EXEMPLE ILLUSTRATIF, VERSION ABRÉGÉE

Rapport d’Audit

Extranet de commande : audit technique et patrimonial

COMMANDITAIRE	PME industrielle fictive, 35 salariés
PRESTATAIRE	Michaël Demeyer – Give me the code
DATE DU RAPPORT	Octobre 2026
VERSION	Extrait de 9 pages (rapport complet : 27 pages)

Cas illustratif. L’entreprise, ses constats et les montants présentés dans ce document sont fictifs. Ils sont construits à partir de situations fréquentes sur les applications web de PME. La structure, la méthode et le niveau de détail sont ceux des rapports réellement livrés.

Cet extrait reprend les parties qu’un dirigeant lit en premier : la synthèse, la cartographie des accès, le test de restaurabilité, le registre des risques, la gouvernance et le plan chiffré. Le rapport complet détaille en plus l’état technique, l’architecture, chaque risque et chaque lot.

1 Synthèse

L’extranet fonctionne et rend le service attendu par les clients, mais l’entreprise n’en a pas la maîtrise : le nom de domaine, le serveur et le code en production sont détenus par des tiers. En l’état, un incident serveur entraînerait la perte définitive des fichiers déposés par les clients et plusieurs jours d’indisponibilité.

Ce qui a été audité : le code source, l’architecture, les dépendances, l’hébergement et la configuration serveur, les sauvegardes, les comptes et les accès, l’interface avec l’ERP. Aucune donnée personnelle n’a été consultée et aucune action irréversible n’a été menée en production.

Quatre constats :

Le code est maintenable.

Développée il y a six ans par un développeur indépendant, l’application est structurée de façon classique et lisible. Elle peut être reprise par un tiers.

Les actifs essentiels appartiennent à d’autres.

Le domaine et le serveur sont sur les comptes de l’agence web. Le code est sur le compte personnel de l’ancien développeur, et la version en production diffère de la dernière version transmise. Un changement de prestataire ou un désaccord bloquerait toute évolution.

La restauration n’est que partielle.

L’instantané hebdomadaire de l’hébergeur restaure la base, mais pas les fichiers déposés par les clients. En cas de sinistre : jusqu’à 7 jours de commandes perdus, perte définitive des fichiers clients, 2 à 4 jours ouvrés d’indisponibilité.

Une partie de la stack est hors maintenance.

Système, PHP, base de données et framework front ne reçoivent plus de correctifs de sécurité ; 7 vulnérabilités de gravité haute ou critique sont recensées dans les dépendances PHP.

A Priorisation et suite proposée

Le registre documente 14 risques, dont 5 immédiats. La remédiation est découpée en 6 lots commandables séparément, pour un total de **23 200 € HT**. Les lots 1 et 2 (**5 800 € HT**) couvrent à eux seuls les 5 risques immédiats.

2 Cartographie des accès

NOM	STATUT	REMARQUE
Nom de domaine	Tiers	Enregistré sur le compte de l’agence web chez le registraire.
Serveur et hébergement	Tiers	Contrat d’hébergement au nom de l’agence web.
Dépôt du code source	Tiers	Compte personnel de l’ancien développeur.
Sauvegardes	À vérifier	Instantané hebdomadaire. Fichiers clients non inclus.
Envoi des mails	Tiers	Messagerie personnelle d’un ancien salarié.
Accès SSH au serveur	À vérifier	Compte partagé par quatre personnes, dont deux parties.
Identifiants de l’ERP	À vérifier	Présents en clair dans le code source.
Statistiques de fréquentation	OK	Compte au nom de l’entreprise.

3 Test de restaurabilité

Le test répond à une seule question : à partir de ce qui existe aujourd’hui, peut-on redémarrer le service sur une autre machine ? Mené sur une machine isolée, il donne un résultat partiel :

- La base de données est restaurée, avec une perte potentielle de 7 jours de commandes.
- Le démarrage a demandé deux heures de corrections manuelles, non documentées.
- Les fichiers déposés par les clients sont absents de l’instantané.
- L’envoi des mails échoue, faute d’identifiants appartenant à l’entreprise.
- La synchronisation avec l’ERP n’a pas pu être testée : le script n’existe que sur le serveur.

Une sauvegarde prévue au contrat n’est pas une sauvegarde : seule une restauration testée en apporte la preuve.

4 Registre des risques

A Résumé

RISQUE	PRIORITÉ	EFFORT
R-1 – Nom de domaine enregistré au nom de l'agence web	Immédiat	Faible
R-2 – Serveur loué sur le compte de l'agence web	Immédiat	Moyen
R-3 – Code en production différent du dépôt, dépôt sur un compte personnel	Immédiat	Moyen
R-4 – Sauvegardes non externalisées et incomplètes	Immédiat	Faible
R-5 – Accès administrateur partagés, dont ceux d'anciens intervenants	Immédiat	Faible
R-6 – Identifiants de l'ERP en clair dans le code	Important	Faible
R-7 – Mails de l'extranet envoyés par une messagerie personnelle	Important	Faible
R-8 – Version de PHP obsolète	Important	Élevé
R-9 – Aucune supervision ni alerte d'indisponibilité	Important	Faible
R-10 – Système d'exploitation obsolète	Planifiable	Moyen
R-11 – Serveur de base de données obsolète	Planifiable	Moyen
R-12 – Synchronisation nocturne avec l'ERP non documentée	Planifiable	Faible
R-13 – Framework front et Node obsolètes	Planifiable	Élevé
R-14 – Absence de test automatique	Amélioration	Élevé

B Exemple de fiche détaillée

Dans le rapport complet, chaque risque fait l’objet d’une fiche de ce type.

R-3 – Code en production différent du dépôt, dépôt sur un compte personnel

Domaine : Code source de l’application

Priorité :

Immédiat

Effort de remédiation :

Moyen

Constat :

Le dépôt Git est hébergé sur le compte personnel de l’ancien développeur, qui n’intervient plus depuis deux ans. L’entreprise dispose d’une archive transmise à son départ.

La comparaison avec le serveur montre 23 fichiers modifiés directement en production depuis cette date, sans trace dans le dépôt.

Impact :

L’entreprise ne détient pas la version de son application qui tourne réellement. Une mise à jour déployée depuis l’archive effacerait les corrections faites depuis, sans qu’on sache lesquelles.

Recommandation :

Créer un dépôt au nom de l’entreprise et y importer le code tel qu’il tourne en production, en conservant l’historique de l’archive.

Documenter les 23 écarts, puis faire passer toute modification par une chaîne de déploiement.

5 Recommandation de gouvernance

La situation constatée découle d’une répartition floue entre ce qui appartient à l’entreprise et ce qui relève de ses prestataires successifs. Ces recommandations valent quel que soit le prestataire retenu pour la suite.

A Ce qui doit rester sous le contrôle de l’entreprise

ACTIF	IMPACT
Nom de domaine et zone DNS	Point d’accès unique à l’extranet et à la messagerie. Le propriétaire doit être l’entreprise.
Compte chez l’hébergeur	Propriété administrative du serveur et accès d’ultime recours.
Dépôt de code et chaîne de déploiement	Le code est un actif de l’entreprise. Le prestataire est mainteneur, jamais propriétaire.
Espace de stockage des sauvegardes	Doit rester disponible en cas de changement de prestataire.
Comptes des services tiers	Envoi des mails, supervision : créés au nom de l’entreprise, accès délégué au prestataire.

B Ce qui doit être évité

A ÉVITER	CONSÉQUENCE
Enregistrer le domaine ou le serveur au nom du prestataire	Toute évolution dépend de sa disponibilité et de sa bonne volonté.
Corriger directement sur le serveur	Le dépôt ne reflète plus la réalité ; la prochaine mise à jour écrase les corrections.
Considérer qu’une sauvegarde existe parce qu’elle est prévue au contrat	Une sauvegarde non testée n’apporte aucune preuve de la possibilité de restauration.
Confier code, infrastructure et sauvegardes au même acteur sans réversibilité écrite	La reprise par un nouveau prestataire devient longue et incertaine.

6

Chiffrage des lots de remédiation

Chaque lot a un périmètre, des hypothèses, un délai, des critères d’acceptation et un prix ferme. L’entreprise commande les lots dans l’ordre et au rythme qui lui conviennent, auprès du prestataire de son choix.

LOT	INTITULÉ	DÉLAI	PRIX FERME HT
1	Reprise de propriété : domaine, serveur, code et accès	~2 semaines	4 200 €
2	Sauvegardes externalisées et restauration testée	~1 semaine	1 600 €
3	Envoi des mails et supervision	~3 jours	1 200 €
4	Migration du serveur et de la base de données	~2 semaines	4 800 €
5	Remise à niveau du moteur applicatif (PHP)	~2 semaines	4 600 €
6	Modernisation de la chaîne front (Vue.js / Node)	~4 semaines	6 800 €
	Total		**23 200 €**

A Exemple de fiche de lot

LOT 1 - REPRISE DE PROPRIÉTÉ : DOMAINE, SERVEUR, CODE ET ACCÈS

Remise de l’outil entre les mains de l’entreprise

PÉRIMÈTRE

- Transfert du nom de domaine et du contrat d’hébergement au nom de l’entreprise
- Création d’un dépôt de code appartenant à l’entreprise et import de la version en production
- Documentation des écarts avec l’ancienne archive
- Création des scripts de construction et de déploiement de l’application
- Création de comptes nominatifs, suppression du compte partagé
- Renouvellement des identifiants de l’ERP et retrait du code

HYPOTHÈSES

- L’agence web accepte le transfert du domaine et du contrat d’hébergement
- Un compte de dépôt de code est créé par l’entreprise

EXCLUSIONS

N/A

DÉLAI PROPOSÉ

~2 semaines

CRITÈRES D’ACCEPTATION

- Le domaine et le serveur sont au nom de l’entreprise.
- Le code en production est identique au dépôt.
- Le déploiement de l’application est possible.
- Les anciens accès sont révoqués.

COUVERTURE DES RISQUES

R-1, R-2, R-3, R-5, R-6

PRIX FERME (HT)

4 200 €

7 Après la remise du rapport

- Le rapport appartient à l’entreprise. Il reste utilisable avec n’importe quel prestataire, y compris le prestataire actuel.
- Les lots se commandent séparément, dans l’ordre choisi. Aucun engagement au-delà de l’audit.

A Audit technique et patrimonial

3 000 € HT, prix fixe, livré sous trois semaines : synthèse, cartographie des accès, test de restaurabilité, registre des risques, recommandation de gouvernance et plan chiffré par lots.

Michaël Demeyer, développeur et ingénieur infrastructure, Bois-le-Roi (77). Plus de 15 ans d’expérience, certifié AWS Solutions Architect, diplômé Administrateur Système DevOps (RNCP niveau 6).

michael@givemetheco.de · 07 57 50 70 90 · www.givemetheco.de