Etude de cas

1 –Réaliser une analyse des risques du SI qui sera restituée sous la forme suivante :

Hypothèses préalables :

- On ne dispose pas de l'organigramme de l'entreprise et des fonctions hiérarchiques.
- On ne dispose pas d'un RACI ni de la liste des gestionnaires/propriétaires des processus informatiques.
- La liste complète des biens (ni leur valeurs business) n'est pas disponible.
- Le niveau d'appétence au risque de l'entreprise est inconnu.
- Soutien de la direction (sponsor) en termes de leadership.

Sources pour l'appréciation, l'analyse, l'évaluation et le traitement du risque : ISO 31000 (2018). ISO 27005

Analyse des risques (non triés)

#Risque (scénario de risque)	Probabilité / Vraisemblance (Peu vraisemblable, Vraisemblable, Très vraisemblable, Quasi Certain)	Impact (Mineur, Significatif, Grave, Critique)	Type de risque	Nature et description
A. Indisponibilité récurrente du site suite à une affluence de trafic	Quasi Certain	Critique	Opérationnel	Pas d'anticipation de la montée en charge ni de load balancing. Preuves : mail du 25 mai 2020, nombres de réclamations
B. Réclamations suite aux multiples opérations bancaires débitées aux clients	Quasi Certain	Grave	Opérationnel, Financier	Anomalies dans le calcul des montants des paniers et workflow de transactions Preuves : mail du 22 avril 2020, mail du 4 mai 2020, nombres de réclamations
C. Livraison au client du mauvais produit	Vraisemblable	Significatif	Opérationnel, Logistique	Gestion des envois non rigoureux, processus de logistique défaillant Preuves : nombres de réclamations

D. Erreur sur la facturation	Très vraisemblable	Significatif	Opérationnel, Financier	Anomalies dans le logiciel de facturation qui indiquent des montants erronés Preuves : mail du 22 avril 2020, nombres de réclamations
E. Lourdes amendes de la CNIL suite au non-respect du traitement des données personnelles	Quasi Certain	Critique	Opérationnel, client, juridique	Divulgation des données client à des tiers sans autorisation Conséquence : juridique (amendes), Perte de confiance de la part des actionnaires et des clients Preuves : mail du 22 avril 2020, nombres de réclamations
F. Vols de données suite à une infraction par un pirate	Quasi Certain	Grave	Opérationnel, sous-traitance	Vulnérabilité : le prestataire communique des éléments sensibles (mots de passe et identifiants) sans chiffrage de ces derniers et canaux non protégés (ftp) Menace : attaquant interne ou externe qui pourrait intercepter ces informations pour s'introduire dans le SI et voler /détruire des données. Preuve : mail du jeudi 5 mars 2020
G. Abandon de paniers, perte de	Très vraisemblable	Grave	Opérationnel, sous-traitance, relation client	Lenteurs et difficultés de navigation, transaction perdue

chiffre d'affaire et de réputation				Preuves : nombres de réclamations
H. Crash du site web, exécution de codes malveillants (côté serveur) suite à un buffer overflow	Quasi Certain	Grave	Opérationnel (développement), sous-traitance	Vulnérabilité : fuite mémoire du logiciel non patché. Absence de security by design. Menace : attaquant interne ou externe qui pourrait exécuter un code malicieux ou une backdoor à distance à des fins malveillantes. Preuve : mail du jeudi 5 mars 2020
I. Incompatibilité entre les versions, plugins, bugs	Vraisemblable	Significatif	Opérationnel (développement), gestion de projet, sous-traitance	Absence de versioning rigoureux, pas de démarche qualité mise en place lors des cycles de développement (tests aléatoires) Preuve : mail du jeudi 5 mars 2020
J. Arrêt de l'activité suite à la non livraison du matériel de télétravail	Très vraisemblable	Critique	Opérationnel (achat), Continuité des activités PCA	Manque de suivi des achats. Pas de traçabilité des opérations en cours. Preuve : mail du vendredi 20 mars 2020
K. Absence de support utilisateur en cas d'urgences	Vraisemblable	Grave	Support, Relation client	Logiciel de ticketing mal configuré, manque de personnel (techniciens supports)

				Preuves : nombres de réclamations
L. Longue indisponibilité des stocks (affichés comme disponibles sur le site)	Très vraisemblable	Significatif	Opérationnel, gestion des stocks	Absence de formalisation du suivi des stocks, pas de registre tenu à jour Preuves : nombres de réclamations

Evaluation du risque

Probabilité Vraisemblance					
	Quasi certain			**B F H**	**A E**
	Très vraisemblable		**D G L**	**J**	
	Vraisemblable		**C I**	**K**	
	Peu vraisemblable				
		Mineur	Significatif	Grave	Critique
		Impact			

A partir de ce constat, donner une liste de 1 à 5 audits qu'il serait utile de programmer

1) Domaine : **audit du SI, audit de la sécurité du SI**

Thèmes couverts : protection et traitement des données personnelles, sécurité de l'information, de la communication, respect juridique du RGPD

Objectifs Cobit 2019: EDM03: Ensured Risk Optimization, APO14: Managed Data, MEA03: Managed Compliance with external Requirements, APO13 : Managed security, DSS05: Managed Security Services, DSS06: Managed Busines Process Controls, APO014: Managed Data

Risque E : lourdes amendes de la CNIL suite au non-respect du traitement des données personnelles

Risque F : vols de données suite à une infraction par un pirate

Risque H : crash du site web, exécution de codes malveillants (côté serveur) suite à un buffer overflow

2) Domaine : **Audit de projet ou de pilotage du SI, audit d'opérations**

Thèmes couverts : tests, qualité en interne et par le sous-traitant, SLA, relation avec les prestataires, gestion de projet et des processus internes/externes

Objectifs Cobit 2019 : EDM02: Ensured Benefits Delivery, APO09 Managed Service Agreements, APO11 Managed Risk, AP013 : Managed security, MEA01: Managed Performance and Conformance Monitoring MEA02: Managed system of Internal Control, DSS05: Managed Security Services, BAI05 Managed Organizational Change, BAI10: Managed Configuration

Risque A : indisponibilité récurrente du site suite à une affluence de trafic

Risque G : abandon de paniers, perte de chiffre d'affaire et de réputation

Risque I : incompatibilité entre les versions, plugins, bugs

3) Domaine : **audit de projet ou de pilotage du SI, audit d'opérations**

Thèmes couverts : support utilisateur, réponse aux incidents, gestion des incidents et des problèmes, continuité des activités

Objectifs Cobit 2019 : APAPO02 Managed strategy, DSS04: Managed Continuity, BAI06: Managed IT Changes, DSS03: Managed Problems, DSS04: Managed Continuity, DSS02 : Managed Service Requests and incidents

Risque J : arrêt de l'activité suite à la non livraison du matériel de télétravail

Risque B : réclamation suite aux multiples opérations bancaires débitées aux clients

Risque K : absence de support utilisateur en cas d'urgence

4) Domaine : **audit d'opérations, audit de projet ou de pilotage du SI, audit interne et contrôle de gestion**

Thèmes couverts : facture et paiement, relation client, logistique, suivi des processus informatiques, gestion des demandes et procédures en cours

Objectifs Cobit 2019 : BAI11 : Managed Projet, APO01: Managed I&T Management Framework, DSS01: Managed Operations

Risque D : erreur sur la facturation

Risque C : livraison au client du mauvais produit

Risque L : longue Indisponibilité des stocks (affichés comme disponibles sur le site)

3 audits à réaliser en priorité

- Les interlocuteurs à interviewer :

  Thème 1 : CIL DPO DSI, RSSI, directions métiers, départements : métiers de la data, commerciaux et relation clients, gestionnaire CRM, responsables métiers

  Thème 2 : le DG, la DSI, auditeurs internes, responsables qualités, prestaires externes

  Thème 3 : la DSI, techniciens support et manager

Les questions à leur poser et les preuves à collecter

Source : guide d'audit de la gouvernance du système d'information de l'entreprise numérique.

- Thème 1 (Sécurité et traitement des données, du SI par l'entreprise et son prestataire)

  Les évolutions numériques intègrent-elles les exigences de gestion des risques, de contrôle et d'audit en lien avec les pratiques réglementaires et éthiques ?
  Les données personnelles ont été collectée de manière loyale, licite et transparente ?
  L'objectif de la collecte et du traitement de la donnée est-il légitime ?
  La finalité du traitement, les catégories et la source de données ont-elles été portée à la connaissance de l'intéressé ?
  La collecte des données a reçu le consentement de son intéressé ?
  Les modalités du droit à l'information sont-elles établies et appliquées ?
  Les accès aux traitements et aux données sont-ils tracés et analysés ?
  En cas d'incidents, un processus de recensement et de communication est-il prévu ?
  Les nouvelles pratiques commerciales numériques sont-elles revues systématiquement en tenant compte des circuits multicanaux, de l'intégration des réseaux sociaux et du Big Data ?
  L'accès, la transformation et la diffusion des données personnelles sont-ils pris en compte dans les projets numériques ?
  Pour chaque donnée critique, un responsable d'application de données est-il nommé ?
  Existe-t-il un registre de classification des données ?
  Y a-t-il un projet GDPR dans l'entreprise ?
  Quelles sont les dispositions en matière de sécurisation des données ? Sont-elles testées et à quelle fréquence ?
  Les autorisations d'accès aux données font-elles l'objet de revues qualitative et quantitative ?
  L'organisation auditée a-t-elle documenté sa politique de contrôle d'accès et tient-elle à jour une matrice des autorisations ?
  Une procédure formelle d'attribution / retrait des droits d'accès par utilisateur est-elle définie, avec circulation d'informations entre les services concernés ?
  Les utilisateurs ont-ils l'interdiction de divulguer, communiquer, partager leur mot de passe ?
  Existe-t-il une politique de chiffrement des données sensibles (mot de passe, supports nomades…)
  Les mots de passe ont-ils une obligation de complexité (longueur mini, 3 types de caractères différents…)

Les fonctions de développement informatique, de tests et d'exploitation sont-elles séparées, avec du personnel différent ?

Preuves : nomination d'un DPO ? Document : traitements et catégorisation des données, réponse aux demandes d'effacement, demande d'accord express, mails de réclamation, logs des traitements et des accès, tenue de registre.

- Thème 2 (Exécution d'un service par un prestataire, audit auprès du prestataire)

  Un organigramme de la fonction informatique est-il formalisé et actualisé de manière régulière ?
  Pour chaque application, un responsable d'application est-il nommé ?
  Si un logiciel est géré par un tiers, les dispositions contractuelles prévoient-elles les conditions de mise à disposition des données ?
  Existe-t-il des démarches qualités pour assurer des livrables qui correspondent à l'attendu ?
  Des méthodologies de gestion de projet logiciels sont-elles mises en place ?
  Ces dispositions sont-elles testées et mesurées régulièrement ?
  Les flux ayant un impact sur l'information comptable et financière sont identifiés ?
  Les interfaces les plus critiques font l'objet de contrôle manuels ou par analyse de données ?

  Preuves : organigramme des fonctions, rôles, responsabilité, RACI, contrats SLA, contrats informatiques avec le sous-traitant, preuves de tests (tests unitaires, d'intégration, de non régression, fuzzing…), preuves de bonnes pratiques en développement, bonne qualification du personnel et formations adéquates (remise à niveau, montée en compétences).

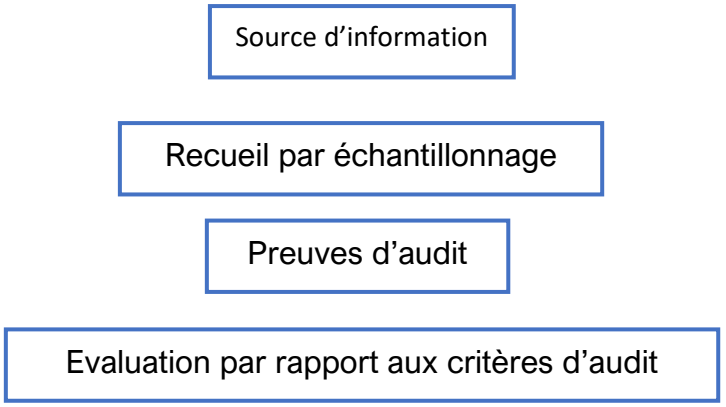
- Thème 3 (Gestion du support utilisateur (incidents/problèmes), Continuité et reprise de l'activité)

  Le parcours numérique du client est-il au cœur du pilotage de la performance opérationnelle (CRM…) ?
  Les procédures de sauvegarde sont-elles formalisées et sont-elles conformes aux besoins de l'entreprise (RPO, RTO) ?
  Des tests de restauration sont-ils menés ? Sur quel périmètre, avec quelles parties prenantes et avec quelle fréquence ?
  Les moyens alloués sont-ils suffisants pour traiter les demandes des utilisateurs ?

Comment sont gérés les plannings des techniciens pour le traitement des demandes des utilisateurs ?
Existe-t-il une procédure de gestion des incidents, de catégorisation, procédure d'escalades ?
Comment sont gérés les problèmes jusqu'à la résolution de ces dernières ?

Preuves : documents de procédures, planning des techniciens, logs des outils de ticketing, Configuration Management System (CMS), Configuration Management Database (CMDB), SKMS (Service Knowledge Management System), plan de PCA/RCA

Etapes



Les recommandations de mesures correctives possibles à proposer si des preuves de non-conformité sont avérées

Sources pour les mesures correctives et les contrôles à proposer suite à l'audit : ISO 27001 (Annexe A), ISO 27002, ISO 20000. Pas de détails techniques sur les mesures à mettre en place dans l'idée de proposer uniquement des conseils généraux et ne pas remplacer la prise de décision du DSI.

Thème 1 (Sécurité et traitement des données, du SI par l'entreprise et son prestataire)		
Clause	Catégorie de contrôle / Mesure	Exemples de contrôle / mesure à proposer
A.5.1.1	Politiques de sécurité de l'information	Un ensemble de politiques de sécurité de l'information doit être défini, approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés.
A.5.1.2	Revue des politiques de sécurité de l'information	Les politiques de sécurité de l'information doivent être revues à intervalles programmés ou en cas de changements majeurs pour garantir leur pertinence, leur adéquation et leur effectivité dans le temps.
A.10.1.1	Politique d'utilisation des mesures cryptographiques	Il convient d'élaborer et de mettre en œuvre une politique d'utilisation de mesures cryptographiques en vue de protéger l'information.
A.13.2.1	Politiques et procédures de transfert de l'information	Des politiques, des procédures et des mesures de transfert formelles doivent être mises en place pour protéger les transferts d'information transitant par tous types d'équipements de communication.
A.9.4.2	Sécuriser les procédures de connexion	Lorsque la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications doit être contrôlé par une procédure de connexion sécurisée.
A.9.3.1	Utilisation d'informations	Les utilisateurs doivent suivre les pratiques de l'organisation pour l'utilisation des informations secrètes d'authentification.

	secrètes d'authentification	
A.13.1.2	Sécurité des services de réseau	Pour tous les services de réseau, les mécanismes de sécurité, les niveaux de service et les exigences de gestion, doivent être identifiés et intégrés dans les accords de services de réseau, que ces services soient fournis en interne ou externalisés.
A.8.2.1	Classification des informations	Les informations doivent être classifiées en termes d'exigences légales, de valeur, de caractère critique et de sensibilité au regard d'une divulgation ou modification non autorisée.
A.9.1.1	Politique de contrôle d'accès	Une politique de contrôle d'accès doit être établie, documentée et revue sur la base des exigences métier et de sécurité de l'information.
A.9.2.5	Revue des droits d'accès utilisateurs	Les propriétaires d'actifs doivent vérifier les droits d'accès des utilisateurs à intervalles réguliers.
A.9.4.1	Restriction d'accès à l'information	L'accès à l'information et aux fonctions d'application système doit être restreint conformément à la politique de contrôle d'accès.
A.10.1.1	Politique d'utilisation des mesures cryptographiques	Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information doit être élaborée et mise en œuvre.
A.12.6.1	Gestion des vulnérabilités techniques	Des informations sur les vulnérabilités techniques des systèmes d'information en exploitation doivent être obtenues en temps opportun, l'exposition de l'organisation à

		ces vulnérabilités doit être évaluée et les mesures appropriées doivent être prises pour traiter le risque associé.
A.13.2.1	Politiques et procédures de transfert de l'information	Des politiques, des procédures et des mesures de transfert formelles doivent être mises en place pour protéger les transferts d'information transitant par tous types d'équipements de communication.
A.13.2.3	Messagerie électronique	L'information transitant par la messagerie électronique doit être protégée de manière appropriée.
A.18.1.4	Protection de la vie privée et protection des données à caractère personnel	La protection de la vie privée et la protection des données à caractère personnel doivent être garanties telles que l'exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant.

Thème 2 (Exécution d'un service par un prestataire, audit auprès du prestataire)		
Clause	Catégorie de contrôle / Mesure	Contrôle / Mesure à proposer
A.14.2.7	Développement externalisé	L'organisation doit superviser et contrôler l'activité de développement du système externalisée.
A.14.2.8	Test de la sécurité du système	Les tests de fonctionnalité de la sécurité doivent être réalisés pendant le développement.
A.15.1.2	La sécurité dans les accords conclus avec les fournisseurs	Les exigences applicables liées à la sécurité de l'information doivent être établies et convenues avec chaque fournisseur pouvant accéder, traiter, stocker, communiquer ou fournir des composants de l'infrastructure informatique destinés à l'information de l'organisation.
A.15.2.1	Surveillance et revue des services des fournisseurs	Les organisations doivent surveiller, vérifier et auditer à intervalles réguliers la prestation des services assurés par les fournisseurs.
A.15.2.2	Gestion des changements apportés dans les services des fournisseurs	Les changements effectués dans les prestations de service des fournisseurs, comprenant le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, doivent être gérés en tenant compte du caractère critique de l'information, des systèmes et des processus concernés et de la réappréciation des risques.
A.7.1.1	Sélection des candidats	Des vérifications doivent être effectuées sur tous les candidats à l'embauche conformément aux lois, aux règlements et à l'éthique et être proportionnées aux exigences métier, à la classification des informations accessibles et aux risques identifiés.

A.7.1.2	Termes et conditions d'embauche	Les accords contractuels entre les salariés et les sous-traitants doivent préciser leurs responsabilités et celles de l'organisation en matière de sécurité de l'information.
A.9.4.5	Contrôle d'accès au code source des programmes	L'accès au code source des programmes doit être restreint.
A.12.1.4	Séparation des environnements de développement, de test et d'exploitation	Les environnements de développement, de test et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans l'environnement en exploitation.
A.12.1.3	Dimensionnement	L'utilisation des ressources doit être surveillée et ajustée et des projections sur les dimensionnements futurs doivent être effectuées pour garantir les performances exigées du système.
A.14.1.1	Analyse et spécification des exigences de sécurité de l'information	Les exigences liées à la sécurité de l'information doivent être intégrées aux exigences des nouveaux systèmes d'information ou des améliorations de systèmes d'information existants.
A.14.2.1	Politique de développement sécurisé	Des règles de développement des logiciels et des systèmes doivent être établies et appliquées aux développements de l'organisation.
A.14.2.3	Revue technique des applications après changement apporté à la plateforme d'exploitation	Lorsque des changements sont apportés aux plateformes d'exploitation, les applications critiques métier doivent être vérifiées et testées afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.

A.14.2.5	Principes d'ingénierie de la sécurité des systèmes	Des principes d'ingénierie de la sécurité des systèmes doivent être établis, documentés, tenus à jour et appliqués à tous les travaux de mise en œuvre des systèmes d'information.
A.14.2.3	Revue technique des applications après changement apporté à la plateforme d'exploitation	Lorsque des changements sont apportés aux plateformes d'exploitation, les applications critiques métier doivent être vérifiées et testées afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.
A.16.1.3	Signalement des failles liées à la sécurité de l'information	Les salariés et les sous-traitants utilisant les systèmes et services d'information de l'organisation doivent noter et signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.

Thème 3 (Gestion du support utilisateur (incidents/problèmes), Continuité et reprise de l'activité)

Clause	Catégorie de contrôle / Mesure	Contrôle / Mesure à proposer
A.17.2.1	Disponibilité des moyens de traitement de l'information	Des moyens de traitement de l'information doivent être mis en œuvre avec suffisamment de redondances pour répondre aux exigences de disponibilité.
A.12.1.1	Procédures d'exploitation documentées	Les procédures d'exploitation doivent être documentées et mises à disposition de tous les utilisateurs concernés.
A.12.1.2	Gestion des changements	Les changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information ayant une incidence sur la sécurité de l'information doivent être contrôlés.
A.12.3.1	Sauvegarde des informations	Des copies de sauvegarde de l'information, des logiciels et des images systèmes doivent être réalisés et testés régulièrement conformément à une politique de sauvegarde convenue.
A.12.7.1	Mesures relatives à l'audit des systèmes d'information	Les exigences et activités d'audit impliquant des vérifications sur des systèmes en exploitation doivent être prévues avec soin et validées afin de réduire au minimum les perturbations subies par les processus métier.
A.17.1.1	Organisation de la continuité de la sécurité de l'information	L'organisation doit déterminer ses exigences en matière de sécurité de l'information et de continuité de management de la sécurité de l'information dans des situations défavorables, comme lors d'une crise ou d'un sinistre
A.17.1.2	Mise en œuvre de la continuité de la sécurité de l'information	L'organisation doit établir, documenter, mettre en œuvre et tenir à jour des processus, des procédures et des mesures

		permettant de fournir le niveau requis de continuité de sécurité de l'information au cours d'une situation défavorable.
A.16.1.5	Réponse aux incidents liés à la sécurité de l'information (dont la sécurité, continuité, disponibilité, capacité selon ISO 20000/ ITIL)	Les incidents liés à la sécurité de l'information doivent être traités conformément aux procédures documentées.
A.16.1.6	Tirer des enseignements des incidents IT	Les connaissances recueillies suite à l'analyse et la résolution d'incidents doivent être utilisées pour réduire la probabilité ou l'impact d'incidents ultérieurs.

Exemple de risque résiduel (à titre indicatif)

Un risque résiduel est un scénario de risque subsistant après application de la stratégie de traitement du risque.

Cette évaluation repose sur la gravité et la vraisemblance du risque.

Risques traités : serveurs locaux, système de commande local, information client (voir section précédente)

Modèle : selon EBIOS Risk Manager de l'ANSSI basée sur ISO 27005 (version 2018)

Options de traitement du risque : réduction du risque

Risque E : divulgation des données client

■ Description sommaire : constat de reventes/partage de données client à des tiers

■ Vulnérabilités résiduelles susceptibles d'être exploitées par la source de risque : employé (habilité à accéder aux données) qui décide d'agir de façon malveillante suite à une mésentente avec la direction.

■ Autres causes ou facteurs aggravants (négligence, erreur, concours de circonstance, etc.)

Événements redoutés concernés :

■ Événement redouté : lourdes amendes de la CNIL suite au non-respect du traitement des données personnelles

Evaluation du risque résiduel					
Gravité initiale	Critique	Vraisemblance initiale	Quasi Certain	Niveau de risque initial	
Gravité résiduelle	Grave	Vraisemblance résiduelle	Peu vraisemblable	Niveau de risque résiduel	

Gestion du risque résiduel : revue des droits d'accès aux données, sensibilisation des utilisateurs, surveillance et alerte des managers en cas de suspicion de salariés malintentionnés.