

Mission d'audit interne des contrats d'acquisition et de maintenance des Assets IT du Groupe

Objectif 1 : S'assurer de l'existence d'un cadre formel et procédural commun permettant de couvrir les aspects liés à l'acquisition et la maintenance des Assets IT du Groupe :

1.1 Obtenir les procédures/notes ou tout autres documents cadrant le processus d'acquisition et de maintenance des Assets IT du Groupe ; si existant :

- S'assurer que le processus est couvert de bout en bout par ces procédures et l'ensemble des assets IT (physiques et logiques),
- S'assurer que les procédures sont partagées avec les parties prenantes concernées,
- S'assurer de l'existence de canevas de contrats d'acquisition et de maintenance des Assets IT,

Risques :

- Défaillance et déficience du processus d'acquisition et de maintenance
- Non optimisation des coûts
- Non atteinte de l'excellence opérationnelle des opérations de maintenance

1.2 Obtenir la liste des Assets IT et leurs contrats d'acquisition et de maintenance (de la CMDB mise en place) :

- S'assurer que l'ensemble des Assets sont couverts par des contrats signés et validés par les parties prenantes concernées (Juridique, achat, DSI...) ;
- Sur la base sur d'un échantillon : S'assurer que les clauses contractuelles intègrent la clause de réversibilité, clause d'auditabilité, clause de confidentialité, clause de protection des données personnelles, SLA et engagements des prestataires, sanctions en cas de non respects des engagements des prestataires, protection de la propriété du code source développé dans le cadre de la maintenance, ...
- S'assurer de l'existence d'un processus de suivi de l'obsolescence des applications en place
- S'assurer que les versions des assets physiques et logiques sont à jour, et qu'un suivi est en place pour anticiper les mises à jour logicielles et les obsolescences matérielles (fin de support du constructeur).

Risques :

- Arrêt du service
- Non optimisation des coûts
- Litiges avec les prestataires
- Non-conformité réglementaire

1-3 S'assurer que la gestion du cycle de vie des assets IT se fait conformément aux procédures internes et aux bonnes pratiques dans la matière :

- S'assurer de l'existence de contrats cadres permettant l'acquisition des Assets IT de façon optimisée et garantissant la continuité des services ; (durée du contrat cadre, couverture des filiales, PV d'adjudication, ...)
- S'assurer que des inventaires périodiques, exhaustifs et structurés sont réalisés pour recenser les licences et les actifs informatiques du Groupe (matériels et logiciels) ainsi que leurs attributs. (Automatisé ou manuel ?)
- S'assurer de la mise en place d'un outil de gestion du parc informatique permettant de suivre le cycle de vie de chaque actif. (Date d'arrivée en stock, identifiant, marque, référence, réparation date d'attribution à un utilisateur, nom de l'utilisateur, date de mise en rebut, restitution en cas de départ (démission, retraite) ou mobilité vers OCP ou filiales, localisation de stockage ...)

- Pour les Assets IT physiques, vérifier que leur mise au rebut (destruction ou dons aux associations) se fait conformément aux procédures internes et aux bonnes pratiques dans la matière.

Risques :

- Non optimisation des coûts
- Atteinte à la sécurité des Asset IT

1-4 S'assurer de l'existence de mesures de suivi de la performance du processus de gestion de l'acquisition et de la maintenance à travers des tableaux de bord et des KPI dédiés. (Évaluation des interventions de maintenance, évaluation des prestataires)

Risques :

- Non atteinte de l'efficacité opérationnelle du SI
- Non maîtrise et détérioration des Assets IT du Groupe

Objectif 2 : S'assurer de l'alignement des contrats conclus et des interventions de la maintenance IT réalisées avec le cadre formel mis en place ainsi qu'avec les bonnes pratiques en la matière :

2.1 S'assurer de l'existence d'outils centralisant l'ensemble des interventions de la maintenance réalisée (équipements Data center siège et sites);

Risques :

- Perte de la traçabilité et des informations relatives à l'Asset IT
- Difficulté de pérennisation et de maintien des solutions ;

2-2 Obtenir la liste de l'ensemble des interventions de maintenance (et de télémaintenance si existant) réalisées durant les 12 derniers mois :

- Sur la base d'un échantillon, s'assurer que l'Asset IT concerné par l'intervention de la maintenance est couvert par un contrat de maintenance ;
- Pour les cas de remplacement d'Asset défectueux, s'assurer que les diligences nécessaires ont été faites pour confirmer les nouvelles acquisitions ;
- Vérifier l'existence de rapports, PV, dossiers assurant la traçabilité des opérations de la maintenance réalisée ;
- Pour les cas de télémaintenance (notamment pour les interventions réalisées par DXC), s'assurer que la connexion établie et les droits alloués au prestataire respectent les exigences de la PSSI, et répondent aux besoins de l'intervention réalisée.

Risques :

- Atteinte à la sécurité des Asset IT
- Non optimisation des coûts
- Perte de la traçabilité et des informations relatives à l'Asset IT

2-3 S'assurer que les intervenants (prestashop) ont signé au préalable des clauses de confidentialité.

Risques :

- Atteinte à la sécurité des Asset IT
- Non-conformité réglementaire
- Litiges avec les prestataires