Offre GRC & Cloud Security

in good we trust.

metanext

METANEXT - La Practice GRC & Cloud Security

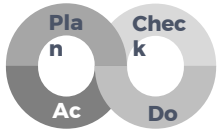
Au-delà des sujets de **Gouvernance**, **Gestion des Risques** et **Conformité liés à la sécurité des infrastructures**, la **practice GRC SSI,** à travers sa composante **Cloud Security** s'est naturellement **bâtie sur plus de 15 années d'expertise et conseil dans la Virtualisation et le Cloud Computing** délivrés au quotidien.

CSEC	GRC	PCA
Cloud Security	**Gouvernance, Gestion des Risques & Conformité**	**Continuité d'Activité**
Confiance numérique des environnements Cloud, sécurisation de la donnée	**Définir un cadre de référence pour gérer la sécurité des actifs informationnels**	**Identifier et sécuriser les services et les activités pour assurer la continuité des fonctions critiques**

La Practice **GRC SSI & Cloud Security** assiste ses clients pour inscrire dans leur l'ADN les notions de **Secure & Privacy by Design** et les **accompagner dans un processus Agile de gestion et d'amélioration continue** de la sécurité.

Vision 360°

Approche orientée risques



Agilité

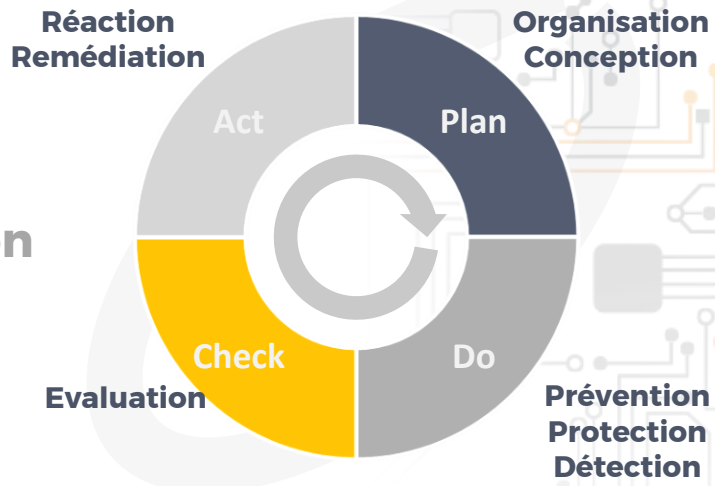
Vos enjeux

La sécurité a pour objectif de **réduire les risques** et vous **prémunir contre les attaques** pesant sur le système d'information, pour **limiter leurs impacts** sur le fonctionnement et les activités métiers des organisations…

La gestion de **la sécurité en tant qu'accélérateur**.

- **Garantir le niveau de protection adapté**
- **Améliorer les usages**, **renforcer l'image** de marque de l'entreprise, **accroitre la confiance**
- **Respecter les contraintes règlementaires** sur le **respect des données à caractère personnel**

Agilité & Amélioration Continue

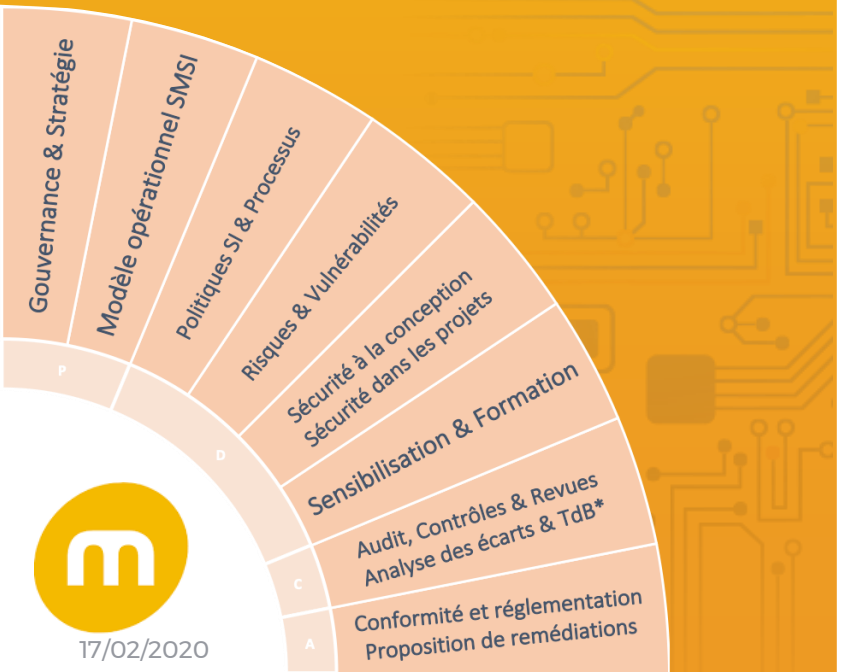


Nos solutions

good solution.

Menaces

1. Une **compréhension** insuffisante **des enjeux** (ex. les risques)
2. **Une gestion insuffisante des coûts** des mesures de **réduction des risques**
3. **Des attaques ciblées** au profit d'une organisation



GRC – Gouvernance, Risques & Conformité

Offre

1. **Stratégie, feuille de route** et investissements
2. **Modèles opérationnels** (Métiers, IT, Architecture, Risques,…)
3. **Politiques, standards et procédures**
4. **Gestion des risques** et **vulnérabilités**
5. **Gestion des processus** et conformité
6. **Intégration de la sécurité** dans les projets
7. **Formation et sensibilisation**
8. **Tableaux de bords**, définition et suivi d'indicateurs

Bénéfices

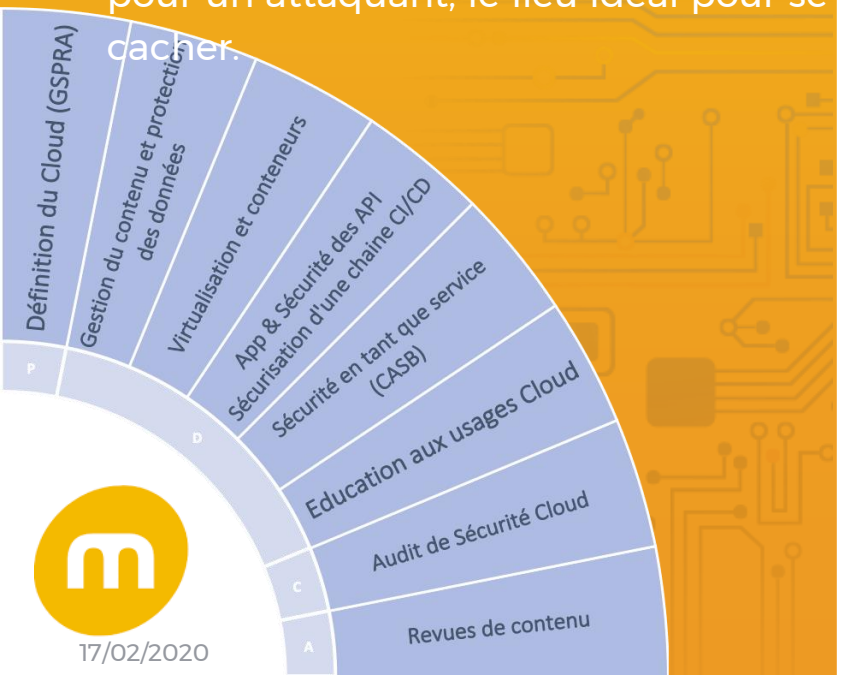
1. Améliorer la **compréhension des enjeux**
2. **Intégrer et partager la sécurité** dans et autour de votre organisation
3. **Security & Privacy by Design - Shift Left**, **Continuous Review** durant le cycle de vie de l'actif (ex. un décomissionnement contrôlé)
4. **Anticiper les menaces** et leurs impacts en apportant des réponses concrètes et suivies dans la **remédiation du risque**

good solution.

CSEC – Sécurité Cloud

Menaces

1. **Des fuites de données, une mauvaise configuration, la gestion des identités et des accès.**
2. **La Vulnérabilité** applicative / socle sous jacent
3. **La Visibilité** de l'utilisation du Cloud / **Shadow IT**
4. **Le MultiCloud et son modèle de responsabilité partagé** est également, pour un attaquant, le lieu idéal pour se cacher.



Offre

1. **Gouvernance, gestion des risques**
2. **Sensibilisation , formation, éducation** à la sécurité
3. **Sécurité des données** (at rest/en transit)
4. **Sécurité des applications et des APIs**
5. **Gestion des accès** et segmentation
6. **Sécurité des conteneurs** et des **environnements virtualisés**
7. **Sécurité des plates-forme** - Modèle Zéro Trust
8. **Conformité et Audit** des plate-formes Cloud
9. **Sécurité** en tant que service **SaaS, PaaS, IaaS**

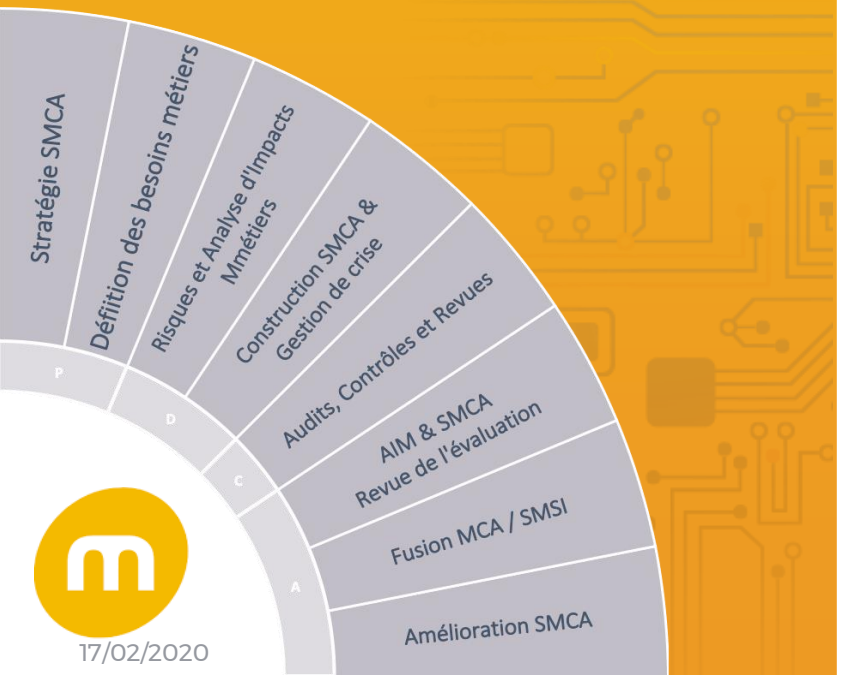
Bénéfices

1. Capacité à atteindre la **conformité et l'uniformité** dans la mise en œuvre **de la sécurité du cloud**, s'affranchir des contraintes règlementaires et d'accréditation
2. **APIs** et chaines **CI/CD** permettent d'**automatiser la sécurité** et les taches **dans le Cloud** et maitriser la **gestion du cycle de vie**
3. **Eviter les erreurs de configuration** pouvant entraîner des fuites de données.

good solution.

Menaces

1. **Une compréhension** insuffisante des **des actifs critiques**
2. Une mauvaise **préparation pour réagir** à la propagation d'un **incident impactant** fortement l'activité
3. **Des processus mal ajustés** pour réagir à des incidents transverses (pandémie, coupure électrique générale, …)



PCA – Continuité

Offre

1. **Formaliser la stratégie** SMCA/PCA
2. **Analyser l'impact et les risques** sur l'activité
3. **Comprendre les exigences**
4. **Identifier les écarts**
5. **Coordonner et maintenir** la mise en œuvre
6. **Contrôler** et suivre toute la chaine de **construction du SMCA ou du PCA**
7. Assister les **revues annuelles**
8. Assister votre **démarche de certification**

Bénéfices

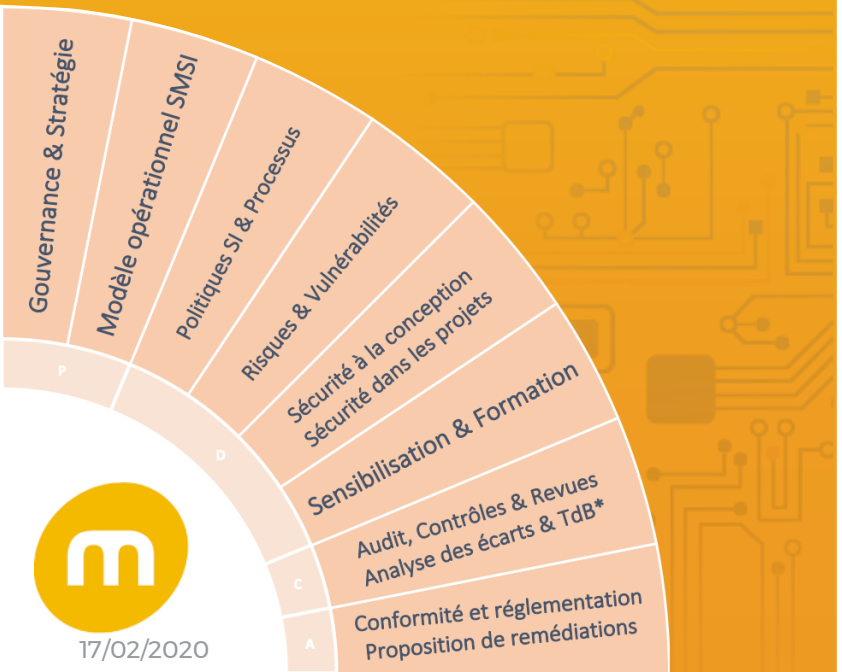
1. **Assurer la continuité** partout au sein de votre entreprise
2. **Réduire les risques** avec une vision claire des impacts
3. **Définir, mettre en œuvre, maintenir et améliorer un SMCA**
4. **Assurer la conformité** avec la politique de continuité d'activité
5. **Certifier son SMCA** par un organisme de certification accrédité
6. **Auto-évaluer** sa conformité

good solution.

GRC – RSSI Temps Partagé

Menaces

1. Evolution du périmètre
2. Une **compréhension** insuffisante **des enjeux** (ex. les risques Métiers)
3. Compréhension des **modèles de responsabilités partagées**
4. **Gestion des priorités** – Approche par les risques



Contexte

1. **Facteurs expositions/environnements/menaces**
2. **Exposition face aux menaces**
3. **Démontrer les apports de la sécurité en tant que « coût nécessaire »**
4. **Avantage concurrentiel (efficacité et résilience)**
5. **Accélérateur de conformité interne et externe**
6. **Catalyser l'innovation**

Offres

Intervention au forfait (projet, périmètre défini) ou en régie – temps complet ou partagé

1. Evolution / mise à jour de **politique de sécurité** – **Déclinaison opérationnelle**
2. Mesure et **amélioration continue de la posture sécurité**
3. **Cartographie des risques** Gestion & analyse de risque
4. Audit et **accompagnement conformité interne et externe**
5. Cycle de **vie de la donnée**
6. Sensibilisation à la sécurité
7. Accompagnement certification ISO 27001

Références Grands Comptes

THALES

Sécurité des usines de développement

Accompagnement du RSSI Group sur la définition d'un modèle de **gouvernance des environnements de Développement**.

- Recensement des plateformes WW.
- Design des architectures des services de sécurité.
- Création d'un catalogue de service.

#GRC #shadow IT #PSSI #Catalogue de services

AXA

Gouvernance des données

Accompagnement du RSSI AXA GIE dans ses projets de protection des données sensibles.

#GRC #Data #Classification

GROUPE BPCE

Conformité réglementaire - LPM

Identifier les chantiers urgents relatifs à la réglementation LPM et RGPD, assister les processus d'homologation, partager la démarche avec l'Agence Nationale de la Sécurité des Systèmes d'Information

#GRC #LPM #RGPD #Conformité

SOCIETE GENERALE

Sécurité des développements Cloud Platform

Assistance RSSI GTS – Intégration Securité@Scale dans le développement de solutions PaaS et IaaS en environnement Cloud public et privé – DevSecOps.

#Sécurité #Cloud #DevSecOps #Classification

SAINT-GOBAIN

SMSI Sécurité

Revoir à la hausse l'ensemble des **exigences sécurité du groupe** à travers le projet de transformation digitale des applications WEB, infrastructure locale et cloud public, assurer la relation fournisseur

#SMSI #Cloud #Web #Infra #SOC

metanext

Satisfaction Client

Présentation de nos activités sécurité

- Architecture sécurité
- Assistance RSSI
- Audit de sécurité
- Gestion des accès
- Gestion de crises
- Gestion des identités
- Gestion des incidents
- Gestion d'un SIEM
- Plan de continuité
- Sécurité des applications
- Sécurité d'architecture
- Sécurité réseaux
- Sécurité des sites
- Sécurité des terminaisons
- Sécurité de la transformation

Les références

Grands comptes et ETIs

metanext

Société Générale

Intégration de la sécurité dans les solutions Infra as Code PaaS et IaaS (DevsecOps).

Contexte

Accompagnement du RSSI GTS Société Générale pour l'intégration de la sécurité – Security@Scale dans le développement de solutions PaaS et IaaS en environnement Cloud public et privé **– DevSecOps.**

Enjeux

- **Evangéliser la sécurité** des développements logiciels / approche « Security by Design »
- **Accompagner les équipes** de développement
- **Valider le niveau de sécurité** des plateformes IaaS et PaaS développées.

Solutions

- Accompagnement à l'**intégration de la sécurité sur les plateforme IaaS et PaaS - DevSecOps**
- **Définition des exigences de sécurité** en fonction du contexte (cloud public / privé, règlementations Métiers,...)
- **Déclinaison des modèles de validation** sécurité des produits et solutions
- Implémentation de l'**outillage DevSecOps**
- **Analyse de Risque** et **Dossier de Sécurité**

Bénéfices

- Nouvelles **plateformes IaaS et PaaS mises à disposition** de la SG et de ses entités.
- **Amélioration du niveau de sécurité** des solutions développées (critères DICP)
- **Intégration de la sécurité dans la chaine CI/CD** et **automatisation du workflow sécurité** dans les projets
- **Réduction des coûts de gestion** sur les activités de RUN sécurité
- **Sensibilisation** des équipes à la **culture sécurité**
- **Vitrine technologique** Groupe
- **Modèle de collaboration des équipes** cité en exemple
- **Validation d'une ligne de 67 produits Cloud** (privé et public)

AXA GIE

Data Classification et Data Leakage Prevention

Contexte

Accompagnement du RSSI AXA GIE dans ses projets de protection des données sensibles.

Enjeux

- **Mettre en conformité** des environnements **vis-à-vis de la PSSI AXA Group**
- **Protéger les des données et le patrimoine informationnel AXA GIE**
- **Analyser les écarts** vis-à-vis des normes et de la PSSI
- Faire **remonter les indicateurs d'avancement** projet
- **Fournir les preuves** et assistance à l'audit interne

Solutions

- Exercice de **Data Classification**
  - Interview des Métiers
  - Validation des inventaires
  - Suivi d'avancement et reporting
- **Définition & optimisation des règles de DLP**
  - Suivi des mesures de protection à mettre en œuvre
  - Récolte de preuves
  - Reporting

Bénéfices

- **Mise en conformité** AXA Group
- **Identification des données** Crown Jewels (10% du total des données)
- **Identification des DCP**
- **Couvrir les risques de non-conformité**
- Mettre en œuvre des **mécanismes de protection adaptés** aux enjeux et risques à couvrir
- **Remonter les sujets de Data Classification** au niveau du COMEX

SAINT GOBAIN

Assistance sécurité programme CIRRUS

Contexte

Assurer à minima, la conformité aux exigences de sécurité du groupe Saint-Gobain dans le cadre du projet de migrations des applications WEB

Enjeux

- **Accompagnement sur les aspects sécurité** à la signature du contrat
- **Valider le niveau de conformité des applications** à migrer chez Claranet
- **Valider le niveau de sécurité de l'infrastructure** Claranet
- **Valider le niveau de sécurité de l'infrastructure Cloud Publique**
- **Evaluer les risques** des solutions de sécurité, de l'obsolescence des actifs
- **Coordonner la relation** entre les SOC Claranet et Saint-Gobain
- **Gérer les processus de détection et de réaction** dans le programme CIRRUS (On-Premise et Saint-Gobain)

Solutions

- **Définition du plan de sécurité** du programme Cirrus
- **Suivi des risques de fuite de données dans les outils en mode SAAS** de support projet
- **Suivi de conformité des exigences sécurité côté fournisseur** (Visite DataCenter, vérification de la prise en compte de la politique de sécurité de Saint-Gobain)
- Suivi de la **mise sous protection applicative IMPERVA** des applications exposées
- **Définir les contrôles et les indicateurs de sécurité** dans le programme CIRRUS

Bénéfices

- **Consolidation des mesures et moyens de sécurité au sein de la DSI centrale**
- **Définition des exigences de sécurité Cloud**
- Migration **GoToCloud**

BPCE-IT

Mise en conformité dans le cadre des règlementations LPM et RGPD.

Contexte

- Dans le cadre de sa démarche de mise en conformité, BPCE-IT a la nécessité d'identifier les chantiers urgents relatifs à la réglementation LPM et RGPD

Enjeux

- **Auditer** les environnements DataCenter
- **Analyser les écarts** vis-à-vis des normes et des règlementations en vigueur
- **Obtenir un état des lieux** clair et exhaustif quant à la complétude des projets de conformité déjà lancés
- Etablir un **plan d'action de mise en conformité** à court, moyen et long terme
- Faire **remonter les constats les plus critiques** à la direction générale en **collaboration avec le service d'audit interne.**

Solutions

- Réaliser un **audit documentaire** afin d'avoir une base de comparaison
- **Superposer le cadre normatif avec le périmètre concerné** (DataCenter) afin de **lister les points de contrôle**
- Mener les **entretiens avec les parties prenantes**
- Etablir une **matrice des risques** incluant les risques de non-conformité
- Réaliser des **visites des Datacenters** de Paris et Castres

Bénéfices

- **Couvrir les risques de non-conformité**
- **Protéger** d'une manière efficace **les données à caractère personnel** hébergées dans les datacenters
- Produire le **dossier d'homologation ANSSI sur la partie LPM**
- **Entretenir et gérer des échanges avec l'ANSSI** sur les nouvelles vulnérabilités concernant les SIIV BPCE-IT
- **Remonter les sujets RGPD et LPM au niveau du COMEX**

Merci

in good we trust.

metanext