

# Compliance Assessment Document

## Introduction

**Objectif :** Vérifier que l'architecture développée est conforme aux normes, réglementations et meilleures pratiques définies dans le cadre du projet, en alignant le document avec le cadre TOGAF, l'architecture cible définie, et la roadmap.

---

## 1. Description Générale de l'Architecture

### Contexte du Projet :

- **Client :** SCS Magazine
- **Objectif :** Développer une Gestion Électronique de Documents pour améliorer la gestion des articles.
- **Attentes Principales :** Versionning des articles, suivi des modifications, système de commentaires.

### Architecture Cible :

- **Front Layer :** Utilisation de frameworks modernes (React, Angular) pour un design réactif et des composants réutilisables.
  - **Service Layer :** Implémentation en Java avec des principes RESTful, utilisation d'une API Gateway, architecture microservices.
  - **Data Layer :** Sécurisation des accès avec des drivers de connexion, utilisation de bases de données hybrides, politiques de sauvegarde et de restauration.
  - **Déploiement :** Utilisation de Docker pour la conteneurisation, Kubernetes pour l'orchestration, CI/CD pour les déploiements automatisés.
  - **Sécurité :** Chiffrement via HTTPS, mécanismes robustes d'authentification et d'autorisation, audits de sécurité réguliers.
-

## 2. Checklist de Conformité pour l'Architecture Cible

### **Applications :**

- L'approche micro-frontend a-t-elle été correctement respectée en intégrant des composants modulaires et réutilisables ?
- Le backend utilise-t-il des microservices correctement configurés avec Spring Boot et l'api gateway Kong ?
- Les interfaces utilisateurs respectent-elles les standards de design responsive et s'adaptent-elles correctement sur mobile, tablette et ordinateurs ?
- L'application dispose-t-elle de toutes les fonctionnalités définies dans le cahier des charges ?
- L'application a-t-elle été testée avec des tests unitaires et d'intégrations afin de garantir une couverture de tests supérieure à 90% ?
- L'application utilise-t-elle le mécanisme de versioning Github ?

### **Gestion des données :**

- Les données sont-elles stockées de manière sécurisée et conforme aux réglementations en vigueur tel que la RGPD ?
- Les mécanismes de sauvegarde pour les bases de données tel que PGBackRest sont-ils fonctionnels ?

### **Sécurité :**

- Les communications entre les composants sont-elles chiffrées en HTTPS ?
- Les mécanismes d'authentification et d'autorisation sont-ils robustes et conformes aux standards tels que OAuth2.0 ?

### **Infrastructures :**

- L'infrastructure réseau supporte-t-elle les besoins en bande passante et en latence pour permettre une utilisation fluide du service ?
- Les composants du système sont-ils conteneurisés avec Docker pour assurer la scalabilité et le déploiement efficace ?

## Méthodes et outils :

- Les moyens de déploiement sont-ils efficaces et automatisés ?
  - Les outils de développement et de test sont-ils alignés avec les meilleures pratiques ?
  - Les méthodes de gestion de projet utilisées permettent-elles une adaptation rapide aux changements ?
- 

## 3. Évaluation des Conformités Techniques et Fonctionnelles

KPI	Description	Objectif Cible	Fréquence de Mesure
<b>Temps de Réponse des Applications</b>	Temps moyen de réponse des services applicatifs.	< 300 ms	Hebdomadaire
<b>Disponibilité du Système</b>	Pourcentage de disponibilité du système.	99.9%	Mensuel
<b>Taux d'Erreurs</b>	Nombre d'erreurs par transaction.	< 0.1%	Hebdomadaire
<b>Performance des Tests de Charge</b>	Capacité du système à gérer un nombre élevé de transactions simultanées.	10000 transactions/sec	Mensuel
<b>Temps de Déploiement</b>	Durée moyenne pour déployer une nouvelle version du logiciel.	< 30 minutes	Par déploiement
<b>Satisfaction des Utilisateurs</b>	Niveau de satisfaction des utilisateurs finaux (enquêtes de feedback).	> 85%	Trimestriel

<b>Conformité de Sécurité</b>	Nombre de failles de sécurité détectées et corrigées.	100% corrigé	Mensuel
<b>Temps de Restauration</b>	Durée pour restaurer les services après une interruption.	< 1 heure	Par incident
<b>Adoption des Nouveaux Processus</b>	Pourcentage d'utilisateurs utilisant les nouvelles fonctionnalités régulièrement.	> 80%	Trimestriel
<b>Qualité des Données</b>	Taux d'intégrité et de précision des données.	> 99.9%	Mensuel
<b>Couverture de Tests</b>	Pourcentage du code faisant l'objet d'un test pour valider son comportement.	> 90%	Hebdomadaire

---