Groupe Professionnel Contrôle Interne
Groupe Professionnel Systèmes d'Information

FICHE DES BONNES PRATIQUES DU CONTRÔLE INTERNE
GESTION DU SYSTEME D'INFORMATION

Points clés

- Utilisation de référentiels de gouvernance ou de normes de conformités SI (COBIT, ITIL, ISO 27001).
- Mise à jour et diffusion des politiques et des procédures du SI en interne et déclinée aux prestataires.
- Application d'une Politique de sécurité revue (yc annexes de sécurité aux contrats) et les règles internes d'utilisation des moyens informatiques.
- La gestion des incidents majeurs (cyber ou services) rejoint le processus de gestion de crise de l'Entreprise (dont communication interne et externe).
- En réponse au contexte de cyber-criminalité, intégration des fondamentaux de sécurité dans le dispositif de Contrôle interne.
- La gestion du Plan de Continuité d'Activité, non traitée ici, au-delà de l'aspect technique géré par le SI (sauvegardes, restauration, architecture. redondante) est confiée à une organisation compétente qui intègre la vision métier (en particulier sur la détermination des ressources critiques).
- Maintenance d'une cartographie des applications supportant les processus et contrôles clés de l'entreprise.
- Les enjeux règlementaires sectoriels (bancaires, OIV, SEC, …) et RGPD sont amenés à se développer.
- *Émergence de nouveaux métiers autour du management de la data (Chief Data Officer) liée à la transformation digitale impliquant l'évolution des référentiels de contrôle interne (cf. COBIT 2019, APO14 – Data Management). Ce point n'est pas développé ci-après.*

Traitement de la menace Cyber

RISQUES

- Pénétration de systèmes informatiques visant à :
  - détourner des fonds,
  - voler/corrompre/détruire des données,
  - dégrader, interrompre ou rendre inaccessibles des services.
- Risque légal et règlementaire (conformité RGPD).
- Utilisation illégitime ou frauduleuse des ressources SI (cryptojacking : utilisation d'un serveur pour produire de la cryptomonnaie)

BONNES PRATIQUES

- *Références : anssi guide tpe pme cybersecurité, guide hygiene informatique anssi, Guide des risques cyber Ifaci-2.0-2020)*
- Une organisation experte en cyber s'assure que :
  - une architecture sécurisée et adaptée est en place (cloisonner les systèmes, surtout accessibles de l'extérieur, utilisation de firewalls, …),
  - la connexion des tiers/sites du groupe aux réseaux est soumise aux règles d'authentification,
  - les logiciels de sécurité (antivirus, spyware, anti-phishing…) sont mis en place et actualisés,
  - une sécurisation des usages mobiles (cryptage disques durs, désactivation ports USB, tél mobile, …) est appliquée,
  - une évaluation périodique des vulnérabilités est réalisée. Des actions correctives sont mises en œuvre et suivies le cas échéant.
  - un système de patch management (détection automatique des failles et identification des correctifs) existe,
  - un dispositif (organisation, procédures) de surveillance du réseau informatique est mis en place pour :
    - détecter des actions inhabituelles ou à risque sur le réseau et le système informatique,
    - réagir pour stopper / réduire l'impact au plus vite,
    - investiguer les causes et mettre en œuvre les actions correctives nécessaires.
- Réaliser régulièrement des actions de sensibilisation et de formation sont sur les sujets liés à la cybersécurité (MOOC ANSSI, Intranet, mails, test de phishing et de fraude au président, etc.).
- S'assurer de la mise en œuvre de moyens adaptés à l'analyse de risque (Gestion de crise, Assurance Cyber, …).

Accès aux applications sensibles (financières, sécurité, RGPD …) aux systèmes et aux données et Séparation des tâches

RISQUES

- Risque de non-conformité légale, réglementaire et sectorielle (RGPD, SAPIN 2, Directives européennes, Loi de Programmation Militaire, …).
- Perte de confidentialité, de disponibilité et d'intégrité (information financière par exemple).
- Risque de non-recevabilité des contrôles par CAC.
- Fraude et malversation.
- Perte ou fuite de données (vol, fuite involontaire, intrusion, sabotage, etc.).
- Utilisation illégale ou inappropriée des données de base (clients, fournisseurs, prix, articles, etc.).

BONNES PRATIQUES

- S'assurer que les **accès aux données** sont segmentés selon les usages et responsabilités (dont données critiques et à caractère personnel)
- S'assurer pour **les accès aux applications**, que :
  - chaque accès utilisateur a été validé par une personne habilitée
  - les accès sont désactivés en cas de départs et de mobilités,
  - une revue annuelle des accès est réalisée par les métiers et le SI (valider la conformité des droits aux responsabilités exercées : principe du moindre privilège),
  - il n'existe pas de comptes génériques et les comptes utilisés par les applications sont distincts des comptes utilisateurs,
  - les comptes à privilèges sont restreints au strict minimum, et leur utilisation est supervisée (logs),
  - un système d'authentification centralisé de type « active directory » facilite la gestion des accès / mots de passe / revue,
  - la politique de mots de passe de la société est respectée (Longueur, complexité, durée de vie, historisation, nombre de tentatives avant blocage).
- Une revue annuelle des **accès aux couches basses** (Systèmes d'exploitation, Bases de données, ordonnanceurs, équipements réseaux) est réalisée. Dans le cas d'impossibilité technique, s'orienter vers des solutions de contournement (revue de logs, coffre-fort de gestions des comptes admin).
- **L'accès physique aux installations** informatiques est restreint au personnel autorisé et vérifié (ex. utilisation de badge).
- **Séparation des tâches** : s'assurer que les cumuls de fonctions à risque (fraude ou malveillance) sont régulièrement recherchés, corrigés ou compensés.
  En cas d'impossibilité de correction, des contrôles compensatoires (intégrité, anti-fraude) et de surveillance sont mis en place.
  Construire la matrice de séparation des tâches à partir de scénarios de fraude / malveillance métier (identifier les fonctions applicatives non cumulables).

Externalisation aux tiers SI

Externalisation d'une ou plusieurs activités SI ou de l'ensemble d'une application (SAAS)

- Hébergement
- Développement
- Supervision
- Helpdesk
- …

RISQUES

- Dégradation de la qualité de services et/ou de la garantie de sécurité.
- Dépendance aux tiers et perte de compétences ou de maitrise.
- Risque sur la continuité d'activité si l'externalisation concerne un processus critique (hébergement).
- Manque de maîtrise budgétaire.
- Non-conformité règlementaire (localisation des données) et légale.
- Perte de certifications (ISO 27001 par exemple).
- Non recevabilité CAC.

BONNES PRATIQUES

- **Bonnes pratiques de contrôle interne achats** (cf. fiche CI achat) : contractualisation + focus sur clause d'audit, PCA, Plan d'Assurance Sécurité et de réversibilité (applicatifs, données).
- S'assurer de l'implication des **expertises SI** nécessaires au respect des exigences SI (architecture, infrastructure, sécurité …).
- S'assurer que les processus SI sous-traités font l'objet de **contrôles directs ou des audits du prestataire** diligentés par l'entité
  Obtention et analyse et suivi des anomalies d'un SOC report (Service Organization Control - ex ISAE 3402).
- Intégrer une évaluation des risques liés à l'activité sous-traitée (continuité, data privacy, etc…) à la cartographie des risques.

Octobre 2021

Cette fiche rassemble des propositions de bonnes pratiques issues de l'expérience et du travail du Groupe Professionnel IFACI Contrôle Interne ainsi que des retours de la Communauté du Contrôle Interne du Workplace. Ces propositions n'engagent ni la responsabilité de ses membres, ni de leurs organisations respectives, ni de l'IFACI.

Groupe Professionnel Contrôle Interne
Groupe Professionnel Systèmes d'Information

Gestion des changements

RISQUES

- Ne pas répondre aux besoins métier, sécurité et architecture ou aux exigences de continuité de service.
- Non-respect des budgets.
- Inefficience en cas de non-respect de la stratégie en matière de SI (par exemple cohérence technologique).
- Interruption / Dégradation de services / Régression fonctionnelle.
- Fraude / Malveillance / Erreurs.
- Non-conformité aux attentes des Commissaires aux Comptes.
- Non-conformité règlementaire et sectorielle.

BONNES PRATIQUES

- S'assurer de l'existence d'un référentiel de projets facilitant les activités de contrôle interne et de contrôle financier.

Expression et validation du besoin

- S'assurer que les changements suivent un processus formel incluant :
  - un besoin de changement défini et documenté par le métier demandeur en partenariat avec le SI,
  - une prise en compte des besoins de conformité (inscription au registre des traitements pour le RGPD), du contrôle interne (workflow, automatisation, alertes) et de la sécurité dès les phases de conception du projet,
  - une validation par une instance de gouvernance qui priorise les projets conjointement avec les métiers (stratégie digitale, roadmap des projets, budget et alignement avec les ressources disponibles).

Recette

- S'assurer de l'existence systématique de recettes techniques (interfaces, robustesse, performance, continuité, reprise de données si migration) et fonctionnelles (adéquation aux besoins et non régression) documentées.
- Les défauts sont documentés et corrigés avant la mise en production.
- S'assurer que le Go de mise en production/service a bien pris en compte le résultat des recettes (pas de défaut bloquant).

Exploitation / Maintenance SI

RISQUES

- Interruption / dégradation de services.
- Perte / altération de données.
- Non-conformité (Commissaires aux Comptes, règlementaire et légal).
- Obsolescence.
- Sauvegarde des programmes et des données indisponibles ou inaccessibles.
- Incidents récurrents.
- Pénalités financières ou paiements à tort (licences logicielles).

BONNES PRATIQUES

Gestion des incidents

- S'assurer que l'ensemble des incidents techniques ou fonctionnels est identifié, suivi jusqu'à résolution et documenté (Supervision des traitements applicatifs et techniques, incidents utilisateurs).

💻 Les incidents sont suivis, classifiés et escaladés dans un outil de ticketing.

- S'assurer qu'une revue régulière des incidents (délais, causes, incidents récurrents) est réalisée.

Correctifs de sécurité (Patchs)

- S'assurer de l'application de processus de mise à jour des équipements réseau, des systèmes d'exploitation, des bases de données et des systèmes applicatifs (patchs / correctifs). Ce processus décrit le niveau de documentation attendu en fonction du type de changement.

Sauvegarde et restauration

- S'assurer de la supervision et de la réalisation des tests de sauvegarde (y compris hors-site) et de restauration régulière des systèmes (serveurs et applications) et des données métiers critiques (y compris bureautique)
  En cas de difficultés techniques de mise en place systématique de tests de restauration, une architecture résiliente (redondance), permet de limiter le risque de perte de continuité d'activité et de perte de données (hors scénario de corruption de données e.g. ransomware).
- S'assurer que les données font l'objet de purges régulières conformément aux durées de rétention légales et réglementaires.
- S'assurer de la réalisation de tests réguliers de l'infrastructure de bascule (système de secours) conformément au Plan de Continuité d'Activité/Plan de Secours Informatique.

Validation des changements

- S'assurer de l'existence systématique d'une autorisation formelle et d'une traçabilité des mises en production et des mises en service.
  Compléter par une revue régulière des mises en production afin de vérifier le bon respect du processus.
- Les exceptions à cette procédure (changement en urgence, changements techniques) sont listées, font l'objet de tests post implémentation dans un délai approprié et tous les problèmes fonctionnels liés sont enregistrés et traités.

Accès en production

- Accès en production restreints et légitimes :
  - Si possible : séparation des tâches et des environnements entre développement et mise en production.
  - Les comptes permettant de réaliser des modifications en environnement de production sont limités, leur usage revu et tracé.

Gestion de configuration

💻 Des outils de déploiements et de gestion de configuration permettent de garantir la conformité et l'intégrité des fichiers mis en production ainsi que le flux de validation.

Immobilisation matérielle et immatérielle / gestion des licences

💻 Il existe une gestion des actifs matériels et logiciels (idéalement automatisée) afin de minimiser les risques de non-conformité aux contrats éditeurs.

- S'assurer que l'ensemble des matériels informatiques décommissionnés et des logiciels désinstallés ont bien fait l'objet d'une sortie des immobilisations.

Automatisation : Avantages CI Exigences CAC

RISQUES

- Ne pas répondre aux exigences SI, en forte croissance, des Commissaires aux Comptes se conformant aux directives de leur régulateur (H3C).
- Contrôles métiers jugés déficients par les Commissaires aux Comptes.
- Couverture insuffisante du dispositif de Contrôle Interne.
- Couverture insuffisante du testing du Contrôle Interne.
- Questionnement de l'entreprise face aux coûts récurrents du CI.

BONNES PRATIQUES

- S'assurer que chaque contrôle basé sur des données issues d'un système dispose des preuves d'intégrité et d'exhaustivité de cette extraction (IPE : Information Provided by Entity).
- S'assurer pour les mécanismes de contrôles automatisés (ITAC Information Technology Application Controls):
  - de la légitimité et la pertinence des droits d'accès (cf Accès aux applications et aux systèmes).
  - de tester la conformité et la fiabilité de l'automatisation (à refaire si l'absence de changement depuis le dernier test ne peut être prouvé)

💻 Automatisation des contrôles ou d'une partie des contrôles (limite les coûts récurrents et minimise le risque d'erreur humaine ou de transaction frauduleuse.
Identifier pour cela les contrôles manipulant des données formatées ou en base)

💻 Automatisation du testing des contrôles (de la macro Excel au développement SI) afin d'en limiter les coûts et augmenter la couverture de test.
Prioriser sur les contrôles nécessitant les temps d'exécution les plus importants.

Octobre 2021

Cette fiche rassemble des propositions de bonnes pratiques issues de l'expérience et du travail du Groupe Professionnel IFACI Contrôle Interne ainsi que des retours de la Communauté du Contrôle Interne du Workplace. Ces propositions n'engagent ni la responsabilité de ses membres, ni de leurs organisations respectives, ni de l'IFACI.