20 septembre 2012

Certification ISO 27001 des prestations d'audit de sécurité des SI

Retour d'expérience - Extension du périmètre du SMSI

solucom
management & IT consulting

Un SMSI certifié depuis 4 ans

- Le 18 septembre 2008 : Solucom annonçait la **certification ISO 27001**
  - De ses prestations d'audit de sécurité des systèmes d'information
  - Réalisées depuis le site de la Paris – La Défense
- En septembre 2011 : cette certification a été renouvelée après **3 ans d'amélioration continue**
- En septembre 2012 : l'**extension de notre périmètre** a été reconnue
  - Ajout du site de l'agence de Nantes

LSTI®

Certifié NF ISO/CEI 27001:2005

SOLUCOM – Certificat LSTI / SMSI / 128

Agenda

1. Enjeux de la certification de nos prestations
2. Retour sur un SMSI de 4 ans
3. Bilan et perspective

Les audits de sécurité : des missions nombreuses et sensibles

Cabinet Solucom
Conseil en système d'Information et management
près de 1100 collaborateurs

Practice
Sécurité & Risk Management
Toutes les prestations liées à la sécurité de l'information et la gestion des risques
175 consultants

Prestations d'audit de sécurité des SI

- Plus de 150 opérations d'audits par an
  - Des audits organisationnels aux tests d'intrusion
- Une vingtaine de consultants dédiés à l'audit
  - Affectation des ressources suivant les expertises et compétences
  - Appui d'autres consultants du Cabinet
- Des missions « sensibles » pour nos clients
  - Avant tout sur la confidentialité et l'intégrité des traces collectées et des conclusions
  - Dans une moindre mesure, en termes de disponibilité

Pourquoi certifier une activité de Solucom ?

Différencier nos prestations dans le domaine de l'audit

- Prouver à nos clients que nous accordons une importance forte à la sécurité des informations qu'ils nous confient

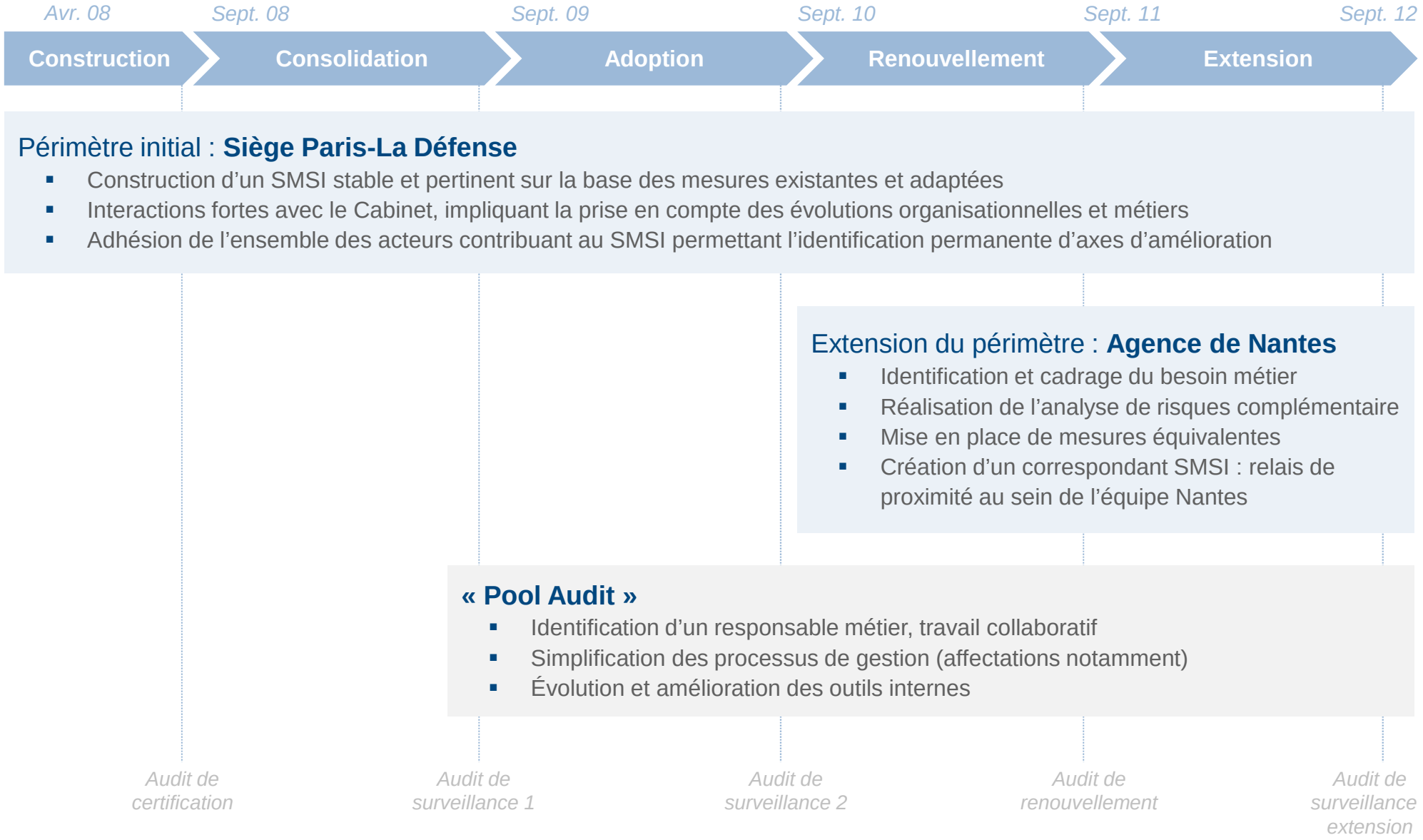
***Mais aussi pour renforcer notre offre de management des risques**, en particulier sur le volet accompagnement aux projets ISO 27001*

« L'homme honorable commence par appliquer ce qu'il veut enseigner » Confucius

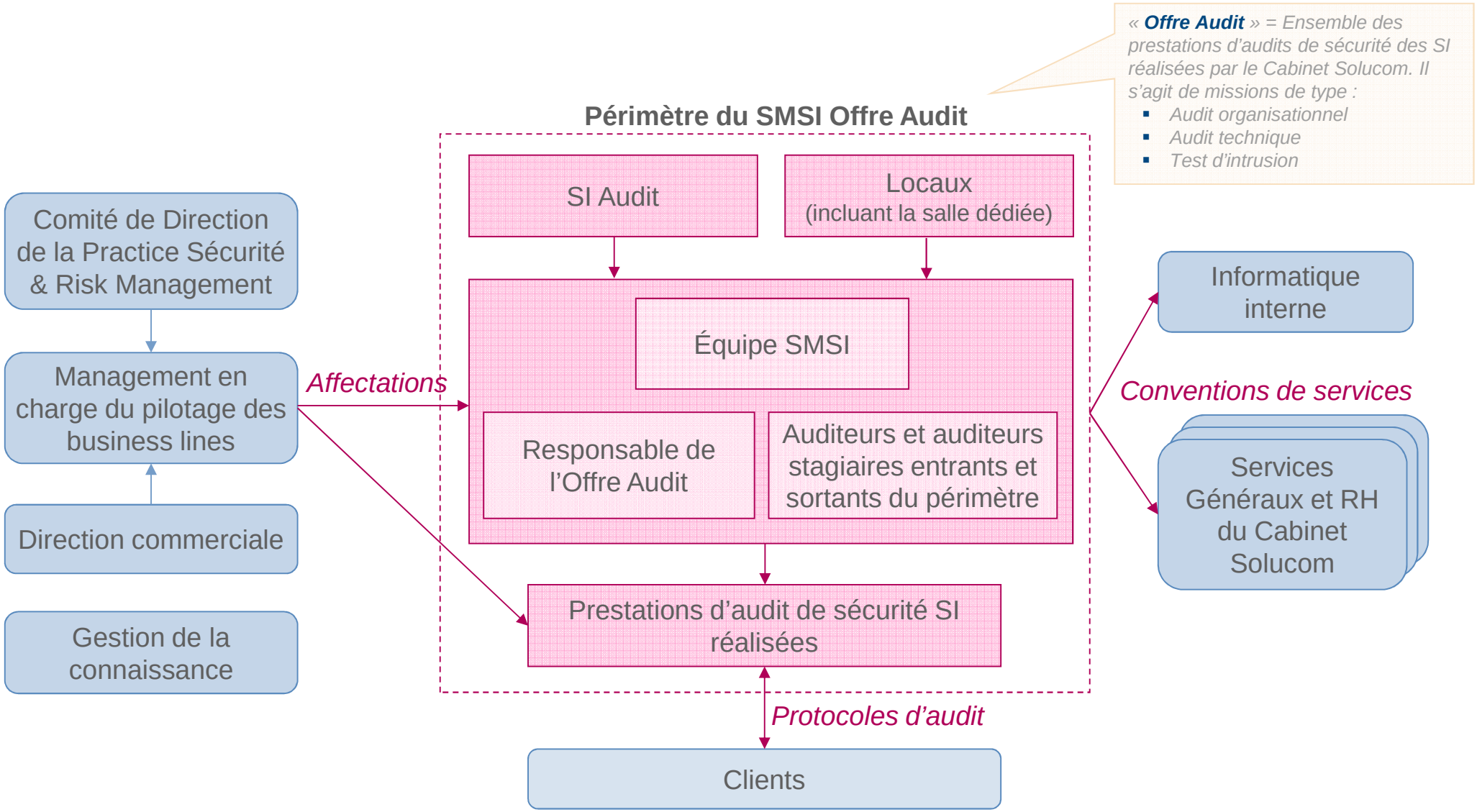
Agenda

1. Enjeux de la certification de nos prestations
2. Retour sur un SMSI de 4 ans
3. Bilan et perspective

Le SMSI Audit Solucom : 4 ans de vie active



Le périmètre de la certification : des interfaces fortement encadrées



Des processus mis en œuvre de façon pérenne

Les processus essentiels du SMSI

Les processus SI et métiers spécifiques

Une analyse de risques qui a su vivre avec le temps

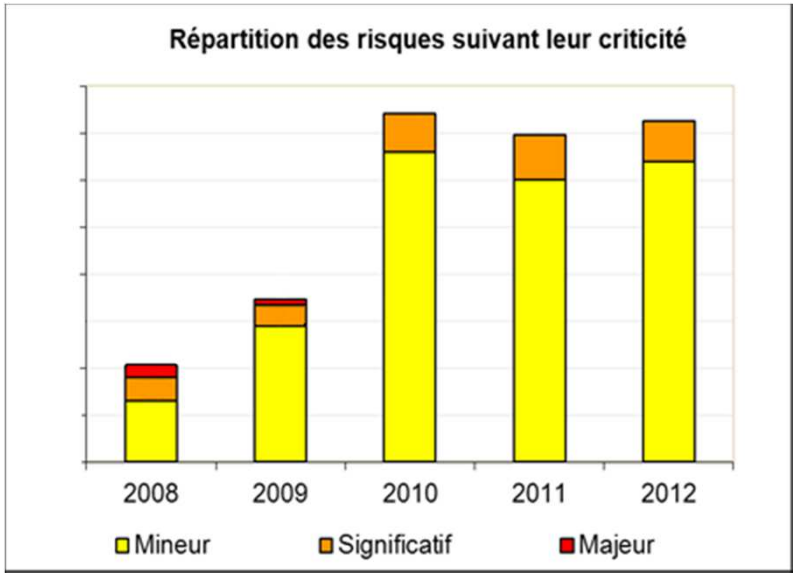
2008
- Première itération

2009-2010
- Prise de recul, granularité plus fine afin de préciser les mesures et les contrôles associés

2011
- Évolution de la méthodologie

2012
- Intégration des actifs nantais et des risques associés

2013 et +
- Optimisation de la cartographie : diminution du nombre de risques et amélioration de leur regroupement afin d'en faciliter la gestion



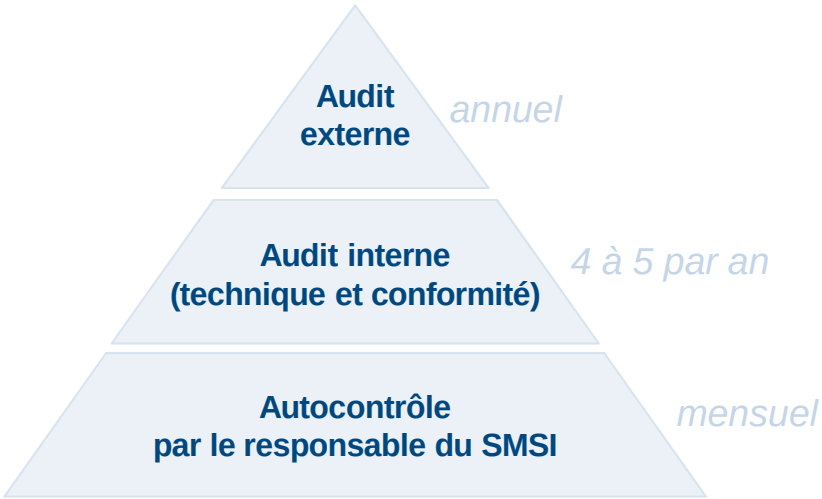
Des mesures de sécurité pour garantir la sécurité de l'information

- Adaptation et pérennisation de pratiques existantes
  - Gestion fine des habilitations
  - Chiffrement des données
  - Protection physique des locaux
  - Infrastructure dédiée au stockage du papier
  - Maintien en condition de la sécurité du SI…

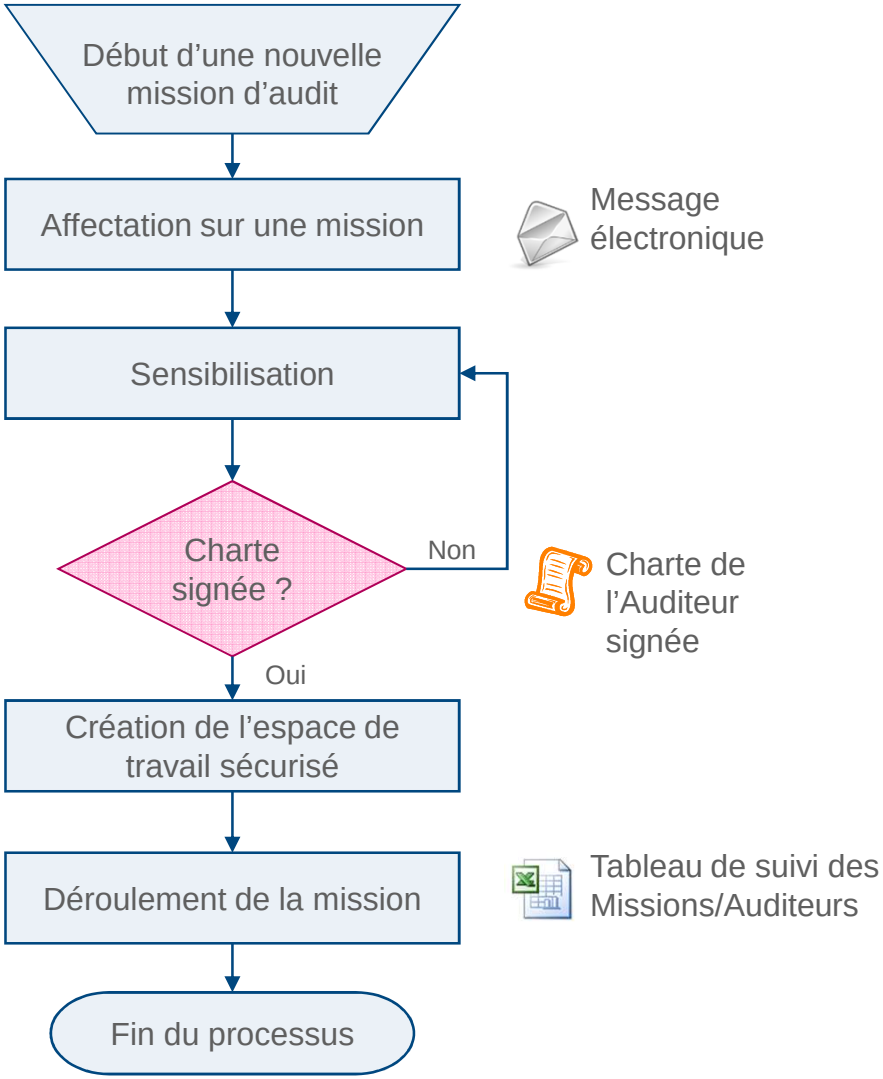
Déclaration d'applicabilité :
115 mesures sélectionnées

Exclusion en particulier des thématiques sur le développement et le commerce électronique

- Mais également la mise en œuvre de nouvelles pratiques « PDCA »
  - Revue formelle avec le management
  - Sensibilisation à la sécurité de l'information
  - Tableau de bord dédié, avec indicateurs d'activité et d'efficacité
  - Focus particulier sur le contrôle :



Zoom sur le processus d'entrée dans le périmètre…

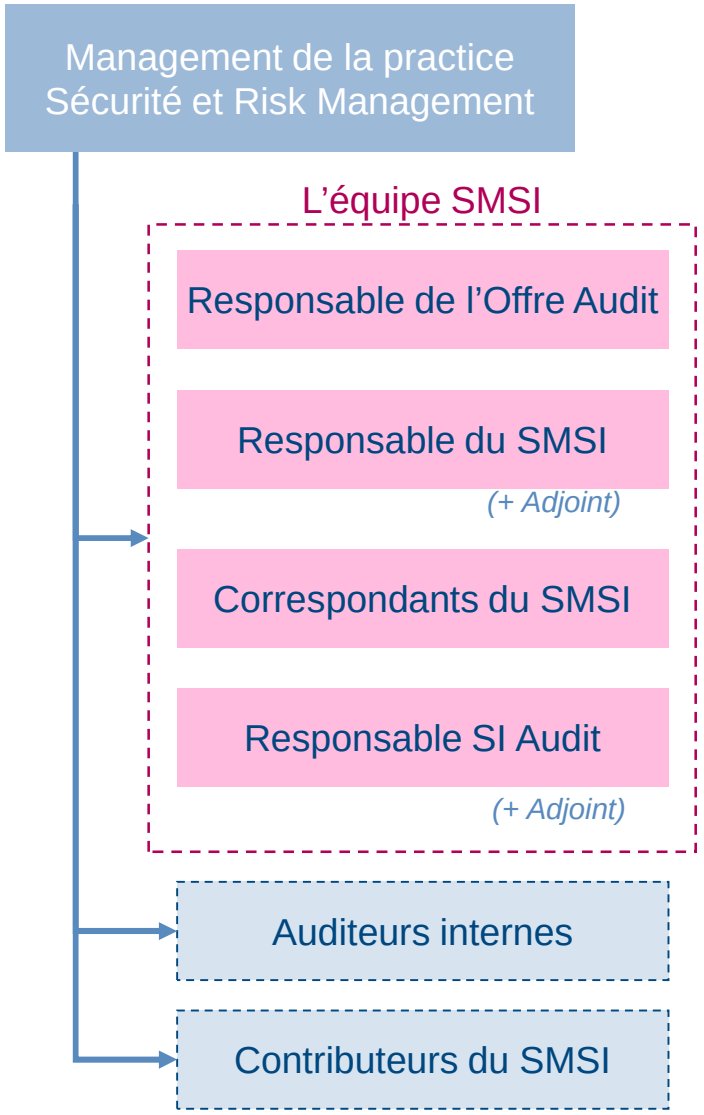


- Des processus équivalents pour la fin des missions
  - Effacement sécurisé des données
  - Destruction des documents…
- Et pour la sortie du périmètre
  - Automatique au bout d'un an sans activité d'audit
  - En cas de mobilité ou de départ de la société

Agenda

1. Enjeux de la certification de nos prestations
2. Retour sur un SMSI de 4 ans
3. Bilan et perspective

Une organisation dédiée au maintien et à l'amélioration du SMSI



- Charges récurrentes : **70 j.h/an** *(+50%)*
  - Suivi du périmètre (gestion des entrées / sorties), mesure de l'efficacité du SMSI, suivi des audits internes et réalisation des revues annuelles
  - Portées par le responsable du SMSI, son adjoint et le responsable du SI Audit
- Réalisation des audits internes : **15 j.h/an**
  - Par les auditeurs internes nommés en fonction des types d'audits
- Projets du plan de traitement des risques et amélioration des processus : **55 j.h/an**

4 ans plus tard, un succès reconnu

Un SMSI pérenne et adopté

- Des consultants impliqués au quotidien dans la vie du SMSI et son maintien
- Une transmission des bonnes pratiques à l'ensemble du Cabinet
- Dynamique forte à l'échelle et de l'activité et du Cabinet

Une volonté d'amélioration continue

- Prise en compte des nouveaux besoins métiers
- Optimisation des processus existants
- Renforcement des mesures de sécurité
- Et d'autres évolutions à venir…

Une intégration de Nantes réussie

- Un correspondant SMSI motivé
- Le support permanent du management local
- Pérennisation des processus et des mesures du SMSI historique

Un succès visible

- Forte activité commerciale sur les audits et l'ISO 27001
- Des clients valorisant nos prestations grâce à la certification

The power of simplicity

«Ce qui est simple est fort»

www.solucom.fr

Contact

Gérôme BILLOIS

Manager

Tel : +33 (0)1 49 03 27 45

Mobile : +33 (0)6 10 99 00 60

Mail : gerome.billois@solucom.fr

Florence LE GOFF

Consultante Sécurité & Risk Management

Tel : +33 (0)1 49 03 27 69

Mobile : +33 (0)6 99 33 69 42

Mail : florence.legoff@solucom.fr