



MIGRATION DU SYSTÈME "REP' AERO"

Plan d'implémentation

ARCHITECTE LOGICIEL			
PROJET		DATE DÉPÔT	DATE SOUTENANCE
P7	Réalisez un plan d'implémentation pour assurer le bon déroulement de votre projet d'architecture.	22/07/2023	26/07/2023
Livrable 2/3	Plan d'implémentation.		

Marc LEFRANÇOIS
mlefrancois.contact@gmail.com

CONTRÔLE DES RÉVISIONS

DATE	STATUT	AUTEUR	RÔLE	ACTIONS
23/06/2023	Brouillon	Marc LEFRANÇOIS	Créateur	Création du document et mise en place du plan.
03/07/2023	Brouillon	Grégoire CATAN	Correcteur	Relecture du document et remarques.
03/07/2023	Brouillon	Marc LEFRANÇOIS	Créateur	Enrichissement du document → V1.
07/07/2023	Brouillon	Grégoire CATAN	Correcteur	Relecture du document et remarques.
07/07/2023	Brouillon	Marc LEFRANÇOIS	Créateur	Enrichissement du document → V2.
14/07/2023	Brouillon	Grégoire CATAN	Correcteur	Relecture du document et remarques.
14/07/2023	Brouillon	Marc LEFRANÇOIS	Créateur	Enrichissement du document → V3.
16/07/2023	Validé	Grégoire CATAN	Valideur	Relecture du document et validation.
16/07/2023	Validé	Marc LEFRANÇOIS	Créateur	Envoi pour relecture et remarques.
20/07/2023	Relu	Jérôme POCHELU	Correcteur	Relecture du document et remarques.
21/07/2023	Finalisé	Marc LEFRANÇOIS	Créateur	Ajustement du contenu.

Légendes :

Statut = Brouillon, Final.

Rôle = Créateur / Modificateur, relecteur/correcteur, valideur.

CONTRÔLE DES RÉVISIONS	1
1. OBJET	2
2. SOURCES.....	2
3. STRATÉGIE DE MIGRATION	2
3.1. GENERALITES.....	2
3.2. IMPLEMENTATION.....	3
3.3. ORGANISATION	4
4. MIGRATION DES DONNÉES ET DES FONCTIONNALITÉS.....	4
4.1. DONNEES	5
4.2. FONCTIONNALITES	5
5. DÉFINITION DES ACTIONS	5
5.1. ÉTAPES (CALENDRIER).....	5
5.2. REACTIVATION DES SERVICES.....	6
5.3. SECURITE	6
5.4. MESURE DU SUCCES	7
6. CONCLUSION	8

1. Objet

Dans le cadre du projet de transformation architecturale de la société **Rep' Aero**¹, le présent document a pour objectif de présenter l'ensemble des éléments constitutifs à l'élaboration du plan d'implémentation de la migration de l'architecture initiale vers l'architecture cible.

2. Sources

Pour pouvoir produire, ce plan d'implémentation se base sur les documents sources suivants :

- diagramme de l'architecture existante ;
- diagramme de l'architecture cible ;
- audit technique ;
- analyse de faisabilité ;
- feuille de route ou roadmap.

3. Stratégie de migration

Avant toute chose, il convient de définir une stratégie de migration, id. la façon dont il faudra procéder pour effectuer la migration susmentionnée.

Cette stratégie se définit aussi bien de manière macro, id. au niveau de l'organisation de la société et donc du projet, mais aussi de manière détaillée, id. au niveau de l'implémentation, tout en passant bien entendu par la migration en elle-même.

3.1. Généralités

Concrètement pour pouvoir se faire, la migration doit obtenir un "GO" pour donner suite à l'analyse de faisabilité, ce qui est le cas dans le présent projet, mais aussi de disposer des éléments suivants, acquis durant les étapes précédentes d'audit, d'analyse de faisabilité, etc. :

- **l'architecture cible**, représentant l'objectif à atteindre pour la migration ;
- **l'analyse de l'écart** (cf. « *Analyse de faisabilité* »), pour la migration des fonctionnalités et des données ;
- **les parties prenantes** (cf. « *Analyse de faisabilité* »), pour définir les intervenants dans le cadre du projet et leur rôle ;
- **les tâches à réaliser** (cf. « *Analyse de faisabilité* »), pour définir les différentes étapes de migration ;
- **la matrice RACI**² (cf. « *Analyse de faisabilité* »), pour définir les responsabilités des parties prenantes, en définissant qui fait quoi ;
- **la feuille de route ou roadmap**, pour la planification des tâches ;
- **les impacts** (cf. « *Analyse de faisabilité* »), pour définir les KPI³ et vérifier l'aptitude de la nouvelle architecture aux attentes du métier (*niveau de service*).
- **les risques** (cf. « *Analyse de faisabilité* »), pour assurer le bon suivi du projet de migration.

¹ Pour la suite du document, on emploiera indépendamment les termes « **société** » ou « **entreprise** » pour parler de la société **Rep' Aero**.

² La matrice RACI pour les rôles : **R**esponsable / **R**éalisateur, **A**ccountable / **A**pprobateur, **C**onsulted / **C**onsulté, et **I**nformed / **I**nformé, c'est une matrice définissant d'un côté les parties prenantes, et de l'autre les tâches à réaliser, permettant ainsi d'attribuer aux parties prenantes les tâches qui leur est attribué en fonction d'un des rôles susmentionnés.

³ KPI pour **K**ey **P**erformance **I**ndicator ou **I**ndicateur **C**lé de **P**erformance ou ICP en français, est un indicateur utilisé pour l'aide à la décision, et il est particulièrement utilisé en **G**estion de la **P**erformance **O**rganisationnelle ou GPO, qui est la manière dont une organisation planifie, organise, contrôle et se dirige afin de réaliser un objectif, la mise en œuvre d'une stratégie ou de l'accomplissement d'un travail ou d'une activité.

La migration se fera en "double run", id. que le système basé sur l'architecture initiale fonctionnera en parallèle et conjointement avec le nouveau système basé sur l'architecture cible, ce qui implique d'une part, que chacun des composants (*GESTION DES FOURNISSEURS*, *GESTION DES CLIENTS...*) soit développé dans son intégralité comme un seul tenant, une seule pièce. Mais aussi d'autre part, de bien veiller durant la migration qu'il y ait un pont de données ou processus ETL⁴ entre les deux systèmes susmentionnés, afin de garantir leur sécurité et leur intégrité.

3.2. Implémentation

Globalement, la stratégie d'implémentation impliquera que chaque partie prenante IT se voit attribuer la responsabilité d'un seul composant à la fois, en fonction de ses qualifications. Cependant, dans certains cas, où un composant requiert plusieurs qualifications, une ou plusieurs autres parties prenantes IT pourront venir en sus afin d'y développer un ou plusieurs éléments spécifiques dudit composant. Ce qui fait que chacune desdites parties prenantes est responsable des éléments implémentés / migrés en fonction de ses propres qualifications.

Les parties prenantes côté métier, quant à elles, se verront attribuer les rôles de :

- pilotage du suivi, en étant régulièrement informées par l'équipe IT ;
- référent métier, pour répondre aux questions de l'équipe IT ;
- approbateur, id. vérificateur d'aptitude au bon fonctionnement et de vérificateur de service régulier / rendu du nouveau système.

La stratégie d'implémentation / migration en elle-même de chaque composant se fera comme suit, et ce afin d'en garantir l'efficacité⁵ :

- base de données, avec la structure et le peuplement de jeux de données ;
- l'IHM et les aspects fonctionnels ;
- et pour finir, les composants tiers, tels que par exemple les API, Middlewares, etc.

Bien entendu, cela n'empêche pas l'implémentation des éléments susmentionnés de manière parallélisée, dans la mesure du possible, id. par plusieurs parties prenantes ou par l'implémentation groupée de lots d'éléments, tel que par exemple un lot de bases de données pour un composant donné.

⁴ ETL pour Extract Transform Load ou extracto-chargeur, est une technologie informatique intergicielle permettant d'effectuer des synchronisations massives d'information d'une source de données (*le plus souvent une base de données*) vers une autre.

⁵ Par efficacité, on entend, la cohérence, l'optimisation et la pertinence de l'implémentation / migration.

3.3. Organisation

Globalement, la stratégie de migration consiste en les étapes suivantes :

- **implémentation**, id. conception et développement ;
- **VABF** ou **Validation d’Aptitude au Bon Fonctionnement**, id. la recette métier / client ;
- **Formation des utilisateurs** sur le composant implémenté, cela inclut également les concepts de sécurités et RGPD ;
- **MEP/MES** ou **Mise en Production et en Service** du composant ;
- **VSR** ou **Vérification de Service Régulier / Rendu**, qui permettra au métier de s’assurer que tout est bien à l’attendu dans l’environnement de production.

Ces étapes sont basées sur la transition des services (*service transition*) d’ITIL :

- planification et support à la transition,
- gestion des changements,
- gestion des mises en production et déploiements,
- validation et tests,
- évaluation,
- gestion de la connaissance.

De plus, pour être complet et optimiser les chances de réussite du projet, il serait intéressant d’adosser notre organisation à la gestion de projet Scrum.

En effet, Scrum est une méthodologie agile qui offre un cadre de travail structuré, en étant basé sur un processus itératif (*holistique*), avec une organisation et des rôles bien définis, facilement appréhendables, pouvant s’intégrer dans n’importe quelle organisation, et permettant d’être réactif en cas de problème. Ce qui fait d’elle un standard incontournable, et dont l’utilisation est la plus répandue des méthodes agiles. Aussi, nous permettra-t-elle sans aucun doute d’atteindre notre objectif dans les meilleures conditions.

4. Migration des données et des fonctionnalités

Afin de respecter la stratégie de migration définie plus haut, et notamment à la section « **3.2. Implémentation** », la migration des données se fera avant celle des fonctionnalités, et ce pour chacun des composants à migrer.

Aussi faudra-t-il bien veiller au bon déroulement du processus d’implémentation / migration, tout en veillant au respect du besoin des utilisateurs défini en amont.

Pour ce faire, l’ensemble des données ainsi que l’ensemble des fonctionnalités à migrer ont été répertoriés dans la section « **4. Analyse de l’écart** » du premier livrable traitant de l’analyse de faisabilité.

4.1. Données

Une fois la structure de données implémentée du composant, il sera nécessaire de la peupler, en commençant par un jeu de données de tests permettant d'une part de s'assurer de sa bonne implémentation, et d'autre part de permettre par la suite l'implémentation des fonctionnalités, et notamment de s'assurer que ces dernières puissent manipuler les données, conformément aux attentes utilisateurs.

Ensuite, une fois le composant intégralement implémenté / migré, il sera nécessaire dans le cadre du "double run" de maintenir le niveau d'informations entre l'ancien et le nouveau système, et ce afin de garantir la continuité de service auprès des utilisateurs.

Pour ce faire et afin de se conformer à l'ensemble des contraintes de migration susmentionnées, il sera nécessaire de définir et mettre en place un ensemble de processus ETL (**Extract Transform Load**), faisant office de pont de données entre les deux systèmes susmentionnés en permettant de synchroniser leurs bases de données respectives.

En ce qui concerne la mise en production et service de chaque composant, il sera aussi nécessaire de définir la récurrence d'exécutions desdits processus ETL, et à quel moment celles-ci doit intervenir, toujours en tenant compte de la contrainte de maintenir la continuité de service pour les utilisateurs tout au long du projet.

4.2. Fonctionnalités

Comme déjà mentionné précédemment, les fonctionnalités de chaque composant seront implémentées / migrées consécutivement à l'implémentation / migration des données vues dans la section précédente, et ce pour des raisons de praticité

Une fois les fonctionnalités implémentées / migrées, le composant est prêt à passer à la phase de VABF, durant laquelle le client / métier va "recetter" celui-ci en fonction des besoins et niveaux de services attendus définis en amont du projet, et valider ou non sa qualification.

5. Définition des actions

Cette section décrit l'ensemble des actions nécessaires à la migration.

5.1. Étapes (calendrier)

Chacune des étapes correspond à un élément d'un composant à implémenter / migrer. Celles-ci ont été définies dans le premier livrable traitant de l'analyse de faisabilité de la migration, à la section « **6.2. Tâches** », et leur planification se trouve dans le second livrable traitant de la feuille de route, qui se trouve sur le [GitHub de la société](#). À toutes fins utiles, la feuille de route a été établie sur la base de la matrice de responsabilité ou matrice RACI, se trouvant à la section « **6.3. Responsabilités** » du premier livrable susmentionné.

5.2. Réactivation des services

Une fois les phases de VABF validées et de MEP/MES terminées, l'ancien composant, si toute fois il en existe un, sera désactivé ne permettant plus ainsi aux utilisateurs de pouvoir l'utiliser. Seule la partie « données » de l'ancien composant restera temporairement active, le temps de la phase VSR du composant nouvellement déployé, et qui se verra synchroniser avec celle du nouveau système par l'emploi de processus ETL.

Cependant, si la phase de VSR ne donne pas entièrement satisfaction, ce qui ne devrait normalement pas arriver, l'ancien composant pourrait être temporairement réactivé, le temps de revoir le nouveau composant avant son redéploiement. Ci-fait, l'ancien composant est de nouveau désactivé, et la phase de VSR prolongée d'autant de temps qu'a nécessité l'intervention sur le nouveau composant.

Une fois la phase de VSR du composant nouvellement déployé terminée, le composant prédécesseur ne pourra plus être réactivé, et les processus ETL inhérents à celui-ci seront également désactivés à ce moment-là, rompant ainsi définitivement la synchronisation des données entre les deux composants, ancien et nouveau.

Ce n'est qu'après la VSR du projet, intervenant après celle du dernier composant déployé, que l'ensemble des composants de l'ancien système seront définitivement démantelés, pour ne laisser que le nouveau système nouvellement déployé.

5.3. Sécurité

En ce qui concerne l'aspect sécurité du système, qui est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à mettre en place et pour en empêcher l'utilisation non autorisée, nous en avons abordé la partie juridique dans la section 5.4 du premier livrable sur l'analyse de faisabilité. Certaines de ces mesures seront employées dans le cadre de la préservation du système, et notamment en s'appuyant sur les organismes tels que l'ANSSI⁶ et la DGSi⁷, et par l'emploi de la norme ISO 27001.

Cette dernière est l'une des plus connues traitant des systèmes de management de la sécurité de l'information ou SMSI, et vise à répondre aux objectifs suivants de :

- **confidentialité**, où seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées (*notions de droits ou permissions*), et que tout accès indésirable doit être empêché ;
- **authenticité**, où les utilisateurs doivent prouver leur identité par l'usage de code d'accès, que seul l'utilisateur connaît, qui mit en correspondance d'un identifiant ou login permet d'en garantir l'authenticité, et par conséquent de gérer les droits d'accès aux ressources concernées, maintenant ainsi la confiance dans les relations d'échange.
- **intégrité**, où les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante, ainsi cet objectif utilise généralement des méthodes de calcul de checksum ou de hachage ;
- **disponibilité**, l'accès aux services et ressources du système d'information doit être permanent et sans faille durant les plages d'utilisation prévues, mais aussi rapidement et régulièrement.

À ces objectifs, s'ajoute celui de traçabilité ou de preuve que l'on retrouve également dans des indicateurs des systèmes d'information sous les sigles DICT⁸ / DICP⁹, mais aussi l'objectif de non-répudiation :

ANSSI pour Agence Nationale de la Sécurité des Systèmes d'Information.

DGSi pour Direction Générale de la Sécurité Intérieure.

DICT pour Disponibilité Intégrité Confidentialité Traçabilité.

DICP pour Disponibilité Intégrité Confidentialité Preuve.

- la **traçabilité** ou **preuve**, garantie que les accès et tentatives d'accès aux éléments considérés, id. services et ressources, sont tracées et que celles-ci sont conservées de manière à être exploitables par la suite ;
- la **non-répudiation** et **l'imputation**, implique qu'aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et qu'aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

De plus, l'ensemble des processus IT et métier devront être mis à jour et contenir, notamment, les mesures de sécurité qui auront été actées en amont.

C'est à la condition sine qua non de répondre à l'ensemble des objectifs susmentionnés que le nouveau système sera sécurisé.

5.4. Mesure du succès

Afin de s'assurer de la conformité de la réalisation, et donc de déterminer le succès du projet, il est impératif de la mesurer. Aussi pour ce faire, on utilisera des indicateurs clés de performance ou KPI (Key Performance Indicator), comme définis ci-dessous.

À noter qu'au besoin, ce catalogue pourra éventuellement évoluer par la suite.

IDENTIFIANT	MÉTRIQUE	MESURE	VALEUR INITIALE	VALEUR CIBLE
KPI-1	Business	L'alignement entre le business et la technique, qui fera l'objet d'audits par les parties prenantes (métier).	NC	Résultats des contrôles et d'audit favorables aux exigences attendues
KPI-2	Métier	L'ergonomie et l'expérience utilisateur, via : -> les retours des utilisateurs via : => les tickets d'incident inhérents au traitement métier ; => des enquêtes de satisfaction ; -> des audits d'ergonomie (UI/UX).	NC	Tickets <= 1 / semestre Satisfaction 9/10
KPI-3	Disponibilité	La disponibilité du système aux utilisateurs en fonction de la DIMA (Durée d'Interruption Maximale Autorisée) actée en amont.	NC	Disponibilité >= 99,90% DIMA <= 0,10%
KPI-4	Accessibilité	La réponse du système aux sollicitation des utilisateurs via : -> un système de sondes mesurant les temps d'accès, délai de réponse et déterminant la latence ; -> les retours des utilisateurs via : => les tickets d'incident inhérents au traitement métier ; => des enquêtes de satisfaction..	NC	Délai <= 1s
KPI-5	Production	Le nombre d'incidents de production : -> du nombre d'incidents de production ; -> du délai d'interruption de la production.	NC	Nombre <= 4 / mois Délai de résolution : -> Critique <= 2 heures -> Majeur <= 1/2 journée -> Mineur <= 1 journée
KPI-6	Sécurité du système	La sécurité du système via : -> une supervision du système ; -> mise en place de logs d'accès ; -> un système de sondes mesurant la cohérence des accès et du trafic. -> des audits en sécurité informatique et cybersécurité ; -> des mises en situation (tests) de restitution / récupération des données basées sur des modes opératoires et l'expérience.	NC	faillies <= 1 / décennie
KPI-7	Sécurité des données	La sécurité et qualité des données (cohérence et fiabilité) ou QoD (Quality of Data), via : -> une supervision des données ; -> des tableaux de bords QoD ; -> un système de sondes mesurant la cohérence des données présent dans leur ensemble et individuellement. -> un système de contrôle de sauvegarde mesure entre autres l'intégrité de celle-ci. -> des mises en situation (tests) de restitution / récupération des données basées sur des modes opératoires et l'expérience ; -> le nombre de tickets relevant de la sécurité de données.	NC	Aucune perte de données Tickets <= 6 / semestre

IDENTIFIANT	MÉTRIQUE	MESURE	VALEUR INITIALE	VALEUR CIBLE
KPI-8	Bonnes pratiques d'implémentation	L'implémentation de la réalisation devra respecter les principes et les bonnes pratiques inhérentes (TOGAF, ITIL, etc), et fera l'objet de contrôle et d'audit pour validation par les parties prenantes.	NC	Résultats des contrôles et d'audit favorables aux exigences attendues
KPI-9	Conformité d'implémentation	La conformité d'implémentation, aussi toute fonctionnalité devra faire l'objet de tests unitaires, recette (VABF) et d'intégration, et passer par une phases de VSR.	NC	1 fonctionnalité = 1 validation de test
KPI-10	Délai de MEP/MES * MEP = Mise en production MES = Mise en service	La fréquence de livraison des mises à jour de la plateforme. Le délai de livraison des mises à jour du système, et celui de l'interruption de production / service pour la MEP (Mise En Production).	NC	Fréquence < 1 semaine Délais <= 2 semaines Interruption <= 1 heure
KPI-11	Documentation de livraison	Toute livraison devra être validée et contractualisée avec les parties prenantes.	NC	1 livraison = 1 validation
KPI-12	Documentation technique	Toute fonctionnalité devra être documentée.	NC	1 fonctionnalité = 1 documentation
KPI-13	Coûts	Les coûts d'implémentation / migration et ceux inhérents à l'exploitation, et le calcul du retour sur investissements.	NC	Coûts = nouveau système < ancien système

6. Conclusion

Le plan d'implémentation, présenté en amont de cette section, a été défini afin d'assurer la réussite du projet de migration tout en assurant la continuité de service auprès des utilisateurs. Le calendrier¹⁰ proposé est en adéquation avec l'ambition du projet en termes de qualité, coût, délai et contrainte.

À noter que le budget de 50k€ est une contrainte très limitante, notamment en ce qui concerne le choix des ressources permettant d'assurer la migration, par conséquent, la direction de s'inscrire dans la durée pour compenser celle-ci a été prise.

 Le lecteur pourra se rapporter au second livrable contenant la feuille de route du projet de migration.