

UNITE CONSULTING

RENFORCEMENT DES EXIGENCES DE CONTRÔLE SUR L'EXTERNALISATION IT PAR L'AUTORITÉ BANCAIRE EUROPÉENNE

RECOMMANDATIONS D'UNITE
CONSULTING POUR DONNER
SUITE AUX PREMIERS CONSTATS

FEVRIER 2023

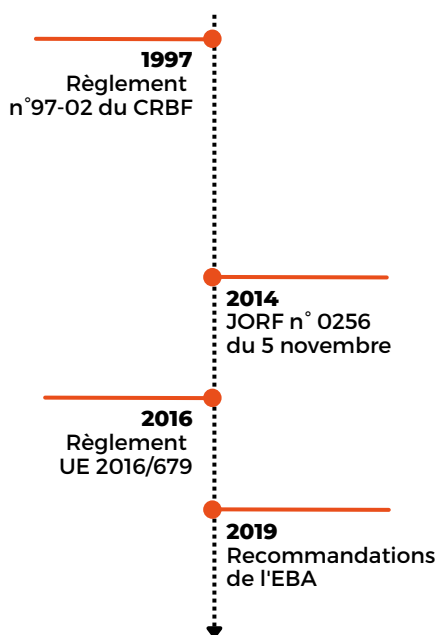
PRÉAMBULE

L'EXTERNALISATION EST UNE RÉALITÉ ÉTABLIE CHEZ LES BANQUES, SOCIÉTÉ DE GESTION ET DE SERVICES FINANCIERS.

Indépendamment de la taille, les cas d'usage répondent souvent au besoin d'industrialiser certaines fonctions critiques (valorisation et middle office des sociétés de gestion) ou d'accéder à un seuil technologique, qui serait inaccessible à des entités n'ayant pas la taille critique (services Cloud notamment).

Les fonctions externalisées quittent donc la sphère des fonctions connexes des institutions financières pour gagner des domaines critiques, voire vitaux. La question de la gouvernance et du contrôle de ces fonctions externalisées a été traitée par les régulateurs européens (EBA et ESMA) sous la forme de recommandations publiées en 2018 et amendées en 2019.

TRAJECTOIRE D'ÉVOLUTION DE LA RÉGLEMENTATION DES SERVICES EXTERNALISÉS



LES RECOMMANDATIONS DE L'EBA

Les recommandations de l'EBA sur l'externalisation visent à garantir que les activités externalisées dans les banques sont gérées de manière efficace et sûre. Ces recommandations ont pour objectif de renforcer la surveillance des activités externalisées afin de s'assurer que les risques associés sont correctement évalués et gérés. Cela permet de protéger les clients tout en garantissant que les banques restent solvables et résilientes.

CYCLE DE VIE DE L'EXTERNALISATION

Les recommandations accompagnent le cycle de vie de l'externalisation, elles peuvent être regroupées en 3 catégories principales:



PHASE PRÉCONTRACTUELLE

Procéder à l'identification et à l'évaluation des risques, en tenant compte des scénarios d'événements à risque, des impacts potentiels associés aux risques et des mesures adoptées par le prestataire de services pour gérer et atténuer les risques.

Une attention particulière doit être accordée à l'évaluation du caractère critique ou de l'importance des fonctions si l'externalisation concerne des fonctions liées à des activités fondamentales¹ et des fonctions critiques².

Réaliser les vérifications nécessaires sur le prestataire dans le cadre du processus de sélection et d'évaluation afin de déterminer la capacité de ce dernier à exécuter les fonctions externalisées. Il convient également de vérifier la nécessité d'une accréditation ou d'un enregistrement par une autorité de réglementation.



PHASE CONTRACTUELLE

Formaliser le contrat d'externalisation.

Un accord écrit doit comprendre:

- La répartition claire et précise des droits et obligations de l'établissement, de l'établissement de paiement et du prestataire.
- L'ensemble des informations sur l'externalisation de fonctions critiques ou importantes.
- Les informations relatives à la sous-externalisation dans le cas précis où la sous-externalisation de fonctions critiques ou importantes est autorisée.
- Les droits de résiliation.

¹ : «activités fondamentales» - article 2, paragraphe 1, points 36, de la directive 2014/59/UE, les activités et services associés qui représentent pour un établissement ou pour un groupe dont un établissement fait partie des sources importantes de revenus, de bénéfices ou de valeur de franchise.

²: «fonctions critiques» - article 2, paragraphe 1, points 35, de la directive 2014/59/UE, les activités, services ou opérations dont l'interruption est susceptible, dans un ou plusieurs États membres, d'entraîner des perturbations des services indispensables à l'économie réelle ou de perturber la stabilité financière en raison de la taille ou de la part de marché de l'établissement ou du groupe, de son inter dépendance interne et externe, de sa complexité ou des activités transfrontières qu'il exerce, une attention particulière étant accordée à la substituable de ces activités, services ou opérations.



PHASE POST-CONTRACTUELLE

Mettre en place des dispositifs de gouvernance et d'externalisation sains. Attribuer les responsabilités en matière de documentation, de gestion et de contrôle des dispositifs d'externalisation.

Maintenir et tester périodiquement des plans appropriés de poursuite de l'activité pour les fonctions critiques ou importantes externalisées, en tenant compte de la qualité de la fourniture de la fonction externalisée et de l'incidence potentielle de l'insolvabilité ou d'autres défaillances des prestataires de services.

Réaliser un plan et programme d'audit interne selon une approche par les risques pour l'examen indépendant des activités externalisées et la révision des dispositifs d'externalisation de fonctions critiques ou importantes.

Veiller à ce que les prestataires respectent les normes de sécurité informatique appropriées. Définir les exigences de sécurité des données et des systèmes dans le cadre du dispositif d'externalisation, et contrôler en permanence le respect de ces exigences.

Etablir des droits d'accès, d'information et d'audit.

Documenter l'ensemble des dispositifs d'externalisation et conserver cette documentation dans un registre, tenu à jour pendant une durée appropriée. L'addition d'un sous-registre est possible.

Effectuer le suivi permanent des performances des prestataires de services en ce qui concerne tous les dispositifs d'externalisation selon une approche par les risques. Lors de changement significatif, réévaluer le caractère critique ou important des fonctions.

Documenter une stratégie de sortie conforme à la politique d'externalisation et aux plans de continuité de l'activité.

LE REGISTRE DE L'EXTERNALISATION

UN PILLIER MAJEUR

Le pilier principal des recommandations est représenté par le registre d'externalisation, qui permet de fournir une cartographie fidèle des services externalisés, de leur profil de risque et des produits et services servis par l'externalisation. Le registre doit refléter l'évolution des services et leur niveau de criticité Métier, et disposer d'une vue suffisamment granulaire des services externalisés, nécessaire à la conception de stratégies de sortie réalistes.

CAS PARTICULIER DES SERVICES CLOUD

Les services Cloud, s'agissant d'une prestation externalisée, obéissent aux mêmes principes. Elle tend à devenir de plus en plus critique étant donné la nature des services métier qui y sont hébergés (traitement massif de données, infrastructures standardisées supportant des applications métier, etc...). Idéalement, le registre des externalisations devrait être mis en corrélation avec les référentiels applicatifs (CMDB), les entrées de ces derniers devant être rattachées aux services définis dans le registre. L'élaboration d'une stratégie de sortie crédible pour les fournisseurs de services en nuage repose sur la qualité des inventaires.

COMMENT ABORDER LA MISE EN PLACE DES RECOMMANDATIONS SUR L'EXTERNALISATION ?

- La mise en place de ces recommandations dépend de la maturité de l'institution financière, au-delà des recommandations prises à titre individuel, l'effort doit se concentrer sur la mise en place d'une gouvernance pérenne du dispositif d'externalisation.
- La mise à jour du cadre de contrôle interne par la revue des politiques et procédures, notamment celles qui traitent des processus de sourcing, de la gestion des inventaires, et du pilotage des risques fournisseurs.
- Le cadre de continuité doit intégrer une dimension temporelle, alignée sur la durée de vie des contrats d'externalisation, qui permet de mieux prendre en compte les risques de sortie, qu'elle soit forcée ou souhaitée. Les mesures de mitigation doivent être cohérentes avec l'appréciation de la criticité Métier des prestataires de services externalisés.
- Le stock de contrats signés doit faire l'objet d'une revue détaillée, basée sur les points de contrôle énumérés dans le texte de l'EBA. Les fenêtres de renouvellement doivent être saisies pour apporter les amendements nécessaires aux contrats, notamment ceux qui préservent les intérêts des institutions financières, en particulier lors de la fin de la relation.
- L'élaboration des stratégies de sortie est un pilier important du texte qui doit s'adapter à la maturité de l'organisation et ses moyens. Une stratégie de sortie n'est pas un plan projet détaillé. Elle apporte une assurance raisonnable aux décideurs quant à la capacité de l'institution à poursuivre l'activité sujette à l'externalisation dans un délai maîtrisé. Un zoom spécifique est apporté à la page suivante.

ÉLABORATION D'UNE STRATÉGIE DE SORTIE

Les exigences relatives au contenu d'une stratégie de sortie n'ont pas été précisées dans le texte, laissant ainsi persister l'incertitude quant aux critères de recevabilité. Conformément à l'esprit du texte, la rédaction d'une stratégie de sortie doit être guidée par l'évaluation des risques qu'elle cherche à atténuer.

Ainsi, limité par le temps et les ressources, le document doit a minima contenir les éléments suivants:

DESCRIPTION DÉTAILLÉE des services faisant l'objet de l'externalisation.

EVALUATION DU RISQUE ET DE LA CRITICITE DES SERVICES sur la base des besoins de continuité préalablement définis avec les principaux consommateurs des services en question.

ETUDE DE MARCHÉ qui présente les offres concurrentes à celles fournies par le prestataire. Des éléments de veille technologique peuvent être recueillis auprès d'organismes de benchmarking tels que Gartner ou Forrester.

SELECTION DES OPTIONS appropriées au contexte de l'externalisation à adopter parmi celles présentes dans le tableau ci-dessous.

ESTIMATION MACRO (top-down) de la complexité, de la charge et des délais nécessaires à l'exécution de la sortie.

L'estimation doit être crédible sans nécessiter un niveau de détail élevé, car la sortie effective d'un service donnera lieu à un projet en bonne et due forme, qui s'attèlera à produire un plan de sortie détaillé en prenant en compte des paramètres plus précis et actuels.

	Principes directeurs	Complexité de la migration
Ne rien faire (arrêter l'usage)	L'arrêt du service doit obtenir l'aval du Métier, c'est une stratégie rarement employée et qui nécessite une récupération des données pour des besoins d'archivage réglementaire.	
Réorganisation du Business/ éviter l'utilisation de cloud externe	Évaluer avec le métier la suppression des services externalisés tout en maintenant le service métier.	
Déplacer le produit vers un autre fournisseur	Une attention particulière doit être apportée à la rédaction de l'appel d'offre, en y intégrant suffisamment d'informations relatives au service existant. L'opportunité de faire évoluer le service doit faire l'objet d'une évaluation précise afin de ne pas pénaliser la migration dans les délais.	
Migrer vers le même produit sur site	La réinternalisation du service demande une étude précise qui prend en compte les détails opérationnels du service fourni afin de garantir la mobilisation des ressources idoines.	

EN CAS DE MANQUEMENT OU DE NON-RESPECT DES RÈGLES RÉGISSANT LES ACTIVITÉS D'EXTERNALISATION, LES ÉTABLISSEMENTS CONCERNÉS S'EXPOSENT À DES SANCTIONS DISCIPLINAIRES DE LA PART DE L'ACPR.

LA RÉGLEMENTATION DORA

Le projet de réglementation DORA (Digital Operational Resilience Act) constitue un cadre additionnel, qui s'inscrit dans la continuité des orientations de l'autorité bancaire européenne de 2019 et entrera en vigueur à partir de 2025.

RENFORCER LA RÉSILIENCE OPÉRATIONNELLE INFORMATIQUE DES ACTEURS DU SECTEUR BANCAIRE ET FINANCIER

La résilience opérationnelle informatique, principe directeur du projet Dora, porté par la commission européenne, peut se traduire par la capacité d'une organisation ou d'une entreprise à pouvoir continuer à fournir des prestations alors qu'elle peut connaître une attaque informatique ou un incident cyber.

Ce projet est destiné à l'ensemble du secteur financier : le secteur bancaire, les compagnies d'assurance, les infrastructures et acteurs des marchés financiers.

UN NOUVEAU CADRE DE GOUVERNANCE ET DE CONTRÔLE INTERNE



GESTION DES RISQUES INFORMATIQUES

Définir un cadre formel pour une bonne gouvernance de la gestion des risques : documents et procédures.



GESTION DES INCIDENTS LIÉS À L'INFORMATIQUE

Harmoniser les rapports d'incidents pertinents et promouvoir l'échange d'informations, ainsi qu'informer les autorités nationales.



GESTION DU RISQUE DE TIERS

Se conformer aux règles essentielles qui régissent la surveillance des risques liés aux tiers par les entités financières et la surveillance des prestataires par les autorités européennes de surveillance (AES).



TESTS DE RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE

Renforcer les processus et les exigences de test dans les entités financières, y compris la mise en œuvre de tests de pénétration (Threat-Led Penetration Testing - TLPT).

VOS CONTACTS



SOFIEN BEN BRAHIM

Partner & Président

+33 6 20 60 15 53



FRANÇOIS DIAS

Partner & COO

+33 6 37 22 12 55



OSWA PONCET

Consultante

+33 6 52 85 04 51

