# Mini guide d'audit du Système d'Information

Auditez l'architecture de votre SI


Yann-Eric DEVARS

www.dynamap.fr
contact@dynamap.fr

# Sommaire

# 1. Introduction et objectifs de l’audit

L’audit d’architecture d’entreprise a pour vocation de clarifier la manière dont chaque composante du système d’information et chaque processus métier s’imbriquent.

Il offre un cadre d’analyse permettant de repérer les éventuels décalages entre la vision stratégique, les outils technologiques et la gouvernance en place.

Lorsque l’on parle d’architecture d’entreprise, on évoque à la fois les choix liés à la structuration de la DSI, la répartition des rôles et responsabilités, l’organisation des données, mais aussi la manière dont ces éléments servent la mission globale de l’entreprise.

## 1.1. Contexte de l’architecture d’entreprise

Une architecture d’entreprise bien construite facilite la communication entre les diverses entités (métier, direction, équipes techniques).

Elle aide à comprendre les interdépendances entre les applications, les processus et les infrastructures, ce qui se révèle fondamental pour éviter les doublons et réduire les coûts liés à la maintenance de briques informatiques redondantes.

Dans bien des cas, l'EA soutient la mise en œuvre de nouvelles stratégies, par exemple le déploiement d'outils analytiques avancés ou la refonte d'un parcours client.

Un tel alignement nécessite que chacun puisse se référer à une cartographie claire et actualisée, mettant en évidence les responsabilités, les flux de données et les règles de gouvernance.

***Lorsque le système d'information n'est pas harmonisé avec les objectifs de l'organisation, des dysfonctionnements apparaissent.***

Les équipes métiers peinent alors à obtenir les informations dont elles ont besoin, et la DSI se retrouve confrontée à des demandes contradictoires ou mal priorisées.

Dans ces conditions, les décisions d'investissement peuvent manquer de cohérence, car les enjeux business ne sont pas toujours bien traduits dans la conception et l'évolution des systèmes.

L'audit intervient justement pour identifier ces écarts et fournir des préconisations visant à les combler.

## 1.2. Objectifs généraux de l’audit

### Évaluer la cohérence de l’architecture par rapport à la stratégie de l’organisation

Un des premiers volets de l’audit consiste à mesurer l’adéquation entre la feuille de route stratégique et la structure actuelle du SI.

***Cette étape repose sur des échanges avec la direction générale, l’étude de documents stratégiques et l’analyse des projets en cours.***

L’idée est de vérifier si les efforts techniques convergent vers les mêmes priorités que les initiatives de transformation ou d’expansion.

### Identifier les forces et faiblesses du SI en termes de structure, de processus et de technologies

Ce diagnostic passe par l’examen détaillé des applications, des plateformes utilisées et des procédures de gestion de projet.

Les points forts se traduisent parfois par une bonne

intégration des services ou une architecture légère favorisant la rapidité de mise à jour.

Les faiblesses se manifestent sous forme de silos organisationnels, de données dupliquées ou de technologies obsolètes.

## Proposer des pistes d'amélioration et un plan d'action priorisé

L'audit aboutit à des recommandations concrètes et chiffrées.

Ces propositions concernent la rationalisation des applications, l'optimisation des processus internes ou encore l'adoption de frameworks plus adaptés.

Le plan d'action détaille l'ordre dans lequel les projets devraient être menés, ainsi que l'estimation de l'effort requis.

**Accompagner le changement et faciliter la gouvernance de l'architecture d'entreprise**

L’audit n’a de sens que s’il s’inscrit dans une dynamique de progrès continu.

Une fois les recommandations validées, il convient de mettre en place une gouvernance spécifique, avec des instances chargées de piloter l’évolution de l’EA.

Cette gouvernance inclut la définition de critères de décision, la coordination entre les métiers et la DSI, ainsi que la mise à jour régulière des référentiels et de la cartographie.

La finalité est de maintenir un équilibre entre innovation, maîtrise des risques et respect des objectifs stratégiques.

Un audit bien mené amène ainsi les parties prenantes à réfléchir aux moyens de faire évoluer l’entreprise dans son ensemble, plutôt que de se focaliser uniquement sur la dimension technologique.

En identifiant les liens entre les processus métiers, la structure applicative et les ressources humaines, il devient possible de valoriser chaque initiative au regard des priorités globales, et de bâtir un socle solide pour la croissance future.

# 2. Préparation de l’audit

La préparation de l’audit permet de définir les contours de la démarche et poser les bases d’une collaboration réussie entre les différents acteurs.

***Elle détermine les objectifs précis, les responsabilités de chacun, ainsi que les modalités de conduite de l’analyse.***

Sans cette étape, l’audit risque de manquer de clarté et de s’éloigner des attentes des parties prenantes.

## 2.1. Définition du périmètre

La première tâche est de fixer un périmètre organisationnel clair.

***Il s’agit de déterminer quelles entités seront concernées par l’audit : un département spécifique, l’intégralité de la DSI, une filiale à l’étranger ou même les partenaires externes.***

Le choix dépend souvent de la complexité de l’entreprise et de la nature des projets en cours.

Si l’ambition est de cartographier l’intégralité de l’architecture, il faudra veiller à inclure tous les

départements critiques, ainsi que les prestataires susceptibles d'impacter directement le Système d'Information.

À l'inverse, lorsque l'audit se concentre sur un domaine précis, on peut se limiter à un périmètre plus restreint pour en approfondir l'analyse.

Vient ensuite la définition du périmètre fonctionnel.

Cette partie consiste à cibler les grands processus métiers et les applications clés à auditer.

Certaines entreprises privilégient un périmètre large, par exemple en étudiant l'ensemble des applications financières ou l'ensemble des processus de gestion de la production.

D'autres choisissent une approche plus ciblée, comme la refonte d'un processus de commande ou d'un ERP spécifique.

Tout dépend des priorités stratégiques et de la disponibilité des ressources.

Il est impératif de préciser dès le début si l'audit s'étendra aux technologies émergentes (micro-services,

virtualisation, conteneurs) ou se concentrera sur des solutions déjà bien implantées.

*L'**échéance et le calendrier*** forment le dernier volet de cette préparation.

Un audit ne saurait être mené indéfiniment : il faut établir des jalons et des durées précises pour chaque phase.

Certains audits s'étendent sur quelques semaines, d'autres sur plusieurs mois.

Un calendrier réaliste tient compte de la disponibilité des parties prenantes, de la nécessité de recueillir des données fiables et de l'importance éventuelle d'intervenir sur plusieurs sites géographiques.

## 2.2. Gouvernance de l'audit

La gouvernance de l'audit s'organise généralement autour d'un **sponsor** ou comité de pilotage.

Le sponsor, souvent issu de la direction générale, valide les grandes orientations et veille à l'alignement avec la stratégie globale.

Le comité de pilotage, quant à lui, réunit les représentants des métiers, de la DSI et parfois des partenaires.

Son rôle est de suivre l'avancée de l'audit, de valider les choix méthodologiques et de faciliter la levée des éventuels obstacles.

*L'**équipe d'audit*** comprend plusieurs profils : architecte d'entreprise, responsable SI, experts fonctionnels, spécialistes de la sécurité, etc.

Chacun apporte son expertise et sa connaissance du terrain.

L'architecte d'entreprise coordonne souvent l'ensemble, en s'assurant que la démarche respecte les principes directeurs de la gouvernance et de l'architecture.

Le responsable SI contribue à l'identification des points faibles ou des contraintes techniques.

Les experts métier, quant à eux, fournissent la vision opérationnelle et guident la collecte d'informations liées aux processus et aux usages concrets.

Un plan de communication interne est indispensable pour tenir informées les équipes.

Il peut inclure des réunions de lancement, des points d'étape réguliers et la diffusion de comptes rendus.

L'objectif est de maintenir un niveau d'adhésion élevé et de faciliter le recueil des informations nécessaires.

Quand les métiers comprennent la finalité de l'audit et voient comment leurs retours seront pris en compte, ils coopèrent plus volontiers et partagent plus facilement leurs besoins.

## 2.3. Choix du référentiel ou des normes

Avant de démarrer l'analyse sur le terrain, il est utile de déterminer si l'on s'appuiera sur des référentiels reconnus tels que **TOGAF**, **Zachman**, **COBIT** ou **ITIL** et bien sûr **DYNAMAP**.

Ces cadres fournissent des bonnes pratiques pour mener l'audit et garantir une approche structurée.

TOGAF, par exemple, propose un cycle de vie (Architecture Development Method) et un vocabulaire commun pour décrire les briques de l'architecture.

Zachman apporte un modèle de classification basé sur plusieurs perspectives (planification, analyse, conception) et diverses interrogations (quoi, comment, où, qui, etc.).

DYNAMAP propose une démarche structurée progressive et inclus la démarche de questionnements indispensable aux audits.

***La personnalisation reste souvent nécessaire, car chaque organisation possède ses spécificités.***

Une PME de service n'a pas les mêmes priorités qu'une multinationale industrielle.

Les niveaux de maturité varient également d'une structure à l'autre : certaines maîtrisent déjà le concept d'architecture d'entreprise, d'autres en sont à leurs premiers essais.

L'essentiel est de retenir les éléments les plus pertinents du référentiel pour les adapter aux besoins réels.

En procédant ainsi, on s'assure que l'audit soit en phase avec la taille, le secteur d'activité et l'ambition digitale de l'entreprise.

Cette phase de préparation donne un cadre solide à l'audit.

Elle fixe le cap, éclaire la méthodologie et pose les fondations d'un travail collaboratif.

Lorsque tous les acteurs se savent impliqués et comprennent l'étendue de la mission, l'audit gagne en efficacité et produit des résultats plus utiles à l'organisation.

Pour aller plus précisément sur la démarche d'audit, retrouvez le framework DYNAMAP : www.dynamap.fr/le-framework

# 3. Collecte d’informations et mobilisation des acteurs

La phase de collecte d’informations et d’implication des différents intervenants constitue un moment décisif pour la réussite de l’audit.

Elle permet de recueillir les données indispensables à la compréhension du système d’information, tout en assurant la participation active des parties prenantes.

Grâce à une démarche structurée, on obtient une vision précise des processus en place, des défis rencontrés et des attentes exprimées, tant au niveau des métiers que de la DSI.

## 3.1. Méthodes de collecte

L’utilisation d’entretiens et questionnaires se révèle souvent très efficace pour collecter des informations directement auprès des personnes concernées.

Dans un premier temps, il est essentiel d’identifier les parties prenantes clés : direction générale, responsables de service, équipes IT et autres contributeurs majeurs.

Chaque entretien doit être préparé avec soin : une liste

de questions ciblées permet de cerner les grands enjeux, de comprendre les flux de travail ou encore d'anticiper les contraintes techniques.

Les questionnaires écrits, distribués à un public plus large, aident à capter des retours plus variés, en laissant aux répondants la possibilité de développer librement leurs points de vue.

Les ateliers collaboratifs sont tout aussi précieux, car ils favorisent l'échange et la co-construction.

Ces sessions, généralement courtes et dynamiques, permettent de faire ressortir rapidement les besoins, les irritants et les processus critiques.

Les participants peuvent, par exemple, travailler sur la cartographie de leur activité ou brainstormer autour des problèmes récurrents.

Grâce à la diversité des perspectives réunies, des solutions émergent plus facilement et les équipes prennent conscience des interdépendances entre leurs fonctions.

L'analyse documentaire complète ce dispositif en apportant une base factuelle à l'audit.

Consulter les organigrammes, les politiques d'entreprise ou encore les schémas d'architecture déjà existants donne un aperçu du cadre dans lequel s'inscrit le SI.

Les procédures métiers, les contrats techniques ou les contrats de support logiciel éclairent la manière dont les services sont structurés, sécurisés et maintenus.

La lecture de ces documents facilite la préparation des entretiens : on peut ainsi approfondir certains points restés flous ou vérifier les écarts entre la théorie et la pratique.

## 3.2. Mobilisation des acteurs métiers et IT

La planification des disponibilités s'avère cruciale pour coordonner l'ensemble de ces méthodes de collecte.

Dans un contexte où chaque collaborateur a déjà ses propres missions, il est essentiel de définir un calendrier raisonnable, permettant de conduire les ateliers et les entretiens sans perturber excessivement l'activité.

Il importe aussi de souligner en amont la valeur ajoutée de l'audit, afin que chacun s'investisse pleinement lors des différentes étapes.

La sensibilisation aux objectifs aide les participants à comprendre pourquoi leur contribution est attendue et comment elle sera exploitée.

En expliquant clairement que l'audit vise à améliorer le Système d'Information et à fluidifier les processus, on donne du sens à la démarche.

Les métiers comme les équipes IT se sentent concernés, ce qui renforce leur engagement et leur motivation à fournir des données pertinentes.

Pour obtenir des retours sincères et fiables, il convient d'instaurer un climat de confiance.

Lorsqu'on aborde des questions liées à la performance, aux responsabilités ou aux éventuels dysfonctionnements, les collaborateurs peuvent parfois hésiter à partager leurs difficultés.

En précisant que les informations recueillies sont destinées à mieux cerner les réalités de terrain, on encourage des échanges ouverts et constructifs.

Si nécessaire, la confidentialité de certaines données doit être garantie, afin de rassurer les intervenants et de préserver la qualité des retours.

Cette phase de collecte et de mobilisation détermine en grande partie la pertinence des conclusions de l'audit.

Elle permet de rassembler tous les éléments factuels et humains nécessaires à la compréhension du SI et de son environnement.

Lorsque la coordination entre métiers et IT est bien orchestrée, l'audit gagne en profondeur et débouche sur des recommandations mieux adaptées aux contraintes et ambitions réelles de l'organisation.

Pour aller plus précisément sur la démarche d'audit, retrouvez le framework DYNAMAP et notamment la première phase :
Analyse de l'existant : https://www.dynamap.fr/1-analyse-de-l-existant

# 4. Analyse de l’alignement stratégique

L’analyse de l’alignement stratégique consiste à évaluer la manière dont le Système d’Information soutient et matérialise la vision globale de l’entreprise.

Cette phase a pour but d’identifier les points de convergence entre les orientations stratégiques et les capacités technologiques, mais aussi de repérer d’éventuels écarts qui pourraient freiner l’exécution des priorités définies par la direction.

En examinant de près les objectifs de l’organisation, on peut mieux comprendre comment chacun d’eux se traduit concrètement dans la feuille de route informatique et dans les projets en cours.

Plus les équipes métiers et IT partagent une compréhension claire des ambitions de l’entreprise, plus il leur sera facile de coopérer et d’ajuster leurs décisions quotidiennes.

## 4.1. Objectifs stratégiques de l’entreprise

La première étape consiste à identifier les objectifs à court, moyen et long terme.

Ces objectifs peuvent prendre des formes variées : croissance du chiffre d'affaires, réduction des coûts d'exploitation, amélioration de la satisfaction client ou pénétration de nouveaux marchés.

Il est primordial de bien distinguer les cibles opérationnelles (par exemple, augmenter la productivité d'une équipe commerciale) des ambitions plus larges, comme renforcer la présence de l'entreprise dans un secteur émergent.

Chaque département ou direction peut disposer de sa propre liste de priorités, qui s'ajoute à la stratégie globale de l'organisation.

Une fois ces objectifs clarifiés, il s'agit de vérifier leur traduction dans la feuille de route SI et technologique.

Concrètement, cela revient à observer si les projets lancés par la DSI ou les investissements technologiques en cours répondent bien aux enjeux métier définis par la direction.

Par exemple, si l'entreprise vise l'excellence opérationnelle, des solutions de process mining ou de robotisation peuvent être envisagées.

Si la priorité est d'optimiser l'expérience client, des

outils de CRM avancés ou des plateformes de self-service peuvent être déployés.

Un examen minutieux de la documentation stratégique (business plans, budgets, plans à cinq ans) et de la liste des projets IT permet de faire un lien explicite entre les ambitions de l'entreprise et les initiatives technologiques.

## 4.2. Alignement stratégique et SI

L'alignement stratégique se mesure souvent grâce à une ***matrice objectifs / capacités SI***, qui met en évidence la correspondance entre chaque objectif majeur et les briques du Système d'Information.

On y recense, par exemple, les applications, les infrastructures ou les services qui contribuent à la réalisation de l'objectif visé.

Lorsque les correspondances sont claires, il devient plus aisé de voir quels projets sont réellement prioritaires, et quelles ressources mobiliser pour les mener à bien.

À l'inverse, si certains objectifs métiers ne trouvent pas de relais technologiques dans la matrice, cela indique un risque de décalage.

C’est dans ce cadre que ***l’évaluation des écarts*** prend tout son sens.

Il s’agit de repérer les éventuels manques, comme l’absence d’un outil d’analyse de données pour piloter la performance en temps réel.

Il peut aussi être question de technologies obsolètes, qui ne répondent plus aux standards actuels et freinent l’entreprise dans sa quête d’agilité.

Parfois, l’architecture applicative est trop fragmentée, entraînant des difficultés de communication entre les services ou un manque de fluidité dans la transmission de données.

Ces constats, s’ils sont bien documentés, aident à prioriser les évolutions à apporter au SI.

## 4.3. Risques stratégiques

Dans tout audit d’alignement, il est fondamental d’analyser les risques qui découlent d’une éventuelle incohérence entre la stratégie business et les choix technologiques.

Une entreprise souhaitant conquérir de nouveaux marchés peut se retrouver freinée par un SI incapable

de gérer de forts volumes de transactions, ou par un manque de modularité qui complique l'intégration de nouveaux partenaires.

Un autre exemple concerne le manque d'agilité : si l'adoption de nouvelles fonctionnalités requiert systématiquement des mois d'implémentation, l'organisation risque de rater des opportunités commerciales ou de rester en retard face à la concurrence.

De plus, l'absence de coordination entre les départements métiers et la DSI peut engendrer des retards dans la mise en œuvre de projets clés, voire des conflits de priorités.

Ces risques, lorsqu'ils sont clairement identifiés, servent de base à l'élaboration d'un ***plan d'action*** ciblé.

Au lieu de multiplier les initiatives dispersées, l'entreprise peut se concentrer sur quelques axes majeurs, comme la modernisation de son infrastructure, la mise en place d'une plateforme d'API pour accélérer les intégrations ou encore le renforcement des compétences internes en matière de data science.

En définitive, l'analyse de l'alignement stratégique offre

une vision globale des forces et faiblesses du SI au regard des ambitions de l'organisation.

Elle constitue un outil précieux pour ajuster la feuille de route et pour garantir que chaque projet, chaque ressource investie, serve réellement la stratégie de croissance et de différenciation de l'entreprise.

Pour aller plus précisément sur la démarche du rapport d'étonnement, retrouvez le framework DYNAMAP et notamment la deuxième phase :
Rapports d'étonnement : https://www.dynamap.fr/2-rapports-d-etonnement

# 5. Étude de l’architecture organisationnelle et fonctionnelle

L’architecture organisationnelle et fonctionnelle désigne la manière dont les processus métiers, les rôles et les responsabilités s’agencent pour soutenir les objectifs de l’entreprise.

Dans le cadre d’un audit, cette étude consiste à comprendre les mécanismes opérationnels, à analyser la cohérence des flux et à évaluer la performance globale.

Une bonne organisation garantit la fluidité des échanges entre les différents services et facilite l’adaptation aux évolutions du marché.

## 5.1. Cartographie des processus métiers

La première étape vise à identifier les macro-processus et processus critiques.

Parmi les macro-processus fréquemment étudiés figurent le cycle de vente, la logistique, la facturation ou encore le support client.

Chaque macro-processus se décompose en sous-processus et en tâches précises, dont la bonne

exécution est essentielle pour délivrer un produit ou un service de qualité.

L'objectif est de délimiter ces processus de manière claire, en repérant les points de jonction et les éventuelles zones de chevauchement.

Une fois cette liste établie, il importe de vérifier la cohérence des flux et les interdépendances internes et externes.

Certains flux concernent des échanges de données entre départements (comptabilité, production, achats), d'autres impliquent des partenaires ou des fournisseurs extérieurs.

Une cartographie détaillée fait ressortir les éventuels goulets d'étranglement, les reprises manuelles et les risques d'erreur.

Dans une organisation fortement digitalisée, ces flux circulent au travers de multiples applications : ERP, CRM, outils de planification, plateformes e-commerce, etc.

L'audit met en évidence la manière dont ces solutions interagissent et si elles répondent efficacement aux besoins des métiers.

## 5.2. Rôles et responsabilités

La pertinence de l'organigramme se vérifie en comparant les missions de chaque service avec les macro-processus identifiés.

L'organigramme doit refléter la réalité opérationnelle et faciliter la collaboration.

Lorsque certains processus clés ne correspondent à aucun poste clairement défini, des dysfonctionnements peuvent émerger : retards de décision, manque de supervision ou conflits de priorité.

En parallèle, la répartition des rôles doit être ajustée pour éviter de cumuler trop de tâches critiques sur un seul service ou une seule personne.

Il convient également de vérifier la clarté des responsabilités autour du SI et de l'architecture d'entreprise.

En pratique, on s'assure que chacun sait qui gère la gouvernance, qui définit les standards technologiques et qui valide les modifications majeures.

Cette clarté est nécessaire pour éviter les doublons et

pour garantir une cohérence dans les décisions d'évolution du SI.

Sans une répartition explicite, l'architecture peut dériver, enchaînant les projets contradictoires ou inutiles.

## 5.3. Indicateurs de performance

Les indicateurs de performance (KPIs) servent à mesurer l'efficacité et la qualité des processus.

Ils permettent de quantifier la vitesse de traitement, le taux d'erreur, la satisfaction client ou encore le coût opérationnel.

Un examen rigoureux recense les KPIs déjà en place, tout en vérifiant leur pertinence au regard des objectifs de l'entreprise.

S'il manque des indicateurs pour évaluer un processus critique, il devient difficile de détecter les dysfonctionnements et de mesurer les progrès réalisés.

Une question clé consiste à savoir si le SI permet de mesurer et suivre facilement ces indicateurs.

Certains outils génèrent des tableaux de bord en temps

réel, d'autres nécessitent des extractions manuelles, plus longues et sujettes à l'erreur.

Lorsque la collecte de données se fait sans automatisation, les équipes perdent un temps précieux et risquent de manquer de fiabilité.

L'audit souligne alors les améliorations possibles, comme l'intégration d'une solution de reporting ou l'harmonisation des formats de données.

L'étude de l'architecture organisationnelle et fonctionnelle éclaire la manière dont l'entreprise s'appuie sur ses processus et ses rôles pour atteindre ses objectifs.

Elle met en évidence les points forts, par exemple une bonne communication entre services, et les axes d'amélioration, tels que la nécessité de clarifier certaines responsabilités ou d'adopter des outils plus performants pour piloter les KPIs.

Pour aller plus précisément sur la démarche de cartographie, retrouvez le framework DYNAMAP et notamment la troisième phase :
Cartographies et points de vue :
https://www.dynamap.fr/3-cartographies-et-points-de-vue

# 6. Analyse de l’architecture applicative

Cette section s’intéresse à la manière dont les différentes applications de l’entreprise interagissent et se complètent pour servir les processus métiers.

En évaluant de près les solutions existantes, leurs interfaces et leur cohérence globale, on peut mesurer la pertinence du domaine applicatif, repérer les redondances et prévoir les améliorations nécessaires.

## 6.1. Inventaire des applications

La première étape consiste à réaliser ou mettre à jour le portfolio applicatif.

Ce recensement couvre l’ensemble des systèmes en production : noms des applications, versions installées, éditeurs, propriétaires internes, niveaux de criticité et coûts associés.

En procédant ainsi, on obtient une vision claire de l’existant, permettant de repérer immédiatement d’éventuels doublons ou des applications obsolètes.

Il arrive parfois que des outils hérités continuent de fonctionner sans que personne n’ait une vue

d’ensemble, ce qui génère un risque élevé en termes de sécurité et de maintenance.

Au-delà de la simple liste, il est judicieux d’identifier les applications redondantes ou non utilisées.

Certaines fonctions peuvent être assurées par plusieurs systèmes, entraînant des coûts superflus et une complexité de gestion accrue.

Dans d’autres cas, une application a peut-être été remplacée, mais subsiste toujours dans le portefeuille, mobilisant inutilement des ressources.

Une fois les doublons révélés, l’entreprise peut planifier leur retrait progressif ou leur consolidation.

## 6.2. Interactions et interfaces

Pour comprendre la dynamique entre les applications, il faut ensuite cartographier les flux de données.

Que ce soit entre un **ERP**, un **CRM** ou des outils plus spécialisés (gestion de production, BI, etc.), ces échanges conditionnent la bonne circulation de l’information.

En identifiant précisément l’origine, la destination et la fréquence des flux, on repère les éventuelles ruptures

ou lenteurs susceptibles de perturber le fonctionnement quotidien.

Par exemple, un flux critique pouvant être bloqué par une passerelle surchargée constitue un risque majeur pour la continuité des opérations.

Analyser la fluidité des échanges permet de voir si des interfaces peuvent être rationalisées ou mises à jour.

Il se peut que certaines intégrations aient été développées sous forme de scripts ponctuels, difficiles à maintenir.

Dans d'autres cas, des solutions de middleware assurent déjà une bonne orchestration, mais nécessitent un suivi ou une mise à niveau.

## 6.3. Évaluation de la cohérence

Enfin, cette analyse doit aboutir à une évaluation de la cohérence globale.

On vérifie l'homogénéité des technologies utilisées, la compatibilité des frameworks et la pertinence des approches d'intégration.

Si une partie du SI repose sur un socle modernisé alors

qu'une autre dépend de technologies en fin de vie, l'architecture peut se révéler fragile et peu évolutive.

L'audit met également en évidence les **doublons fonctionnels** ou les **incompatibilités techniques**.

Parfois, deux applications différentes couvrent un même besoin métier, entraînant une multiplication des coûts et un risque de divergence des données.

À l'inverse, une incompatibilité entre systèmes peut obliger à des manipulations manuelles, cause de retard et de saisies répétitives.

En consolidant ces informations, l'organisation obtient une vision globale et peut prioriser les améliorations à apporter pour renforcer la solidité et la pertinence de son architecture applicative.

Pour aller plus précisément sur la démarche de cartographie, retrouvez le framework DYNAMAP et notamment la troisième phase :
Cartographies et points de vue :
https://www.dynamap.fr/3-cartographies-et-points-de-vue

# 7. Analyse de l’architecture technologique et infrastructurelle

L’architecture technologique et infrastructurelle constitue le socle sur lequel reposent toutes les applications et tous les services métier.

En analyser la robustesse et la cohérence permet de garantir la continuité des opérations, de maîtriser les coûts et de préparer l’entreprise aux évolutions futures.

Il s’agit non seulement de dresser un inventaire détaillé des ressources matérielles et logicielles, mais aussi d’évaluer leur adéquation avec les besoins en performance, résilience et sécurité.

## 7.1. Inventaire des infrastructures

La première étape consiste à répertorier l’ensemble des éléments qui composent la pile technologique : centres de données, serveurs physiques et virtuels, réseau, solutions de stockage, plateformes de virtualisation et de conteneurs, ainsi que les éventuels services cloud.

Ce travail permet de clarifier la couverture géographique (implantation des data centers, répartition des serveurs) et de repérer les configurations spécifiques susceptibles d’impacter la disponibilité des services.

Durant cet inventaire, il est recommandé d'identifier les éléments critiques, c'est-à-dire ceux dont la panne pourrait interrompre un processus vital pour l'entreprise.

On se penche également sur la capacité de chaque composant (bande passante réseau, volume de stockage, puissance de calcul) en regard des charges actuelles et à venir.

Cette prise de recul facilite la détection d'éventuels goulets d'étranglement et prépare les arbitrages en cas de nécessité d'extension ou de migration.

## 7.2. Normes et standards techniques

L'examen des normes et standards techniques vise à vérifier l'adoption de pratiques reconnues, qu'il s'agisse de protocoles réseau, de règles de sécurité ou d'exigences de compatibilité entre systèmes.

Un usage cohérent de ces standards contribue à la solidité de l'infrastructure, tout en rendant plus simple et moins coûteuse l'interopérabilité avec d'autres environnements.

Il est donc préférable de vérifier la présence de certifications éventuelles, l'application des bonnes

pratiques en matière de chiffrement et le respect des réglementations en vigueur.

La question des mises à jour et de la gestion des obsolescences occupe une place centrale dans cet audit.

Une politique claire en la matière garantit que les correctifs de sécurité sont appliqués sans retard, évitant ainsi des vulnérabilités qui pourraient compromettre le bon fonctionnement du SI.

L'identification de composants en fin de vie ou non supportés permet par ailleurs de planifier le remplacement ou la migration de manière proactive, limitant les interruptions de service.

## 7.3. Performance et résilience

Enfin, il convient d'évaluer la performance de l'architecture et sa capacité à soutenir les pics de charge.

Pour certaines entreprises, ces pics se produisent lors de périodes saisonnières (soldes, fin d'année fiscale), pour d'autres, ils peuvent survenir de manière imprévisible.

La flexibilité de l'environnement, la répartition de la

charge sur plusieurs serveurs et la possibilité de monter en puissance rapidement sont autant de facteurs à analyser.

En parallèle, la résilience se mesure en vérifiant l'existence et la pertinence des mécanismes de sauvegarde et de restauration.

Un plan de reprise d'activité (PRA) bien conçu définit les scénarios de crise, les délais de rétablissement (RTO) et les points de reprise (RPO).

L'identification des points faibles, tels que les single points of failure, contribue à mieux cibler les actions de renforcement à mener.

Si l'architecture présente trop de dépendances critiques ou un seul centre de données, le risque de panne majeure augmente, et la continuité d'activité peut être compromise en cas d'incident.

Pour aller plus précisément sur la démarche de cartographie, retrouvez le framework DYNAMAP et notamment la troisième phase :
Cartographies et points de vue :
https://www.dynamap.fr/3-cartographies-et-points-de-vue

# 8. Analyse de l’architecture des données

L’architecture des données regroupe l’ensemble des principes, des pratiques et des outils qui assurent la bonne gestion, la qualité et la sécurité de l’information au sein de l’entreprise.

## 8.1. Gouvernance des données

La gouvernance des données concerne toutes les règles et les processus visant à organiser la collecte, la manipulation et l’utilisation des informations critiques.

Un dispositif de gouvernance bien conçu s’appuie sur des rôles clairement définis, comme le Data Owner, responsable de la qualité et de la conformité des données, ou le Data Steward, chargé de la maintenance opérationnelle des référentiels.

Ces rôles assurent une répartition des tâches qui évite les duplications et les confusions de responsabilité.

Dans l’audit, on s’intéresse particulièrement aux politiques de gouvernance de la donnée en place, ainsi qu’aux règles de partage et de confidentialité des données.

Les équipes doivent connaître les règles de stockage, de

diffusion et de suppression ***afin de respecter les exigences légales et de préserver la valeur de l'information.***

Une attention spéciale est portée à l'existence d'un dictionnaire de données et d'un glossaire métier, qui facilitent la compréhension et l'harmonisation de la terminologie dans l'ensemble de l'entreprise.

***Sans un vocabulaire commun, les différentes entités risquent de manipuler des informations identiques sous des noms distincts, compliquant ainsi leur exploitation et leur consolidation.***

## 8.2. Qualité et intégrité

L'évaluation de la qualité des données est une composante centrale de l'audit, car elle détermine en grande partie la fiabilité des rapports, des analyses et des prises de décision.

Cette qualité se mesure notamment à travers l'exhaustivité (taux de données manquantes), la fiabilité (présence d'erreurs ou de valeurs incohérentes), la cohérence (homogénéité des formats), ou encore la rapidité de mise à jour.

Si les données sont obsolètes ou imprécises, même les

meilleurs outils d'analyse ne pourront produire des résultats pertinents.

Les doublons et divergences sont des symptômes fréquents d'une gouvernance insuffisante.

Il peut arriver qu'un même client ou une même référence produit soit enregistré plusieurs fois dans différentes bases, créant de la confusion et des écarts entre les rapports.

De même, les flux manuels ou multiples intégrations peuvent générer des retards et des problèmes de synchronisation qui nuisent à l'intégrité du patrimoine informationnel.

En identifiant ces goulots d'étranglement, l'audit aide à prioriser les actions correctives : adoption d'un outil de ***Master Data Management (MDM),*** automatisation de la collecte, normalisation des formats, etc.

## 8.3. Sécurisation et conformité

Dans le contexte actuel, la sécurisation des données revêt une importance capitale, tant pour protéger l'activité de l'entreprise que pour respecter les exigences légales.

L'audit vérifie la conformité réglementaire aux textes en

vigueur, tels que le RGPD (Règlement Général sur la Protection des Données) en Europe, ou certaines normes sectorielles dans la santé, la finance ou la défense.

La non-conformité peut entraîner des sanctions financières importantes et porter préjudice à la réputation de l'organisation.

Différents mécanismes de protection peuvent être examinés lors de cette phase : chiffrement en transit ou au repos, anonymisation des données sensibles, ou encore contrôles d'accès robustes.

L'objectif est d'évaluer si les processus de sécurité existants sont à la fois efficaces et cohérents avec le niveau de risque associé à chaque type de donnée.

Des outils de monitoring, des alertes en cas de tentative d'accès non autorisé et des procédures de gestion d'incident viennent compléter ce dispositif.

De manière générale, l'analyse de l'architecture des données fournit un aperçu complet de la manière dont l'organisation collecte, gère et sécurise ses informations essentielles.

Elle révèle les lacunes éventuelles au niveau de la

gouvernance, de la qualité ou de la conformité, tout en soulignant les bonnes pratiques à pérenniser.

Lorsque l'ensemble du SI repose sur des données fiables et sécurisées, l'entreprise peut exploiter pleinement son capital informationnel, prendre de meilleures décisions et développer de nouveaux services basés sur l'intelligence artificielle ou l'analyse prédictive.

Pour aller plus précisément sur la démarche de gouvernance de la donnée, retrouvez la méthode DYNAMAP et notamment le guide de gouvernance de la donnée :
https://www.dynamap.fr/boutique/la-gouv-de-la-donnee

# 9. Analyse de l’architecture de sécurité

La sécurité occupe une place centrale dans l’architecture d’entreprise, car elle garantit la protection des informations stratégiques, des données personnelles et de la réputation de l’organisation.

Une architecture de sécurité solide repose sur un ensemble de politiques claires, de contrôles techniques et de processus de gouvernance qui permettent d’anticiper les menaces et de réagir efficacement en cas d’incident.

## 9.1. Politique de sécurité

La première étape consiste à vérifier l’existence d’une politique formelle de sécurité.

Il peut s’agir d’une Politique de Sécurité des Systèmes d’Information (PSSI) interne ou de l’adoption de référentiels reconnus, comme les normes **ISO 27001** ou **NIST**.

Cette politique doit couvrir les grands principes de protection des données et préciser les responsabilités de chacun : direction, DSI, métiers.

En l’absence d’un tel document, l’organisation risque de manquer de cohérence dans la mise en œuvre de ses mesures de sécurité.

Une fois la politique identifiée, on valide sa mise en œuvre concrète.

Cela concerne les contrôles d’accès (définition et répartition des droits), les méthodes d’authentification (mots de passe robustes, authentification multifacteur), ainsi que la gestion fine des habilitations.

L’objectif est de s’assurer que chaque collaborateur ne puisse accéder qu’aux ressources strictement nécessaires à l’accomplissement de ses missions, réduisant ainsi le risque d’erreur ou de fuite de données.

## 9.2. Risques et vulnérabilités

La cartographie des risques est un volet essentiel de l’audit.

Elle permet d’identifier les menaces majeures telles que les cyberattaques, les fuites ou vols de données, les tentatives de déni de service et les ransomwares.

Cette étape implique un échange approfondi avec les équipes responsables de la sécurité (RSSI, SOC) pour

comprendre quelles sont les sources de vulnérabilités recensées et les mécanismes de défense mis en place.

Dans un second temps, on audite la posture de sécurité.

Cela passe par l'examen des pares-feux, des solutions antivirus, des outils de détection d'intrusion (IDS/IPS) et du patch management (gestion des correctifs).

Une attention particulière est portée aux systèmes anciens, aux logiciels non maintenus et aux défauts de configuration qui pourraient servir de porte d'entrée à un attaquant.

Il convient également d'évaluer le niveau de sensibilisation du personnel, car l'ingénierie sociale reste l'une des méthodes les plus courantes pour contourner les défenses techniques.

## 9.3. Continuité et plan de crise

La sécurité ne se limite pas à la prévention : elle englobe aussi la capacité de l'entreprise à se relever d'un incident majeur.

On vérifie l'existence d'un plan de continuité d'activité (PCA) et d'un plan de reprise d'activité (PRA), documents qui définissent comment l'organisation

assure la continuité de ses opérations en cas de crise (panne informatique, désastre naturel, cyberattaque).

Le PCA se concentre sur les solutions provisoires pour maintenir un niveau minimal de service, tandis que le PRA vise à rétablir les systèmes principaux dans les délais prévus (RTO et RPO).

Il est souhaitable de tester ou de valider l'existence de tests réguliers pour s'assurer que ces plans fonctionnent réellement sur le terrain.

De nombreux incidents démontrent que les plans ne sont pas toujours mis à jour ou que les équipes ne sont pas suffisamment formées.

Des exercices de simulation, des scénarios de crise et des audits périodiques renforcent la résilience et permettent de repérer d'éventuels points faibles avant qu'ils ne se transforment en incidents critiques.

L'architecture de sécurité doit être envisagée comme un dispositif vivant, évoluant en fonction des menaces et des besoins de l'entreprise.

Quand la politique de sécurité, la gestion des risques et la continuité d'activité sont correctement intégrées à la gouvernance globale du SI, l'organisation gagne en

sérénité et peut se concentrer sur ses objectifs stratégiques sans craindre de perturbations majeures.

Pour aller plus précisément sur la démarche d'architecture de la sécurité, retrouvez les guides DYNAMAP et notamment les guides cybersécurité et PRA :

https://www.dynamap.fr/boutique/cyber-securite-l-essentiel

# 10. Évaluation de la gouvernance, des processus et de la maturité

Cette section vise à apprécier la manière dont l'organisation pilote son architecture d'entreprise, gère le cycle de vie des applications et progresse dans sa démarche d'amélioration continue.

Une gouvernance bien établie et des processus maîtrisés contribuent à la cohérence d'ensemble, tandis que la maturité se mesure par la capacité à adapter ces processus aux besoins évolutifs de l'entreprise.

## 10.1. Gouvernance de l'architecture d'entreprise

La gouvernance de l'architecture recouvre la façon dont sont prises les décisions relatives au SI, du choix des technologies à l'arbitrage budgétaire.

Dans un audit, on commence par identifier les instances en place : comité d'architecture, comité de pilotage, une gouvernance d'architecture.

Le rôle des architectes, qu'ils soient fonctionnels, techniques ou d'entreprise, est également passé en revue.

Il s'agit de déterminer si chacun de ces acteurs sait exactement quelles responsabilités lui incombent et si des mécanismes de collaboration efficaces existent avec les équipes métiers et la DSI.

Ensuite, on vérifie les mécanismes de revue.

Une design authority ou un comité d'architecture régulier offrent un espace pour débattre des propositions, valider les évolutions majeures et s'assurer de leur alignement avec la stratégie.

Si de tels mécanismes font défaut, des projets peuvent naître hors de tout contrôle, engendrant une prolifération d'initiatives incohérentes et des dépenses superflues.

L'audit évalue donc la clarté des processus de validation, ainsi que la capacité de l'organisation à documenter, partager et faire respecter les standards retenus.

## 10.2. Processus de gestion du cycle de vie applicatif

La gestion du cycle de vie applicatif recouvre les méthodes de développement, de test, de déploiement et de maintenance.

Pour dresser un état précis, on recense les pratiques en vigueur : **DevOps**, **Agile**, **Waterfall** ou un mix de plusieurs approches.

Chaque méthode a ses avantages et ses contraintes, mais le plus important est qu'elle soit appliquée de manière cohérente, avec un suivi rigoureux et une bonne visibilité pour les parties prenantes.

On apprécie également la maturité en gestion de projet, depuis la phase de conception jusqu'à la mise en production et la maintenance.

La qualité de la documentation technique et fonctionnelle est un indicateur clé : sans documentation fiable, le transfert de connaissances devient difficile, notamment lorsqu'une équipe quitte le projet ou qu'il faut effectuer des corrections rapides.

La réactivité aux incidents est un autre point critique : des processus bien rôdés permettent de détecter et de résoudre rapidement les problèmes, minimisant l'impact sur les opérations métiers.

## 10.3. Modèles de maturité

Pour qualifier le niveau de maîtrise de l'organisation, on utilise souvent un modèle de maturité, comme **CMMI**, **COBIT** ou d'autres référentiels spécialisés.

Ces cadres évaluent la maturité sur plusieurs domaines : processus (efficacité, standardisation), organisation (rôles, gouvernance) et technologies (outils, automatisation).

Le résultat se présente souvent sous la forme d'un score ou d'un niveau (initial, géré, défini, quantitativement géré, optimisé), offrant une vision synthétique de la progression possible.

Il est alors nécessaire d'identifier le niveau actuel et le niveau cible souhaité.

Certaines entreprises visent l'excellence dans tous les domaines, tandis que d'autres préfèrent progresser par paliers, en améliorant d'abord les fondations.

L'audit propose ainsi un cheminement adapté, tenant compte des ressources disponibles, de la culture interne et des priorités stratégiques.

Cette approche graduée, soutenue par un suivi régulier, permet d'ancrer progressivement les meilleures pratiques et de faire évoluer l'architecture au rythme de la croissance de l'organisation.

Pour aller plus précisément sur la démarche d'audit, retrouvez le framework DYNAMAP : www.dynamap.fr/le-framework

# 11. Synthèse, recommandations et plan d'actions

Une fois l'audit achevé, il est nécessaire de regrouper et de présenter clairement l'ensemble des observations recueillies afin de faciliter la prise de décision.

Cette étape ultime permet non seulement de mettre en lumière les points forts et les zones de vulnérabilité, mais aussi de proposer des recommandations concrètes pour guider la transformation de l'architecture d'entreprise.

## 11.1. Consolidation des constats

La consolidation des constats peut prendre la forme d'un tableau SWOT (Forces, Faiblesses, Opportunités, Menaces) ou d'un rapport plus détaillé.

Le format choisi dépend souvent de la culture de l'organisation et de l'usage envisagé (présentation en comité, diffusion aux équipes, etc.).

L'essentiel est de rendre lisible la synthèse en insistant sur les éléments les plus critiques, comme les **goulots d'étranglement**, les **incohérences stratégiques** ou les **risques majeurs** identifiés au cours de l'audit.

En s'appuyant sur les informations rassemblées dans les chapitres précédents, on souligne les aspects clés :

- Les atouts actuels (technologies performantes, bonne gouvernance, compétences internes solides)
- Les dysfonctionnements ou lacunes à corriger (absence de stratégie claire pour la donnée, manque de documentation, applicatifs obsolètes, etc.)

Cette synthèse offre une vue d'ensemble qui aide les décideurs à comprendre la situation dans son ensemble, sans se noyer dans un trop-plein de détails techniques.

## 11.2. Recommandations et priorités

Sur la base des constats, l'audit propose des solutions concrètes.

Ces recommandations peuvent concerner la rationalisation d'applications (fusion de deux outils similaires, suppression des systèmes sous-utilisés), la refonte de processus métiers jugés trop complexes ou la modernisation d'infrastructures vieillissantes.

En reliant chaque recommandation à une problématique identifiée, on montre clairement sa valeur ajoutée et son impact potentiel.

Une étape importante consiste à prioriser les actions en fonction de leur influence sur le métier et de la complexité de mise en œuvre.

Les projets à fort impact et à effort modéré sont souvent à traiter en priorité, tandis que les initiatives plus coûteuses et à bénéfice incertain peuvent être reconsidérées ou reportées.

Certains besoins stratégiques, comme l'adoption de standards de sécurité ou la mise en place d'un nouveau modèle de gouvernance, peuvent en revanche nécessiter des investissements conséquents mais indispensables.

Il est ensuite conseillé de définir une roadmap couvrant plusieurs horizons temporels :

- **Court terme (6 mois)** : Actions correctives urgentes, mise en conformité réglementaire, sécurisation rapide de points critiques.
- **Moyen terme (1 an)** : Projets d'envergure moyenne, tels que la réorganisation de certains processus métiers ou la consolidation de la cartographie applicative.
- **Long terme (2-3 ans)** : Transformations structurelles, adoption d'innovations majeures et déploiement à grande échelle de nouvelles pratiques (ex. déploiement d'un cadre de

référence EA complet, migration vers un socle technologique unifié).

## 11.3. Plan de transformation

Pour rendre ces recommandations opérationnelles, le plan de transformation doit présenter l'enchaînement logique des initiatives.

Il peut être préférable de commencer par renforcer la **gouvernance**, afin de poser des bases solides, avant de s'attaquer à la **consolidation du socle technologique** ou à la **refonte des processus métiers**.

Un déploiement étape par étape évite une dispersion des ressources et facilite l'appropriation des changements par les équipes concernées.

Ce plan de transformation doit également identifier les ressources nécessaires.

Il s'agit ici de préciser les moyens humains (ex. recrutement de nouveaux profils, formation des équipes existantes), budgétaires (investissements matériels, licences logicielles, éventuels coûts de conseil) et techniques (acquisition de serveurs, virtualisation, licences cloud, etc.).

Le dimensionnement correct de ces ressources est

essentiel pour que la feuille de route soit réaliste et pour éviter les retards liés à un manque de moyens.

Dans l'idéal, ce plan est révisé périodiquement en comité de pilotage, afin de suivre l'avancement, de réévaluer les priorités si nécessaire et d'intégrer les retours d'expérience.

Ainsi, l'ensemble de l'organisation peut se projeter dans une dynamique de transformation continue et bénéficier pleinement des améliorations proposées par l'audit.

Pour aller plus précisément sur la démarche d'audit, retrouvez le framework DYNAMAP : www.dynamap.fr/le-framework

# 12. Conclusion et suivi post-audit

L'aboutissement d'un audit d'architecture d'entreprise ne se limite pas à la production d'un rapport.

Il s'agit d'ouvrir la voie à une amélioration continue, de piloter la mise en œuvre des recommandations et d'instaurer une dynamique de collaboration pérenne entre tous les acteurs de l'organisation.

## 12.1. Présentation des résultats

La première étape consiste à restituer officiellement les conclusions de l'audit.

Cette présentation, souvent destinée à l'équipe de direction et aux principales parties prenantes (comité d'architecture, responsables métiers, DSI), doit être conçue pour mettre en avant les informations essentielles.

Un document complet décrivant l'ensemble du processus, des constats et des recommandations est alors partagé, ***tandis qu'un rapport synthétique sera également produit (les décideurs ayants rarement le temps de s'attarder sur les détails).***

Ce double format permet de répondre aux besoins de différents publics : d'un côté, les experts et les

opérationnels qui souhaitent entrer dans le détail, de l'autre, la direction, désireuse d'identifier rapidement les points majeurs et les actions stratégiques.

La qualité de cette restitution influe largement sur l'adhésion et l'engagement futurs.

En soulignant les bénéfices attendus (gains de performance, réduction des coûts, meilleure sécurité, etc.), on démontre la valeur ajoutée du travail réalisé.

De plus, la transparence quant aux risques identifiés et aux efforts nécessaires renforce la confiance et la crédibilité de la démarche.

## 12.2. Pilotage de la mise en œuvre

Une fois les résultats validés, le vrai défi consiste à définir des indicateurs de suivi pour chaque recommandation.

Ces KPI peuvent porter sur le déploiement effectif des solutions (pourcentage de serveurs migrés, nombre de processus mis à jour), sur le respect des jalons (délais de réalisation), ou encore sur le suivi budgétaire (écarts par rapport aux prévisions).

Leur rôle est de mesurer la progression et de détecter

rapidement d'éventuels dérapages, afin d'y remédier sans attendre.

Des comités de suivi réguliers doivent être organisés pour ajuster le plan d'actions en fonction des retours du terrain et des évolutions stratégiques.

Idéalement, ces comités rassemblent la direction, la DSI, les métiers et l'architecte d'entreprise, de façon à couvrir l'ensemble des perspectives.

En suivant un calendrier prédéfini, on évite que les projets lancés à la suite de l'audit ne se perdent dans les priorités quotidiennes.

## 12.3. Retour d'expérience et amélioration continue

Enfin, il est essentiel de mettre en place un processus d'amélioration continue, surtout dans un environnement où les technologies et les besoins métiers évoluent en permanence.

L'actualisation régulière de la cartographie et du référentiel d'architecture garantit que l'entreprise dispose toujours d'une vision à jour de son SI, ce qui prévient les dérives et les pertes de cohérence.

Cet entretien peut être confié à un comité

d’architecture, qui s’assure que les changements proposés respectent les standards définis et restent alignés avec la stratégie globale.

Au-delà de la simple mise à jour des documents, il convient aussi d’encourager la culture d’architecture d’entreprise par des formations, des ateliers de sensibilisation ou la participation à des communautés de pratique.

Lorsque les équipes métiers et la DSI partagent une même vision, les arbitrages se font plus rapidement, et la pertinence des choix technologiques s’en trouve renforcée.

***Cette culture commune favorise en outre la création de synergies entre les projets, évitant les redondances et les incompatibilités.***

Pour aller plus précisément sur la démarche d’audit, retrouvez le framework DYNAMAP : www.dynamap.fr/le-framework

# Le mot de la fin

J'espère que ce guide vous a apporté les réponses aux questions générales que vous vous posez sur votre système d'information et vous permettra d'initier une première démarche.

Rappel : ce guide ne pas remplacer le travail d'expertise et d'adaptation au contexte de votre organisation tel que le ferai un expert dédié à l'audit de votre Système d'Information.

Yann-Eric DEVARS

Profil Linkedin :

https://www.linkedin.com/in/yann-eric-devars-architecte-entreprise

Site Internet : www.dynamap.fr

DYNAMAP©

# Connaitre et faire évoluer son SI


# Manuel de cartographie Architecture d'entreprise


Yann-Eric DEVARS

# Manuel de survie de l'architecte du SI

# Manuel de survie

## Architecte du Système d'Information


Yann-Eric DEVARS

DYNAMAP©

# 45 livrables détaillés et expliqués

## Livrables architecture d'entreprise




*Yann-Eric DEVARS*

# La gouvernance de la donnée


# Manuel de gouvernance de la donnée

Yann-Eric DEVARS

# Le plan de reprise d'activité


Yann-Eric DEVARS

# Architecture pour la sécurité des Systèmes d'Information selon le modèle OSI


Yann-Eric DEVARS

# La gestion économique des systèmes d'information


## L'économie du Système d'Information

Yann-Eric DEVARS