

Partie 01	Préambule : objectifs du rapport	▶	[04]
Partie 02	Synthèse : les clés de la transformation digitale	▶	[09]
Partie 03	Analyse S.V.O.R. et recommandations	▶	[12]
Partie 04	Roadmap de la transformation du Système d'Information	▶	[26]
Partie 05	Cartographie complète du Système d'Information	▶	[28]
Partie 06	Annexes et détail des points d'audit	▶	[35]

Méthodologie d'élaboration de ce rapport



01

Cartographie

Une **représentation détaillée du Système d'Information** : infrastructures, applications, flux, réseau et sécurité. Permet de comprendre l'organisation et les interactions majeures afin de fournir une **vue d'ensemble claire, utile aux décideurs**.



02

Points d'audit

Cette étape consiste à cibler et analyser les **points sensibles ou critiques du système**, en identifiant les forces, faiblesses et risques. Elle alimente des recommandations précises pour **renforcer la sécurité et la performance**.



03

Matrice S.V.O.R.

La matrice résume les **forces, vulnérabilités, opportunités et risques** mis en évidence par la cartographie et l'audit. Elle offre une vision structurée pour faciliter les **décisions stratégiques** et les **priorités d'action**.



04

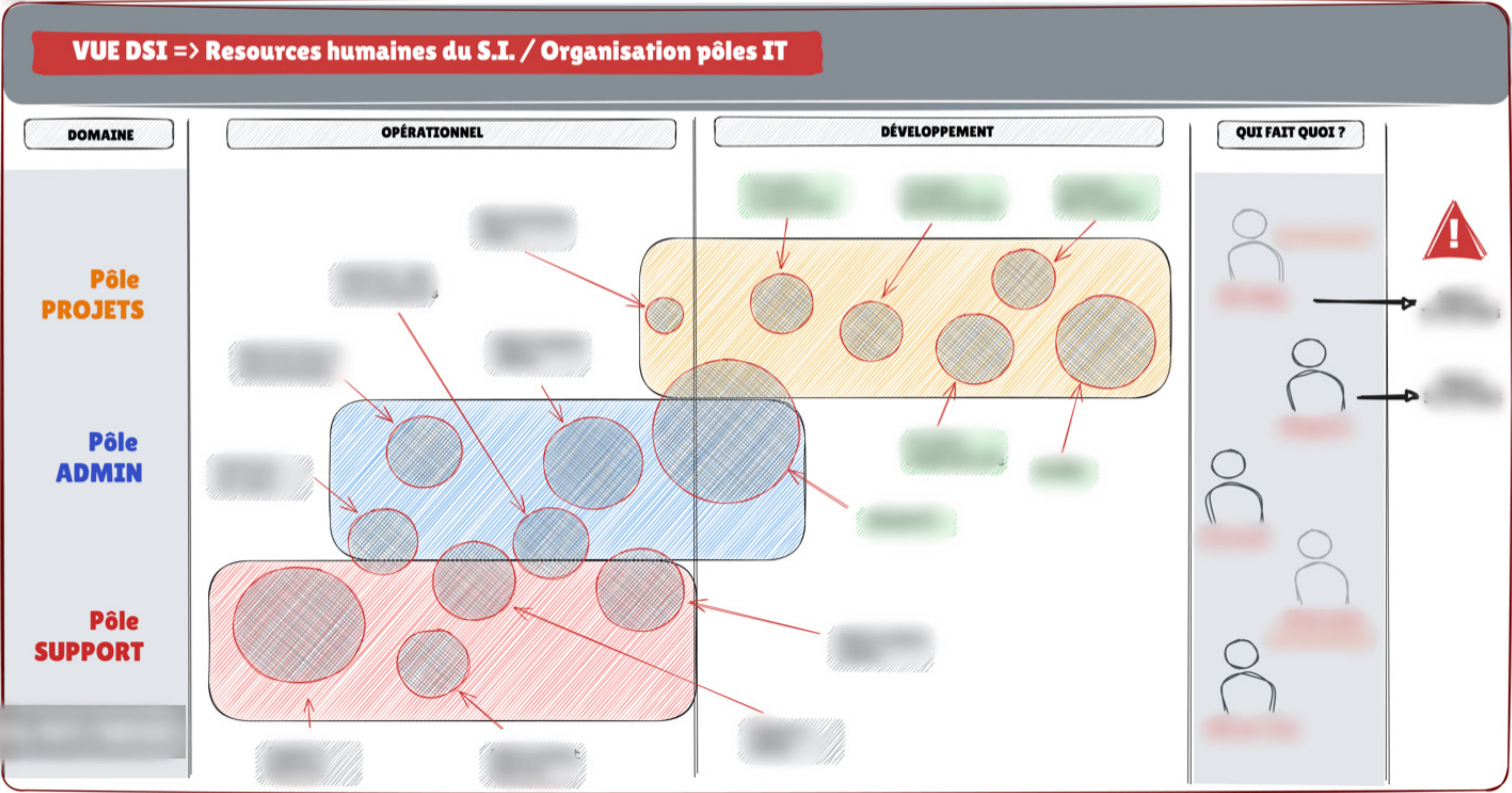
Roadmap

La roadmap décline un **plan d'action** organisé selon les axes d'amélioration identifiés. Elle précise les **priorités** et le **calendrier des mesures à mettre en œuvre** pour accompagner la transformation du Système d'Information.

Anonymisé

synthèse

Organisation humaine de l'IT à mi-2023



Anonymisé

S.V.O.R.

Strengths

Vulnerabilities

Opportunities

Risks

La matrice SVOR (Strengths, Vulnerabilities, Opportunities, Risks) présente un intérêt majeur dans l'analyse stratégique du système d'information (SI) en offrant **une vision structurée et synthétique des principaux enjeux** internes et externes.

Elle permet d'identifier clairement les forces et les vulnérabilités du SI. Cet outil favorise une **prise de décision éclairée**, la **priorisation des actions** et l'élaboration d'une **feuille de route adaptée aux évolutions du SI**.

Ainsi, la matrice SVOR servira de base à un diagnostic pertinent pour **optimiser la gouvernance du SI et assurer son alignement avec les objectifs stratégiques de l'organisation**.

Navigation

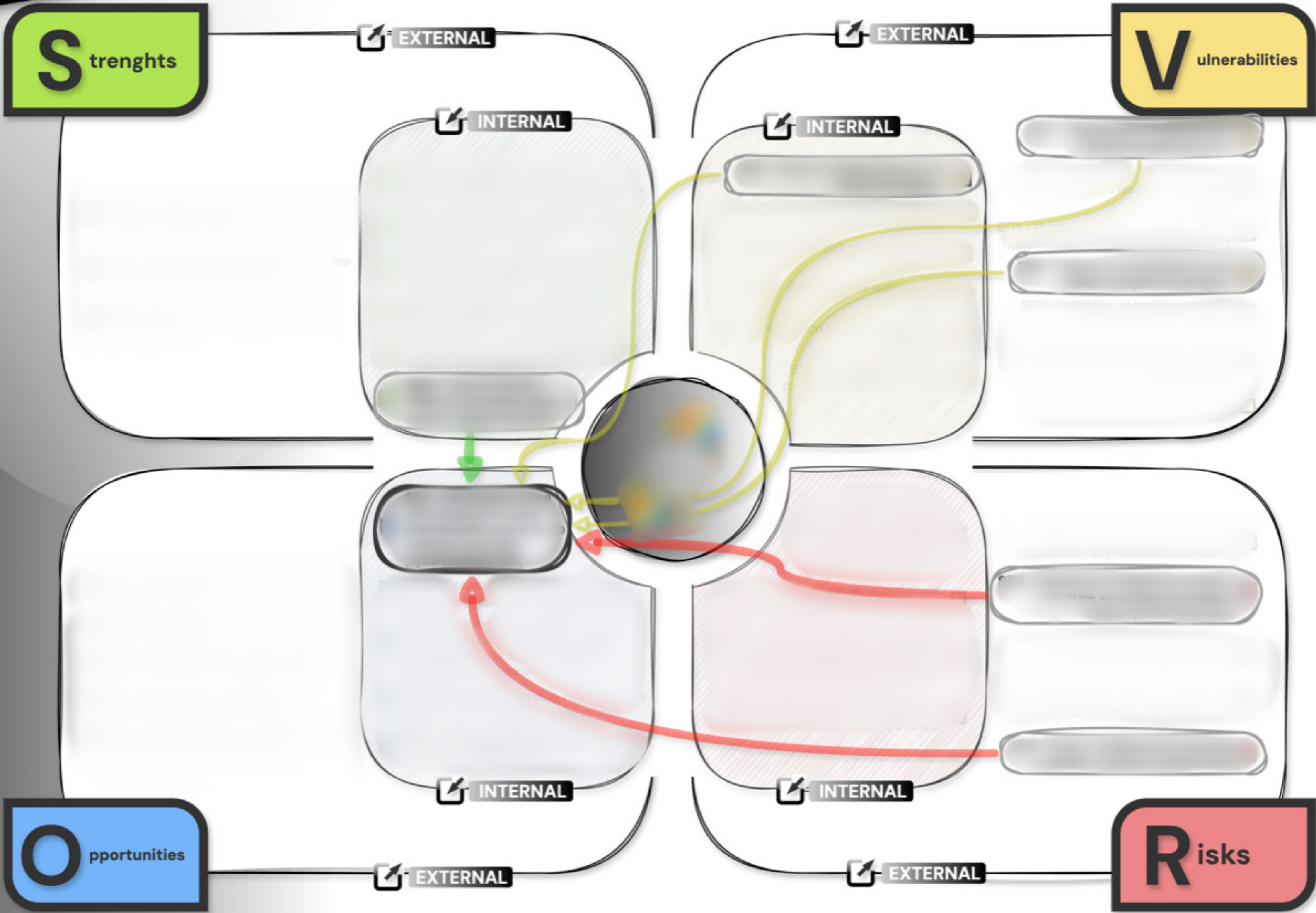
Grille de lecture

Les éléments actionnables sont tous représentés dans la catégorie “Opportunités – interne” du schéma. Chacun de ces éléments vise un ou une combinaison des objectifs suivants :

- ▶ **corriger une vulnérabilité** identifiée
- ▶ **limiter ou mitiger un risque** identifié (impact FORT => actions prioritaires)
- ▶ **s'appuyer sur une force** identifiée (impact FORT => actions prioritaires)
- ▶ **profiter d'une opportunité** externe

Anonymisé

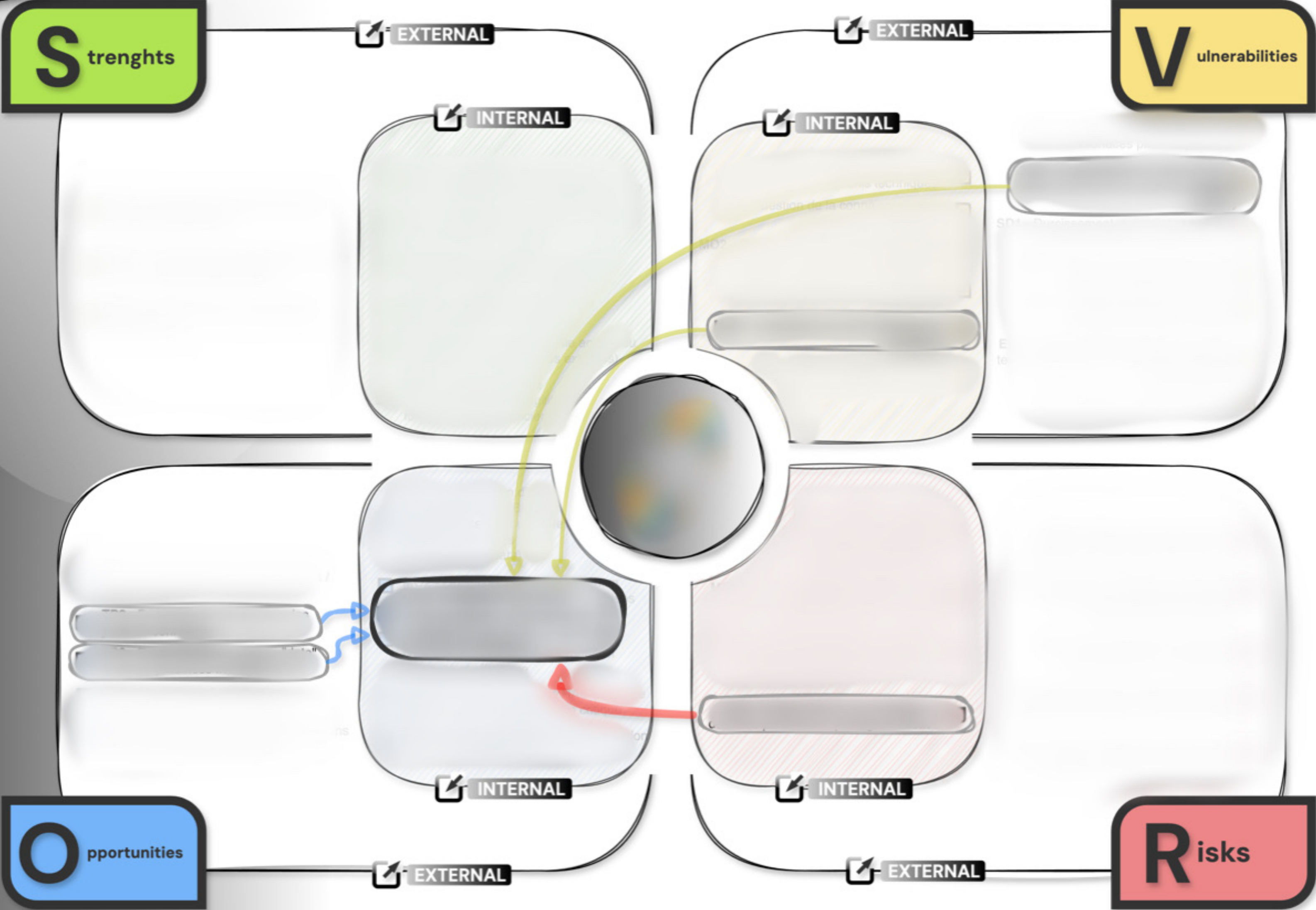
S.V.O.R.



[Blurred text]

Anonymisé

S.V.O.R.



Anonymisé

recommandations

S.V.O.R.



QUESTIONNAIRE N° 1	QUI ? QUOI ? QUAND ? COMMENT ?		01
QUESTIONNAIRE N° 2	QUI ? QUOI ? QUAND ? COMMENT ?		02
QUESTIONNAIRE N° 3	QUI ? QUOI ? QUAND ? COMMENT ?		03
QUESTIONNAIRE N° 4	QUI ? QUOI ? QUAND ? COMMENT ?		04



Anonymisé

roadmap



Anonymisé

Objectifs des vues proposées

Les vues de la cartographie sont des schémas présentant l'ensemble des éléments du S.I. de manière très synthétique. Le niveau d'abstraction élevé ainsi obtenu permet d'isoler des interactions et relations de dépendance de manière précise.

Vue INFRASTRUCTURE

Le schéma global des sites et serveurs physiques, flux et infra cloud.

Objectif : identifier clairement le backbone du S.I. et ses éléments stratégiques les plus importants.

Vue APPLICATION

Liste les services utilisateurs finaux dans leurs applications (containers).

Objectif : identifier l'ensemble des services critiques à l'activité de l'entreprise, ainsi que leurs grandes dépendances, d'un point de vue métier.

Vue DONNÉES

Détaille les flux d'échanges de données informatisés (EDI).

Objectif : représenter les flux de communication ERP / extérieur ainsi que les flux de données internes.

Vue SERVICES & RÉSEAU

Une carte des dépendances entre applications et services requis pour les faire fonctionner.

Objectif : identifier les relations de dépendances entre les services métier et les services d'infrastructure ainsi que les effets de bord potentiels.

Vue SÉCURITÉ

Liste toutes les mesures de sécurité : politiques, plans, configurations backups et firewall, outils SaaS.

Objectif : lister l'ensemble des mesures techniques et procédurales mises en oeuvre pour sécuriser l'infrastructure.

Anonymisé

cartographie



INFRASTRUCTURES

Cette vue dresse le paysage physique et logique de l'ensemble des ressources matérielles et virtuelles : serveurs, datacenters, sites distants, postes de travail, liaisons réseau, cloud, etc. Son objectif est de permettre une compréhension rapide de l'implantation des infrastructures, d'identifier où résident les points critiques (redondance, sauvegardes, accès distants) et d'accompagner la prise de décision technique ou le diagnostic lors d'incidents. L'enjeu principal réside dans la résilience du système et la capacité à anticiper ou limiter les interruptions d'activité.

Points clés

- ▶ Infrastructure en plusieurs sites (France internationale, cloud, etc.)
- ▶ Répartition géographique des ressources (VM, serveurs, etc.)
- ▶ Architecture complexe pour l'alignement des données
- ▶ Sites distants connectés via réseau sécurisé
- ▶ Services clés (DB, etc.) répartis
- ▶ Redondance des données et des services



SWITCHES - ROUTERS - FIREWALLS

Anonymisé

cartographie

APPLICATIONS

Cette représentation synthétise tous les logiciels et services utilisés par l'entreprise, en montrant leur rôle métier, leur mode d'hébergement (on-premises, SaaS), les utilisateurs concernés et les principales interactions avec les autres briques SI. Son objectif est de visualiser au plus vite la chaîne de valeur, l'interconnexion des outils, et les dépendances applicatives qui impactent l'efficacité opérationnelle. Les enjeux portent sur la maîtrise des flux, la couverture fonctionnelle et l'alignement entre l'IT et les besoins métiers.



Points clés

- ▶ Applications métier de l'entreprise (CRM, ERP, SCM, etc.)
- ▶ Outils collaboratifs et de productivité (Office 365, Teams, Slack, etc.)
- ▶ Solutions de marketing digital (CRM, Analytics, etc.)
- ▶ Applications de gestion de projet et de collaboration (Jira, Trello, etc.)
- ▶ Outils de gestion des ressources humaines (SIRH, etc.)
- ▶ Outils de gestion des finances (SIRF, etc.)
- ▶ Applications de gestion des données (Data Lake, etc.)
- ▶ Applications de gestion des infrastructures (Cloud, etc.)



Anonymisé

cartographie



DONNÉES

La vue Données met en lumière les flux, les lieux de stockage (internes ou externes), les échanges entre applications et la circulation des informations critiques : ERP, NAS, bases de données, etc. Objectif : cartographier la traçabilité, la sécurisation, les risques de perte ou de fuite, et faciliter l'analyse de conformité (RGPD, protection des actifs stratégiques). Les enjeux principaux sont la qualité, l'intégrité, la confidentialité et la disponibilité des données.

Points clés

- ▶ Flux de données structurés entre ERP & co-commerce, production, Finance et logistique
- ▶ Stockage hybride : services internes (ERP, CRM) et solutions cloud selon le volume et la criticité des données
- ▶ Interconnexions externalisées : transferts de clients, commandes, factures, reporting, échanges entre applications métiers
- ▶ Traçabilité des flux critiques



Données critiques - Données sensibles - Données publiques - Données non classées

Anonymisé

cartographie

SERVICES & RÉSEAU

Cette arborescence précise les dépendances techniques entre sites, serveurs, services et interconnexions (VPN, MPLS, accès distants) pour visualiser les routes empruntées par les flux, les zones à risques, et les dispositifs d'interconnexion (switchs, routeurs, firewalls). Elle sert à gérer la performance, la sécurité et la continuité des échanges au sein du SI. Les principaux enjeux concernent la sécurité périmétrique, la segmentation et la performance réseau.



Points clés

- ▶ Répertorier l'ensemble des services métier (CRM, ERP, applications métier, applications d'infrastructure, etc.) et leurs dépendances.
- ▶ Identifier les points de rupture pour la continuité de l'activité et les risques associés.
- ▶ Définir les zones de sécurité (DMZ, VPN, etc.) et les règles de sécurité.
- ▶ Définir les protocoles de sécurité (VPN, MPLS, etc.) et les règles de sécurité.
- ▶ Définir les protocoles de sécurité (VPN, MPLS, etc.) et les règles de sécurité.

Document - 10/10/2010

Anonymisé

SÉCURITÉ

La vue Sécurité recense toutes les protections techniques et organisationnelles: firewall, supervision, MFA, sauvegardes, procédures, plans d'urgence, politiques RGPD, etc. Elle vise à montrer l'arsenal défensif et les dispositifs en place pour garantir la disponibilité des services, l'intégrité des données et la conformité réglementaire. L'enjeu central est de limiter les risques opérationnels, juridiques et réputationnels liés aux menaces internes ou externes.

cartographie

Points clés

- Liste des services, logiciels et outils de sécurité (firewall, IDS, IPS, SIEM, etc.)
- Actions et processus de sécurité (MFA, PAM, etc.)
- Sauvegardes et applications de continuité d'activité
- Plans de réponse aux incidents (IRP, etc.)
- Politiques de sécurité (RGPD, etc.)
- Liste des fournisseurs de services de sécurité (SOC, etc.)
- Liste des contacts de secours (support, etc.)
- Liste des contacts de secours (support, etc.)



Vulnérabilités Externes Points d'audit	[37]
Vulnérabilités Internes Points d'audit	[45]
Risques Externes Points d'audit	[52]
Risques Internes Points d'audit	[58]
Forces Externes Points d'audit	[63]
Forces Internes Points d'audit	[67]
Opportunités Externes Points d'audit	[74]
Opportunités Internes Points d'audit	[80]
Sources des recommandations du S.V.O.R.	[85]