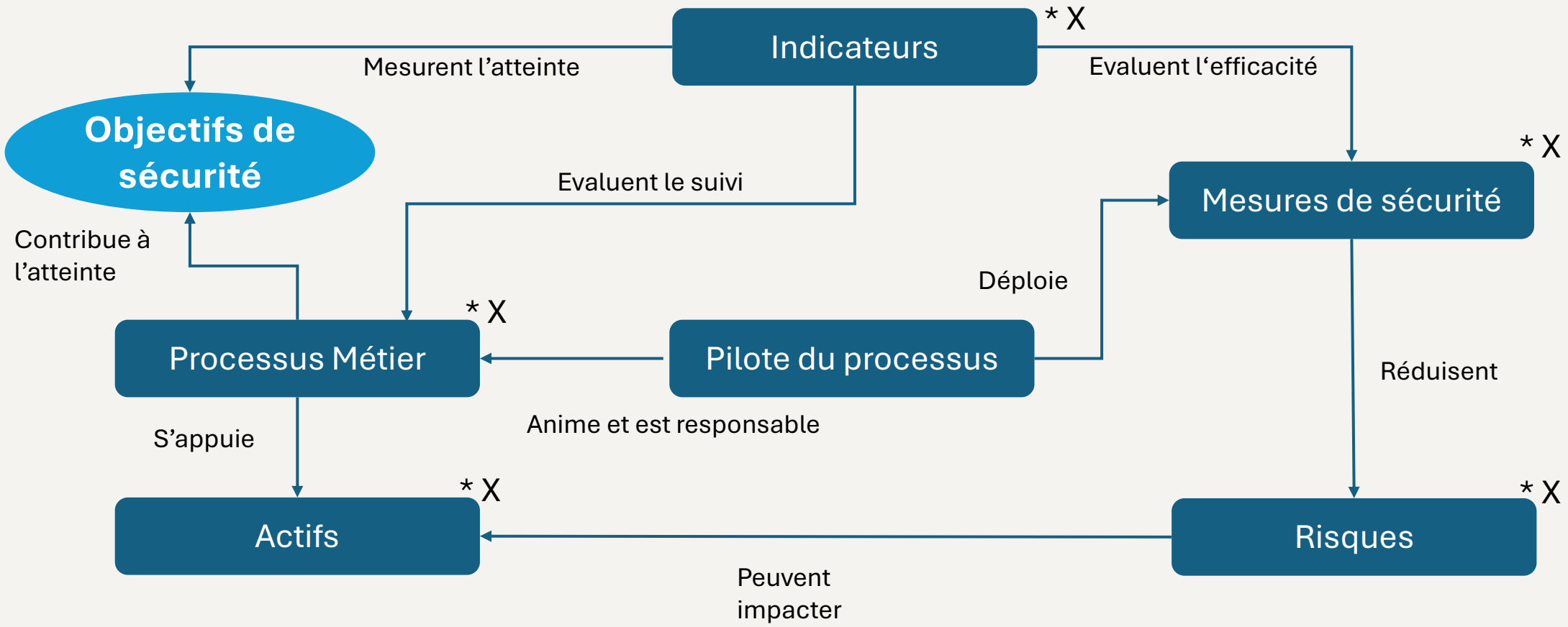
Cyberiane Conseil

Qu’est ce qu’un SMSI certifié ISO 27001 ?

- **Un Système de Management de la Sécurité de l’Information (SMSI)** est un cadre permettant de **gérer et réduire les risques liés à la sécurité de l’information** grâce à une approche de gestion des risques adaptée aux enjeux de l’organisation.
- Il aide à **identifier, évaluer et maîtriser les risques cyber**, en assurant la **confidentialité, l’intégrité et la disponibilité** des informations.
- La norme **ISO 27001** définit les exigences pour **concevoir, déployer et maintenir** ce SMSI dans une démarche d’amélioration continue.
- Elle est **applicable à tout organisme**, quel que soit son secteur ou sa taille, et peut conduire à une **certification**.

Liens entre les différents composants du SMSI

A retenir : L'approche Processus permet l'atteinte des objectifs de sécurité de l'entreprise



Une démarche de certification en 4 étapes

Conception

Définition du périmètre du SMSI,

Cadrage du projet (ressources, planning),

Cartographie des actifs essentiels,

Evaluation des risques,

Formalisation des mesures de sécurité retenues dans la Déclaration d'Applicabilité.

Mise en œuvre

Déploiement des mesures de sécurité retenues :

Mesures techniques, organisationnelles et humaines,

Sensibilisation,

Contrôles et processus.

Surveillance

Vérification de l'efficacité du SMSI via :

Un audit interne,

Une revue de direction,

Un suivi des indicateurs.

Maintien et amélioration continue

Préparation de l'organisation à la certification ISO 27001 du SMSI :

Traitement des écarts,

Mise en œuvre les actions d'amélioration,

Audit de certification.

***Cyberiane Conseil** est une **société indépendante** dédiée aux **enjeux en cybersécurité** intervenant sur Nantes et sa région ou en distanciel*

Cyberiane Conseil

Démarche détaillée de certification du SMSI

Conception	Mise en œuvre	Surveillance	Maintien et amélioration continue
Compréhension de l'organisme et de son contexte	Sélection et conception des mesures	Contrôles, KPI & dashboards	Traitement des non-conformités
Domaine d'application du SMSI	Mise en œuvre des mesures	Audit interne	Amélioration continue
Leadership et approbation du projet	Gestion des informations documentées	Revue de direction	
Structure organisationnelle	Communication		
Analyse du système existant	Plan de formation et sensibilisation		
Politique de sécurité de l'information			
Analyse de risques			
Déclaration d'applicabilité			

Des focus seront effectués uniquement sur les activités sur lesquelles des bonnes pratiques sont à partager.

Cyberiane Conseil est une société indépendante dédiée aux enjeux en cybersécurité intervenant sur Nantes et sa région ou en distanciel

Cyberiane Conseil

Focus sur la compréhension de l'organisme et son contexte

Ce que demande la norme

Il est nécessaire de **comprendre** et **documenter** :

- Le **business** et les **processus clés de l'entreprise** pour mettre en place un SMSI adapté pour protéger les actifs essentiels,
- Les **objectifs de sécurité de l'information** définis par la Direction Générale (focus effectué plus tard sur la slide 'Politique de Sécurité de l'Information'),
- Une **analyse des forces et faibles**, internes et externes de l'organisation,
- Les **parties prenantes internes et externes** en lien avec l'entreprise et leurs **attentes en matière de sécurité de l'information** (employés, clients, etc.).

Mes recommandations

- Documenter tous ces éléments dans un livrable « **Politique du SMSI** ».
- Pour chaque **processus clé** de l'entreprise, rédiger une fiche avec le **pilote du processus**, les **activités sous jacentes** du processus et les **liaisons entre les objectifs de sécurité et ces processus**.
- Privilégier la **matrice SWOT** pour l'analyse des forces et faiblesses de l'entreprise.

Structure organisationnelle

Ce que demande la norme

- La norme demande notamment de **spécifier et documenter les rôles et responsabilités** des intervenants du SMSI en matière de sécurité de l'information.
- En règle générale, un **RACI** est documenté pour répondre à cette exigence.

Mes recommandations

- Ne pas se limiter à réaliser un **copier // coller d'un RACI « générique »** mais matérialiser comment l'organisation **délègue les responsabilités** au sein de l'ensemble de l'organisation afin que la « sécurité » ne soit pas portée seule par le RSSI :
  - **Direction** : définit les **orientations stratégiques et alloue les moyens**.
  - **RSSI** : identifie les **risques**, recommande et met en œuvre les plans d'action validés, **supervise le fonctionnement du SMSI** et agit comme coach auprès des pilotes de processus.
  - **Pilotes de processus** : responsables des **mesures de sécurité relevant de leur périmètre** (ex. : le pilote RH garantit l'intégration des **clauses de confidentialité** dans les contrats).

Focus sur l'Analyse du système existant

- Il est nécessaire de réaliser un **écart de conformité** (gap analysis) par rapport à l'existant vis-à-vis de exigences de la norme afin de **planifier des actions de mise en conformité**.

Mes recommandations

- Un **fichier excel suffit** pour réaliser cet écart de conformité. Toutefois, **j'affectionne l'utilisation de l'outil CISO Assistant** pour son ergonomie et ses dashboards.
- Pour que l'analyse d'écart soit complète, il est primordial de faire l'analyse sur les mesures de sécurité de l'annexe A par rapport au périmètre établi du SMSI et aux exigences contenues dans les articles 1 à 10 de la norme :

Périmètre du SMSI	Objectifs de sécurité	Matrice des compétences	Plan de formation et sensibilisation
Politique de gestion documentaire	KPI du SMSI	CR de revue de direction	Résultats de l'audit interne
Plan de communication	Plan de surveillance	Suivi des non-conformités	Suivi des actions d'amélioration continue

Conception | Mise en œuvre | Surveillance | Maintien et amélioration continue

Focus sur la Politique de Sécurité de l'Information

Ce que demande la norme

- La Direction Générale doit notamment définir des **objectifs de sécurité** dans une **Politique de Sécurité de l'Information (PSI).**
- Ces objectifs doivent être en **cohérence** avec les **missions** de l'organisation, **mesurables** et **compréhensibles** de tous.
- Exemples : Assurer la disponibilité de son SI, Assurer la confidentialité des données, Réduire les incidents de sécurité, etc.

Mes recommandations

- Pour une **première certification** : définir des **objectifs simples et fondamentaux** (Disponibilité, Confidentialité, Intégrité via sauvegardes, etc.).
- Pour des organisations **plus matures** : ajouter des **objectifs liés à l'image de marque** et à la posture cyber externe -> des outils tel que 'Security Scorecard' ou 'Board of Cyber' permettent de scanner les actifs externes de votre société pour faire un état des lieux et donner une note de maturité.
- Intégrer dans une section dédiée les objectifs de sécurité de la PSI dans la PSSI afin d'avoir un seul et même document.

Point d'attention

De base, la **PSI et la PSSI sont deux livrables différents** :

- La PSI présente les objectifs de sécurité.
- La PSSI peut définir les objectifs de sécurité ET les principes et règles de sécurité à respecter pour garantir la sécurité de l'information.

Focus sur l'Analyse de risques

Conception | Mise en œuvre | Surveillance | Maintien et amélioration continue

Ce que demande la norme

- Réaliser une **analyse de risques complète** : identification des risques, stratégie de traitement et sélection des **mesures de sécurité** adaptées (le framework d'analyse de risques n'est pas imposé par la norme)
- Produire une cartographie claire des actifs et des risques associés

Mes recommandations

- Utiliser l'outil de GRC **CISO Assistant** (édité par Intuitem), open source et efficace à mon goût pour :
  - cartographier les actifs,
  - réaliser l'analyse de risques,
  - documenter les traitements et mesures de sécurité.
- J'apprécie aussi la méthode EBIOS RM car elle permet de se concentrer sur les risques cyber et de mettre rapidement de côté les risques physiques, environnementaux, etc., déjà couverts par les mesures de base de l'ISO 27001.
- Une analyse peut être faite sous **Excel**, mais CISO Assistant offre une **ergonomie et une structuration bien meilleures**

CISO Assistant
Extra arms for your cyber security program

Point d'attention

- Pour une analyse réellement exploitable, se limiter à **10–15 scénarios de risques au maximum.**
- Des analyses trop exhaustives (ex. 100 scénarios) nuisent à la **priorisation** et à la prise de décision et prennent trop de temps.

Focus sur la Déclaration d'Applicabilité

Ce que demande la norme

- Lister dans un livrable appelé la **Déclaration d'Applicabilité (DDA)** toutes les **mesures de sécurité de l'annexe A retenues** ou exclues du périmètre du SMSI
- **Justifier de l'inclusion ou l'exclusion** des mesures.

Mes recommandations

Inclure dans la DDA :

- Les **déclinaisons opérationnelles et techniques** (politiques, solutions techniques, etc.) de chaque mesure de sécurité.
- Les **responsables métier en responsabilité** de chaque mesure de sécurité (DSI, RSSI, RH, etc.).
- Les **contrôles prévus** pour chaque mesure de sécurité.

Point d'attention

- En règle générale, **très peu de mesures sont exclues** (1 à 3 mesures). Attention à bien justifier leur exclusion !

Conception | **Mise en œuvre** | Surveillance | Maintien et amélioration continue

Focus sur la Mise en place des mesures de sécurité

Partage de points d'attention & pièges à éviter sur certaines mesures de sécurité.

ID	Mesure	Recommandations
5.1	Politique de sécurité de l'information	Dans la rédaction des politiques, décrire les processus existants de manière fidèle sous couvert d'être en non-conformité.
5.7	Renseignements sur les menaces	Prévoir dans le cadre de l'analyse de risques annuelle une veille sur les nouvelles menaces au travers de la revue des panoramas des nouvelles cybermenaces (Wavestone, ANSSI, ...).
5.8	Sécurité de l'information dans la gestion de projets	Prévoir la mise en place d'un processus d'Intégration de la Sécurité dans les Projets (ISP) intégrant l'analyse des besoins en matière de sécurité par l'équipe RSSI en amont des projets.
5.19	Sécurité de l'information sur les relations avec les fournisseurs	La gestion de la sécurité dans les relations fournisseur peut être intégrée dans le processus d'intégration de la sécurité dans les projets : lors des projets faisant appel à des fournisseurs (SaaS, ...), l'équipe SSI définit les exigences de sécurité avec le métier et contrôle ces dernières dans les Plans d'Assurance Sécurité avec le fournisseur.
5.20	Aborder la sécurité de l'information dans le cadre de l'accord fournisseur	
5.21	Gérer la sécurité dans la chaîne d'approvisionnement des TIC	
5.23	Sécurité de l'information pour une utilisation dans les services cloud	
5.22	Suivi, examen et gestion du changement des services fournisseurs	Prévoir une revue annuelle des clauses de sécurité des fournisseurs les plus sensibles
8.11	Masquage des données	Le chiffrement au repos des données peut permettre selon les cas de figure de répondre à cette exigence.
8.16	Activités de surveillance	L'activité de surveillance vise à analyser les logs afin de remonter des alertes de sécurité sur la base des évènements détectés. La simple journalisation des logs ne permet pas de couvrir cette exigence

Conception | **Mise en œuvre** | Surveillance | Maintien et amélioration continue

Gestion des Informations documentées

Ce que demande la norme

- **Aucun formalisme n'est imposé** pour les politiques, mais il est nécessaire de définir un standard commun pour tous les documents décrit dans une politique de gestion documentaire.
- Ces dernières doivent notamment être **validées par la Direction**, documenter les mises à jour des politiques de manière datée et **indiquer le niveau de confidentialité** des politiques (publique, interne, confidentiel, ...).

Mes recommandations

- Faire **signer la PSSI globale par la Direction**. Les **politiques spécifiques** peuvent être **validées par le RSSI** ou un **comité**.
- Ne pas oublier de **tagguer les documents en provenance de l'externe** de votre organisation.
- Intégrer une cartouche de validation dans les templates de documents (version, valideur, date, niveau de diffusion) pour faciliter les mises à jour mineures et accélérer les cycles de validation.

Modifications	Date de mise à jour	Auteur	Approbateur
xxx	xxx	xxx	xxx

Point d'attention

- Pour aller plus loin sur la gestion des informations documentées, la société 'Feel Agile' a rédigé un guide de bonnes pratiques très détaillé en la matière (https://www.feelagile.com/ressources/le-guide-de-la-documentation-iso-27001).

Conception | **Mise en œuvre** | Surveillance | Maintien et amélioration continue

Focus sur le Plan de communication

Ce que demande la norme

- L'organisation doit définir les **sujets, le moment, les interlocuteurs et les méthodes de communication** liés au système de management de la sécurité de l'information.
- Cette stratégie doit être **documentée**.

Mes recommandations

- Intégrer notamment dans le plan de communication :
  - La **communication des mises à jour des politiques en interne**,
  - La **communication sur les bonnes pratiques** à la suite d'un incident de sécurité,
  - Une **méthode d'évaluation du niveau de satisfaction** des parties prenantes sur le mode de fonctionnement du SMSI.
- **Faire un seul et même document** intégrant les **actions de communication et de sensibilisation** qui peuvent se recouper par moment.

Point d'attention

- Regarder les **besoins en matière de communication des parties prenantes** listées dans la Politique de SMI pour compléter le plan de communication.

Conception | Mise en œuvre | **Surveillance** | Maintien et amélioration continue

Focus sur les contrôles, les KPI et dashboards

Ce que demande la norme

- L'organisation doit contrôler que :
  - Les **processus définis sont bien appliqués** et suivis,
  - Les **processus et dispositifs en place sont efficaces**.

Mes recommandations

- Définir et documenter la **stratégie de contrôles permanents effectués pour vérifier le bon niveau de conformité du SI et des processus de manière** ventilée par mesure de sécurité de l'annexe A en indiquant :
  - La **fréquence des contrôles**,
  - Les **responsables** de la réalisation des contrôles,
  - Les **KPI d'activité** par mesure de sécurité,
  - Les **KPI de performance** par mesure de sécurité.
- Positionner le **RSSI comme auditeur** de la bonne réalisation des contrôles permanents par chaque responsable.
- **Limiter le dashboard à 10 indicateurs maximum** (activité et performance confondu) sur le volet sécurité en liant les indicateurs aux objectifs de sécurité définis par la Direction.

Point d'attention

- **KPI d'activité** = **mesure de l'application du processus** (ex. nombre d'incidents / mois).
- **KPI de performance** = **mesure de l'efficacité du processus** (ex. temps moyen de traitement des incidents).

Conception | Mise en œuvre | **Surveillance** | Maintien et amélioration continue

Focus sur la Revue de direction

Ce que demande la norme

La revue de direction est notamment l'occasion pour la Direction et le Responsable du SMSI de faire le point sur les éléments suivants :

- Les **risques identifiés** dans l'analyse de risques,
- Le **financement et le planning des plans d'action** validés dans le cadre du traitement des risques,
- Les **indicateurs** de **performance** du SMSI,
- Le **traitement** des **non-conformités** issues de l'audit interne.

Mes recommandations

- Organiser un **atelier dédié pour présenter les résultats actualisés de l'analyse de risques** et les plans d'action à valider pour ne pas surcharger la revue de direction.
- Lors de la revue de direction, faire une synthèse des risques mis à jour et du planning du plan d'action validé
- NE PAS OUBLIER DE FAIRE UN **COMPTE RENDU** SUITE A LA REVUE DE DIRECTION

Point d'attention

- **Souvent oublié** dans la revue de direction, il est attendu de présenter un indicateur sur le **niveau de satisfaction des parties prenantes** vis-à-vis du bon fonctionnement du SMSI.
- Une bonne pratique : ajouter un **questionnaire de satisfaction** des parties prenantes vis-à-vis du SMSI.

Conception | Mise en œuvre | Surveillance | **Maintien et amélioration continue**

Non-conformités et actions d'amélioration continue

Ce que demande la norme

- Réaliser un **suivi des non-conformités** relevées lors de **l'audit interne**.
- Réaliser un **suivi des plans d'amélioration continue** identifiés notamment dans le cadre de l'analyse de risques.

Mes recommandations

- Réaliser un suivi distinct des actions de non-conformité et d'amélioration continue.
- Réaliser une **analyse des causes profondes** expliquant les non-conformités et définir des plans d'action pour y **remédier de manière pérenne** suivant les principes du traitement des problèmes de la norme ITIL.
- **Il ne faut pas oublier de définir et documenter les critères d'efficacité des mesures dans les plans d'action, afin de pouvoir évaluer clairement leur efficacité sur la réduction des risques.**

Ressources externes pour aller plus loin

- Les meetings du club ISO 27001 (1 réunion d'échange / trimestre)

- Publication APSSIS : Guide d'implémentation de l'ISO 27001 (Cédric Cartau)

Guide Cyber-résilience - Opus 8 - L'ISO 27001 par étape

- Publication Feel Agile : Guide Documentation ISO 27001 (Thomas De Mota)

https://www.feelagile.com/ressources/le-guide-de-la-documentation-iso-27001

Cyberiane Conseil est une société indépendante dédiée aux enjeux en cybersécurité intervenant sur Nantes et sa région ou en distanciel

Cyberiane Conseil

Découvrir Cyberiane Conseil

- **Cyberiane Conseil** est une **société indépendante** dédiée aux **enjeux en cybersécurité** intervenant sur Nantes et sa région ou en distanciel avec une approche pragmatique et humaine.
- Qui suis-je ? Je m'appelle **Raphael Nonotte-Varly**, consultant cyber senior avec **12 ans d'expérience** terrain et d'engagement sur le territoire.
- Notre objectif : Vos enjeux de cybersécurité sont un labyrinthe => Nous sommes votre GPS, votre fil d'Ariane pour en trouver la sortie.
- **Notre offre de services se structure autour de 4 domaines d'intervention** :

Gouvernance et Conformité Cyber

Assistance RSSI

Pilotage de projets cyber

Cyber-Résilience

06 64 90 70 57

Raphael.nonotte-varly@outlook.fr

Cyberiane Conseil