

Ready for Cloud ?

L'accompagnement VeriSafe pour assurer la sécurité de vos données dans le Cloud

Présentation

Bien que l'adoption du Cloud computing progresse en France, la sécurité constitue toujours le principal obstacle. Pour aider les entreprises à franchir le pas, Verisafe lance **Ready for Cloud**, une offre de conseil et d'accompagnement dédiée à la sécurité dans le Cloud computing. Avec **Ready for Cloud**, vous serez en mesure d'identifier les risques, de construire une matrice MERC (Matrice d'Evaluation des Risques dans le Cloud), de sélectionner les bonnes mesures de sécurité (ISO 27017, CCM, CASB, cyberassurance), de classer vos données, de rédiger une politique de sécurité Cloud, d'identifier vos obligations réglementaires, d'évaluer la sécurité des fournisseurs, de déterminer les indicateurs de sécurité pertinents, d'utiliser la méthodologie EFICAS (Evaluation Formelle de Cloud pour l'Adopter en toute Sécurité) et de négocier les clauses contractuelles de sécurité indispensables.

L'offre « Ready for Cloud »

- **100% personnalisée sur vos projets Cloud**
 - Contraintes légales ou sectorielle spécifiques
 - Criticité des données
 - etc...
- **Tarif forfaitaire**
 - De 5 à 30 jours/homme selon le périmètre de la mission
- **Réalisée par des experts**
 - Expert sécurité Cloud certifié (CCSP, CCSK ou ESC)
 - Avocat spécialisé IT & Cloud

Ready for Cloud ?

Quelques exemples de missions d'accompagnement

Gestion des risques

- Définir un modèle de classification des données adapté au Cloud et identifier les données éligibles selon leur classification, la localisation des datacenters et le type de service (IaaS, PaaS, SaaS)
- Cartographier les risques dans le Cloud et construire une grille de tolérance adaptée à votre organisme
- Réaliser une analyse de risques pertinente dans un contexte Cloud
- Former à la méthodologie EFICAS (Evaluation Formelle et Indépendante du Cloud pour l'Adopter en toute Sécurité)
- Définir la matrice MERC (Matrice d'Evaluation des Risques dans le Cloud) selon vos exigences de sécurité
- Identifier l'ensemble des mesures de sécurité disponibles pour sécuriser les données dans le Cloud (ISO 27017, ISO 27018, Matrice CCM et solutions CASB)

Conformité réglementaire

- Identifier les obligations réglementaires sur la sécurité de l'information qui impactent les usages du Cloud
- Identifier les obligations légales sur la protection des données à respecter dans le Cloud

Evaluation de la sécurité

- Evaluer la sécurité des fournisseurs Cloud selon 5 axes : audit, test d'intrusion, questionnaire, P.A.S et certifications
- Identifier les indicateurs de sécurité pertinents et définir un plan de contrôle continu sur toute la durée du contrat

Contrat

- Etablir les exigences contractuelles d'un contrat Cloud : respect du cadre légal, SLA, responsabilité des parties, réversibilité, sécurisation des données, gestion des accès, clause d'audit, ...
- Définir les rôles en interne (RSSI, Service juridique, DSI, métiers) pour une négociation contractuelle optimale avec les fournisseurs
- Identifier les contrats de cyber-assurance adaptés au cloud afin de pallier à des pénalités insuffisantes du fournisseur ou de prendre en charge les conséquences financières d'un incident de sécurité

Accompagnement des utilisateurs

- Former les métiers aux risques associés au Cloud et aux bonnes pratiques
- Rédiger une politique de sécurité pour les achats de services Cloud
- Rédiger un guide de bonnes pratiques de sécurité à l'intention des utilisateurs du service Cloud