Les cahiers de la souveraineté

Les livrables proposés ci-dessous sont des modèles de tableurs conçus pour structurer la démarche de souveraineté et permettent une analyse rigoureuse et un suivi continu des facteurs de souveraineté.

Livrable 1 : Cartographie des dépendances et de la Chaîne de Valeur

Objectif : Identifier toutes les dépendances critiques (technologies, logiciels, fournisseurs, compétences, clients) et évaluer leur impact sur la souveraineté de l'entreprise, en incluant une vision sur les dépendances indirectes (N-2).

Maillon de la Chaîne / Catégorie	Acteur / Technologie / Ressource	Type de Dépendance (Techno, Humaine, Fournisseur, Géo...)	Rôle / Usage dans l'entreprise	Criticité (Vitale, Importante, Secondaire)	Pays de l'acteur / Origine	Fournisseur de l'acteur (N-2) / Info Complémentaire	Actions de Mitigation
Logiciel	CRM "SalesCloudXYZ"	Technologique (SaaS, Vendor lock-in)	Gestion de la relation client	Vitale	États-Unis	Hébergé sur CloudXYZ Inc.	1. Négocier une clause de réversibilité. 2. Veille sur les alternatives open-source. 3. Avoir une autre solution non

							déployée visible mais active
Données	Base de données clients	Données Maîtres	Cœur de métier	Vitale	États-Unis	Données stockées chez CloudXYZ Inc.	1. Chiffrer avec clés internes. 2. Étudier hébergement souverain. 3. Avoir un contrat et une solution non déployée visible mais active
Infrastructures IT	Hébergement Cloud "Cloud ZYXYX"	Technologique / Juridique (Lois extra-UE)	Hébergement de toutes les applications	Vitale	États-Unis	Fournisseurs d'énergie, de fibre optique	1. Mettre en place un plan de bascule vers un cloud souverain. 2. Privilégier les formats ouverts.
Matières Premières	Fournisseur A (composants)	Géographique (Fournisseur unique)	Production	Vitale	Asie	Producteur de Silicium XYZ	1. Identifier un fournisseur en Europe. 2. Augmenter les stocks stratégiques. 3. Négocier des contrats à petit volume avec d'autres

							acteurs même « chers »
Ressources Humaines	Expert Maintenance ERP	Compétences (Savoir-faire unique)	Maintenance du logiciel ERP critique	Vitale	N/A	Personne proche de la retraite	1. Lancer un projet de documentation. 2. Former 2 personnes en backup.
Clients	Client Majoritaire D	Financière (80% du CA)	Flux de revenus principal	Vitale	N/A	N/A	1. Lancer une offre pour un nouveau segment de marché. 2. Renforcer la prospection.
Distribution	Partenaire C (logistique)	Opérationnelle	Livraison des produits finis	Importante	France	Sous-traitants transporteurs locaux	1. Contrat avec un logisticien secondaire. 2. Auditer la chaîne des sous-traitants.

Livrable 2 : Matrice d'analyse et de suivi des risques de souveraineté

Objectif : Centraliser, quantifier et suivre les risques liés aux dépendances, et définir les plans d'action pour les atténuer.

ID Risque	Actif / Processus concerné	Catégorie de risque	Description du Risque	Probabilité (Faible, Moyenne, Élevée)	Impact (Faible, Moyen, Élevé, Vital)	Niveau de Risque (Calculé)	Mesures d'Atténuation / Plan d'action	Solution de repli et délai de bascule	Responsable	Statut
R-001	CRM "SalesCloudXYZ"	Coût / Dépendance commerciale	Augmentation drastique des coûts de licence, bloquant le budget.	Moyenne	Élevé	Élevé	1. Négocier un contrat pluriannuel avec plafond. 2. Lancer une veille pour identifier des alternatives.	Solution OpenSource XYZ (3 semaines)	DAF / DSI	En cours
R-002	CRM "SalesCloudXYZ"	Modification imposée / Perte de contrôle	Le fournisseur impose une mise à jour majeure à une période critique (fin d'année).	Élevée	Élevé	Élevé	1. Négocier une clause de flexibilité sur le planning. 2. Préparer un plan de continuité d'activité.	N/A	DSI / Métiers	À faire
R-003	Hébergement Cloud "Cloud ZYX"	Géopolitique / Réglementaire	Pression d'un État étranger (Cloud Act) menant à un	Faible	Vital	Moyen	1. Chiffrer toutes les données avec clés maîtrisées en	Migration vers Cloud W (72 heures)	RSSI / DSI	En veille

			espionnage ou une indisponibilité des données.				interne. 2. Étudier une solution d'hébergement souverain.			
R-004	Expert Maintenance ERP	Dépendance Humaine / Compétence	Départ de l'unique expert (retraite). Risque de perte de connaissance et d'incapacité à maintenir l'ERP.	Moyenne	Vital	Élevé	1. Documenter le savoir-faire. 2. Former deux personnes en backup.	Maintenance externe (coût élevé)	DSI / DRH	Plan de formation initié
R-005	Client Majoritaire D	Financier	Le client fait défaut ou change de stratégie, entraînant un tarissement de 80% du CA.	Faible	Vital	Moyen	1. Lancer une offre pour un nouveau segment de marché. 2. Renforcer la prospection commerciale.	Diversification (6-12 mois)	Direction Commerciale	Budget à valider
R-006	Duplication Données Sensibles	Sécurité	Compromission multiple si une même faille est exploitée sur des données dupliquées.	Moyenne	Élevé	Élevé	Utiliser des solutions de sécurité hétérogènes et un chiffrement multi-couches pour chaque copie.	N/A	RSSI	En place

Livrable 3 : Registre de Traçabilité des Décisions Stratégiques et Audits

Objectif : Documenter le processus décisionnel et le suivi par audit pour garantir l'agilité et la capacité à pivoter, un pilier de la souveraineté.

Partie A : Registre des décisions

ID Décision	Date de Décision	Décision Prise	Contexte et Problématique	Décideur(s)	Hypothèses et Contraintes Clés	Options Écartées et Justification	Risques Générés (ID)
D-001	2025-09-15	Choix de la solution CRM "SalesCloudXYZ" (SaaS)	Remplacement de l'ancien CRM obsolète. Besoin d'une solution moderne et intégrée.	CODIR	**H:** Coût stable (+/- 5%/an). **C:** Déploiement avant fin T1 2026.	1. **Développement interne:** Coût/délai trop élevés. 2. **Open-source:** Complexité d'intégration.	R-001, R-002
D-002	2025-11-03	Maintien de l'hébergement chez "Cloud ZYX"	Analyse annuelle du contrat d'hébergement.	DSI, CODIR	**H:** Stabilité géopolitique. **C:** Budget IT contraint.	**Migration vers cloud souverain:** Surcoût de 15% jugé trop élevé à court terme.	R-003

Partie B : Suivi des audits de souveraineté

Type d'Audit	Périmètre Audité	Date du Dernier Audit	Principales Conclusions	Plan d'Action Associé	Responsable du Suivi	Prochain Audit Prévu
Fournisseur Critique	Fournisseur A (composants)	2025-10-15	Dépendance forte à un seul fournisseur de rang 2. Pas de plan de continuité formalisé.	1. Exiger le plan de continuité sous 3 mois. 2. Lancer la recherche d'une alternative.	Service Achats	2026-10-15
Réversibilité	Extraction des données du CRM "SalesCloudXYZ"	2026-01-10	Formats de données propriétaires. Coût d'extraction élevé et non budgété.	1. Négocier une clause de réversibilité à coût fixe. 2. Provisionner le budget.	DSI, Direction Juridique	2027-01-10
Plan de Reprise d'Activité (PRA)	Bascule de l'infrastructure vers le site de secours	2025-07-20	Succès technique mais dépendance à des experts clés présents uniquement en juillet.	1. Documenter la procédure pour non-experts. 2. Planifier un test hors période estivale.	DSI	2026-07-18
Conformité RGPD	Solution de repli (Plan B) pour la paie	N/A	Non audité à ce jour. Le risque de non-conformité est élevé.	Lancer un audit de conformité complet avant tout test en production.	DPO	2026-04-01

Cartographie des dépendances et des risques associés

L'analyse part des dépendances technologiques (logiciels, SaaS), qui sont elles-mêmes liées à des sociétés (privées ou publiques) potentiellement situées dans des pays étrangers.
Une cartographie de ces dépendances est essentielle pour maîtriser la souveraineté.

De ces dépendances découlent de multiples risques :

- **Risques économiques et réglementaires :** Augmentation forte des coûts de licence, pressions commerciales, ou pressions d'États sur les fournisseurs.
  Les changements de réglementation, comme le RGPD, peuvent également entraîner des hausses de coûts dues aux développements supplémentaires nécessaires (chiffrement, documentation).
- **Risques Opérationnels :**
  - **Obsolescence et rigidité :** Un logiciel ancien ou peu maniable peut empêcher une entreprise de s'adapter à une évolution du marché, la rendant non concurrentielle.
  - **Modifications et mises à jour forcées :** Un fournisseur (notamment en SaaS, mais aussi on premise) peut imposer des modifications ou des mises à jour à un moment inopportun, impactant les processus métier et la continuité de service.
  - **Corruption des données :** Une erreur humaine chez un fournisseur (ex: mauvaise requête SQL lors d'une correction de masse) peut corrompre une base de données entière et interrompre l'activité.
- **Risques de Sécurité :** l'espionnage industriel est un risque majeur, où un fournisseur (SaaS ou autre) pourrait écouter les données, les logs d'activité ou les événements système.
- **Dépendances non évidentes :** La souveraineté peut être compromise par des fournisseurs uniques pour des services périphériques mais critiques.
  L'exemple typique est celui de la téléphonie : une entreprise peut avoir des systèmes informatiques redondants, mais dépendre d'un seul opérateur téléphonique : avec la téléphonie sur IP, cette dépendance s'étend au fournisseur d'accès internet.

Ces fournisseurs, non vitaux au quotidien, le deviennent en situation de crise.
L'électricité est un autre exemple de dépendance de base critique.

L'analyse doit donc s'étendre à tous les niveaux : données, logiciels, infrastructures et réseaux, en incluant les dépendances fondamentales comme l'alimentation électrique, qui nécessite une réflexion sur des adductions multiples avec des fournisseurs différents.

Stratégies de verrouillage par les fournisseurs et contre-mesures

Un fournisseur peut asseoir sa domination non pas en contrôlant le logiciel métier principal, mais en proposant un écosystème d'outils périphériques indispensables qui, à terme, rendent le client captif.
Cette stratégie est souvent amorcée par des offres commerciales très attractives qui masquent une ambition de contrôle à long terme.
Une fois l'écosystème en place, le client se retrouve dans l'incapacité de changer de fournisseur, car toutes ses données et ses flux sont intégrés chez ce dernier.

Face à ces stratégies, la contre-mesure principale est d'éviter la dépendance à un fournisseur unique.
La souveraineté réside dans la capacité à basculer d'une solution à une autre, ceci implique de maintenir activement des solutions alternatives (plans B, C, D) et de s'assurer que le fournisseur est conscient que le client n'est pas captif.

Cette posture, qui peut relever du bluff stratégique, neutralise les leviers de pression du fournisseur et l'empêche de « tenir » ou « d'étrangler » son client.

Il faut donc se méfier des offres trop belles pour être vraies, car elles conduisent souvent à une perte de souveraineté en rendant tout changement de fournisseur financièrement injustifiable à l'avenir.

Analyse stratégique de la Chaîne de Valeur Étendue

La dépendance ne se limite pas aux fournisseurs directs, elle s'étend aux fournisseurs des fournisseurs et même aux matières premières.
Un défaut d'approvisionnement en amont de la chaîne peut rendre un fournisseur incapable de respecter ses obligations contractuelles.
Il est donc nécessaire de monitorer cette chaîne d'approvisionnement profonde, en définissant un niveau d'analyse pertinent en fonction de la criticité.

De même, en aval, la dépendance à un client unique, à un seul type de clientèle, ou à un secteur en crise représente un risque majeur.
L'assèchement des flux financiers entrants, parce que les clients ne peuvent plus payer, interrompt la continuité de l'entreprise aussi sûrement qu'une défaillance technique.
Sans revenus, il devient impossible de financer les opérations, le marketing ou de payer ses propres fournisseurs.

L'analyse conclut que chaque acteur de la chaîne de valeur cherche logiquement à sécuriser sa propre continuité, souvent en essayant de mettre ses partenaires en situation de dépendance.
Ainsi, tout comme une entreprise cherche à sécuriser sa relation avec ses fournisseurs, ses clients chercheront à faire de même avec elle.
Comprendre cette dynamique est essentiel pour identifier les points faibles et les risques de rupture sur l'ensemble de l'écosystème.

Autres éléments à ne pas négliger

I. Facteurs humains et organisationnels

1. **Rétention des talents et souveraineté des compétences :**
    - **« Guerre des talents » :** Une entreprise peut perdre sa souveraineté si les compétences clés (maintenance, développement, sécurité) sont débauchées par des concurrents ou des fournisseurs, créant une dépendance externe forcée.
      La stratégie offensive pour attirer et retenir ces compétences est parfois vitale.
    - **Pyramide des âges :** Un risque majeur est le départ à la retraite des experts détenant la connaissance des systèmes legacy.
      Sans plan de transmission, la souveraineté sur ces systèmes s'évapore.
    - **Formation et culture d'entreprise :** Développer une culture de la documentation, du partage de connaissances et de la formation continue pour ne pas dépendre d'une poignée d'experts uniques.
      La formation doit aussi inclure la sensibilisation des utilisateurs aux bonnes pratiques de sécurité (hameçonnage, ingénierie sociale).
    - **Gestion du patrimoine intellectuel :** Mettre en place des stratégies de capitalisation et de transmission pour que le savoir-faire critique (brevets, processus non documentés) ne quitte pas l'entreprise avec les experts.
2. **Souveraineté décisionnelle et gouvernance :**
    - **Pression des actionnaires :** Des actionnaires peuvent imposer des choix technologiques à court terme qui nuisent à la souveraineté à long terme (ex: migration vers un cloud unique pour réduire les coûts).

- **Culture du « pas de vague » :** La peur de remettre en cause des décisions historiques ou des partenariats établis, même s'ils créent une dépendance.
- **L'humain comme faille :** La corruption, l'ingénierie sociale ou le chantage visant des employés clés peuvent être des vecteurs directs de perte de souveraineté.
- **Politique de Sécurité (PSSI) :** Définir une gouvernance claire avec des rôles et responsabilités (RSSI, DPO), des procédures d'urgence et un plan de continuité d'activité (PCA/PRA).
- **Contrôle des accès basé sur les rôles :** Attribuer des droits stricts selon le principe du moindre privilège pour limiter les risques internes.

II. Dimensions économiques, législatives et géopolitiques

1. **Souveraineté budgétaire et financière :**
   - **Dette technique invisible :** Repousser les mises à jour pour des raisons budgétaires crée une dette qui, à terme, force à accepter les conditions d'un fournisseur.
   - **Modèles de licences prédateurs :** Des modèles de licences opaques et changeants (basés sur cœurs CPU, appels API, etc.) rendent toute prévision impossible et créent une dépendance.
   - **Effet de levier par le financement :** Des conditions de paiement attractives peuvent enfermer un client dans une solution via des pénalités de sortie insurmontables.
2. **Souveraineté juridique et géopolitique :**
   - **Impact des lois extraterritoriales :** Des lois comme le CLOUD Act américain peuvent donner accès aux données, même hébergées en Europe, si le fournisseur est de nationalité américaine.
     La localisation géographique ne suffit pas.

- **Instabilité politique et embargos :** Le risque d'un changement politique brutal dans un pays où se situe un fournisseur ou un client critique doit être modélisé.
- **Souveraineté nationale et industrielle :** Inscription dans une stratégie de filière pour mutualiser les coûts (ex: cloud de confiance, consortiums industriels).

III. Aspects technologiques et stratégiques

1. **La Souveraineté par l'architecture et les standards :**
   - **Le « Zero Trust » :** Adopter une architecture où aucun utilisateur ou appareil n'est fiable par défaut, même à l'intérieur du réseau.
     Chaque accès est systématiquement vérifié.
   - **Informatique confidentielle :** Utiliser des enclaves sécurisées pour que les données restent chiffrées même pendant leur traitement en mémoire.
   - **Portabilité et Interopérabilité :** Le vrai « lock-in » n'est pas le logiciel mais les données.
     Imposer l'usage de formats standards et ouverts est clé pour garantir la réversibilité.
   - **Dépendance aux API :** Si un fournisseur change ses API, c'est tout un écosystème qui peut s'effondrer.
   - **Risque de la « boîte noire » algorithmique :** Avec l'IA, il devient strictement nécessaire d'exiger l'auditabilité et l'explicabilité des algorithmes pour conserver la souveraineté décisionnelle.
2. **L'Open Source, un faux ami de la souveraineté ?**
   - **Dépendance à la communauté :** Un projet open source peut être abandonné, laissant l'entreprise avec un logiciel vulnérable et sans support.
   - **Open Washing :** Des versions communauté limitées qui forcent à passer à la version entreprise payante pour des fonctionnalités essentielles.

- **Contamination par licence :** Une licence virale (type GPL) peut obliger une entreprise à publier le code source de son propre logiciel propriétaire.

3. **La Souveraineté physique logistique :**
   - **Chaîne d'approvisionnement matériel :** La dépendance aux composants physiques (serveurs, puces) d'un seul fournisseur ou d'une seule région du monde est un risque majeur (crise géopolitique, pandémie).
   - **Sécurité physique des locaux :** Protéger l'accès physique aux serveurs pour éviter le vol ou l'accès direct non autorisé.
   - **Câbles sous-marins :** La souveraineté réseau dépend de ces infrastructures critiques, souvent hors du contrôle direct d'une entreprise.

IV. Nouvelles frontières de la souveraineté

1. **Souveraineté culturelle et éthique :**
   - **Alignement des valeurs :** Un fournisseur peut avoir des pratiques éthiques contraires aux valeurs de l'entreprise, créant un risque de réputation.
   - **Influence culturelle et « soft power » :** L'adoption massive d'outils d'un même écosystème façonne la culture d'entreprise.
     Comment préserver une culture propre et ne pas devenir une filiale culturelle de son fournisseur ?
   - **Souveraineté algorithmique :** La manière dont les algorithmes (recommandation, tri) façonnent l'accès à l'information et peuvent introduire des biais culturels ou commerciaux (cas de l'IA qui orienterait la culture à ne pas négliger).
2. **Souveraineté écologique et énergétique :**
   - **Dépendance aux ressources naturelles rares :** La dépendance aux métaux rares (pour les serveurs) ou à l'eau (pour le refroidissement) constitue un nouveau risque de souveraineté.

- **Souveraineté énergétique :** Face à la volatilité des prix et aux risques de coupures, développer une stratégie d'autonomie énergétique devient critique.

3. **Défense et réponse aux cyber-incidents :**
    - **Détection et réponse (EDR/XDR) :** Surveiller activement les comportements suspects pour détecter des attaques inconnues.
    - **Chasse aux Menaces :** Démarche proactive où des experts recherchent des traces de compromission, plutôt que d'attendre une alerte.
    - **La cyberguerre comme outil de déstabilisation :** Se prémunir contre les attaques qui ne visent pas l'interruption mais la perte de crédibilité par la manipulation d'informations.
    - **Assurance cyber :** Intégrer la souscription à une assurance spécialisée dans la stratégie de gestion des risques.
    - **Tests d'intrusion et Red Team :** Mandater des experts pour simuler des attaques réelles afin de découvrir les failles.

Solve DSI accompagne les entreprises et services publics dans les analyses de dépendances

Yann-Eric DEVARS Directeur Solve DSI
Créateur du framework DYNAMAP SI

www.solve-dsi.fr

www.dynamap.fr

Pour aller plus loin : découvrez l'ouvrage consacré à la souveraineté numérique

Lire l'échantillon

Suivre l'auteur

Souveraineté d'entreprise et souveraineté numérique: Pas de souveraineté possible sans souveraineté numérique Relié – 7 août 2025

de Mr Yann-Eric DEVARS (Auteur)

En lien avec DYNAMAP, framework d'architecture d'entreprise — Voir tous les formats et éditions

-5 % & livraison GRATUITE en points de retrait éligibles, à sélectionner lors du paiement. Détails ›

Les entreprises de la fin de l'ère industrielle, encore engourdies par un confort relatif hérité de décennies de croissance linéaire et de chaînes de valeur globalisées, se découvrent depuis peu tributaires d'une ressource immatérielle : la capacité à conserver la main sur leurs propres informations.

Cette "souveraineté" des systèmes d'information, longtemps perçue comme une posture de spécialistes soucieux de protéger leurs environnements techniques, s'est métamorphosée en prérequis stratégique, dont la perte se mesure soudainement en parts de marché évaporées, en appels d'offres perdus ou en amendes réglementaires qui annulent en un trimestre les bénéfices d'une année complète.

À mesure que le monde bascule dans l'économie des services connectés où chaque geste produit une trace, chaque trace un actif, et chaque actif un risque, la question n'est plus de savoir si l'on veut la souveraineté, mais combien il en coûte de ne pas la posséder.

En lire plus

Signaler un problème avec ce produit

Nombre de pages de l'édition…	Langue	Date de publication	Dimensions	ISBN-13
95 pages	Français	7 août 2025	15.84 x 1.04 x 23.46 cm	979-8297013797

Voir tous les détails

Relié 32,70 € | Broché 26,38 €

Autres offres D'occasion et Neuf

32,70 €

Les prix incluent la TVA. Informations sur la TVA

Retours GRATUITS

Livraison à 0,01€ **mercredi 25 février** dès 35€ d'achat de livres. Détails

Ou livraison accélérée **mardi 24 février**. Détails

La réglementation impose 3€ minimum de frais de livraison pour les commandes de livres neufs inférieures à 35€

Livraison à Paris 75001 — Mettre à jour l'emplacement

En stock

Quantité : 1

Ajouter au panier

Acheter cet article