IRON : Indice de Robustesse des Organisations face au Numérique

Une méthode d'évaluation de la fragilité numérique organisationnelle

Stéphan Peccini

Stéphan Peccini Conseil

Mars 2026

Résumé

La dépendance croissante des organisations au numérique crée une fragilité structurelle rarement mesurée. Les référentiels existants (ISO 27001, ISO 22301, NIST CSF, DORA) évaluent la sécurité ou la continuité du système d'information, mais aucun ne croise la substituabilité fonctionnelle du numérique, la résilience des services numériques et l'impact sur la pérennité organisationnelle. Cet article propose IRON (Indice de Robustesse des Organisations face au Numérique), une méthode fondée sur trois axes : la substituabilité numérique (X), la résilience numérique (Y) et la criticité métier (Z). IRON produit un score unique entre 4 % et 100 %, sans calibrage sectoriel, conçu pour l'auto-évaluation et le suivi de progression. La formule IRON $= \frac{\sum Z_i \cdot X_i \cdot Y_i}{25 \cdot \sum Z_i}$ est une moyenne pondérée des taux de maîtrise du risque numérique, où le poids de chaque processus est sa criticité Z. L'article présente les fondements théoriques, la méthode complète et une stratégie de validation.

Table des matières

1 Introduction

1.1 Une dépendance devenue structurelle

Le numérique a cessé d'être un outil au service des organisations : il en est devenu l'ossature. Qu'il s'agisse d'une entreprise industrielle, d'un hôpital, d'une collectivité territoriale ou d'une association, rares sont les 📖 processus métier qui peuvent encore fonctionner sans infrastructure informatique. Cette dépendance s'est construite progressivement, portée par des gains d'efficacité réels, mais elle a créé une fragilité structurelle que peu d'organisations mesurent.

Le problème n'est pas nouveau, mais son ampleur l'est. Quand une organisation de dix personnes perd son serveur de messagerie, elle revient au téléphone. Quand une compagnie aérienne perd ses systèmes de réservation, elle cloue sa flotte au sol. La différence ne tient pas à la nature de la panne, mais au degré de dépendance : certains processus ont des alternatives, d'autres non.

1.2 Quatre incidents, une même leçon

Quatre incidents récents illustrent cette fragilité sous des angles différents.

CrowdStrike, juillet 2024

Une mise à jour défectueuse de l'agent de sécurité Falcon provoque le blocage de 8,5 millions de machines Windows dans le monde (CrowdStrike 2024). Delta Air Lines annule plus de 6 000 vols et subit 500 millions de dollars de pertes (Lines 2024). Au Royaume-Uni, la majorité des cabinets de médecine générale perdent l'accès aux dossiers patients (BBC News 2024) ; aux États-Unis, des hôpitaux annulent toutes leurs interventions non urgentes (Mathews 2024). En Australie, les caisses automatiques des supermarchés ferment (SBS News 2024). Au total, les pertes directes pour le « Fortune 500 » sont estimées à 5,4 milliards de dollars (Parametrix 2024). L'incident ne résulte ni d'une cyberattaque, ni d'une catastrophe naturelle : un agent unique, sur un système d'exploitation unique, constituait un 📖 Single Point of Failure (SPOF) sur le chemin critique de millions d'organisations.

OVHcloud Strasbourg, mars 2021

L'incendie du datacenter SBG2 détruit physiquement des milliers de serveurs. Des entreprises, des administrations et des associations perdent leurs données de manière définitive — certaines sans sauvegarde externalisée (OVHcloud 2021). L'incident révèle une confusion répandue : héberger ses données chez un prestataire ne constitue pas une sauvegarde ni une assurance.

NotPetya, juin 2017

Un logiciel de destruction déguisé en rançongiciel se propage via la mise à jour de M.E.Doc, un logiciel de comptabilité fiscale que toute entreprise opérant en Ukraine était tenue d'utiliser. Maersk, premier armateur mondial, avait ce logiciel installé dans sa filiale ukrainienne — une dépendance indirecte, enfouie, dont le siège à Copenhague n'avait probablement pas connaissance. De cette unique porte d'entrée, le logiciel malveillant se propage à l'ensemble du réseau mondial et paralyse 76 ports (Greenberg 2019). L'impact est estimé à plus de 10 milliards de dollars. Ce cas illustre un mécanisme de dépendance transitive : une obligation réglementaire locale impose un logiciel tiers, qui devient le vecteur d'une paralysie globale.

NIRS Daejeon, septembre 2025

L'explosion d'une batterie lithium-ion lors d'une opération de maintenance déclenche un incendie dans le datacenter gouvernemental sud-coréen NIRS à Daejeon (Ministry of the Interior and Safety, Republic of Korea 2025). Sur les 1 600 services numériques de l'État hébergés sur trois sites, 647 sont paralysés simultanément — dont les services postaux, la vérification d'identité et la géolocalisation des appels d'urgence. 858 téraoctets de données gouvernementales sont définitivement détruits. Le rétablissement complet prendra plus de quatre semaines. L'incident révèle qu'un tiers des services critiques d'un État étaient concentrés sur un site unique, sans basculement automatique.

Ces quatre cas partagent un trait commun : l'ampleur des conséquences n'est pas proportionnelle à la sophistication de la cause, mais au degré de dépendance des organisations touchées et à l'absence d'alternatives opérationnelles.

1.3 Un angle mort des référentiels existants

Les référentiels de gestion des risques numériques ne manquent pas. L'ISO 27001 structure la sécurité de l'information autour de 93 contrôles. L'ISO 22301 organise la continuité d'activité. Le NIST CSF propose un cadre pour la cyber-sécurité en cinq fonctions. Le règlement DORA impose des exigences de résilience numérique au secteur financier européen. Chacun apporte une contribution essentielle, mais aucun ne répond à une question simple : *si ce* 📖 *service numérique tombe, que se passe-t-il pour l'organisation ?*

Cette question exige de croiser trois dimensions que les référentiels existants traitent séparément :

- le processus métier peut-il continuer sans le numérique qui le porte ? (📖 substituabilité fonctionnelle) ;
- le service numérique est-il capable de résister à une perturbation ? (📖 résilience technique) ;

- que se passe-t-il pour l'organisation si ce processus métier s'arrête ? (impact sur la 🕮pérennité organisationnelle).

1.4 Contribution : l'indice IRON

Cet article propose IRON (Indice de Robustesse des Organisations face au Numérique), une méthode d'évaluation qui croise ces trois dimensions. Chaque processus métier est évalué sur trois axes indépendants :

- **X** — la 🕮substituabilité fonctionnelle numérique ;
- **Y** — la 🕮résilience du service numérique ;
- **Z** — la 🕮criticité métier métier (impact sur la 🕮pérennité organisationnelle).

La figure 1 montre comment ces trois axes s'articulent : X et Y se combinent en un taux de maîtrise par processus, que Z pondère pour produire le score agrégé.

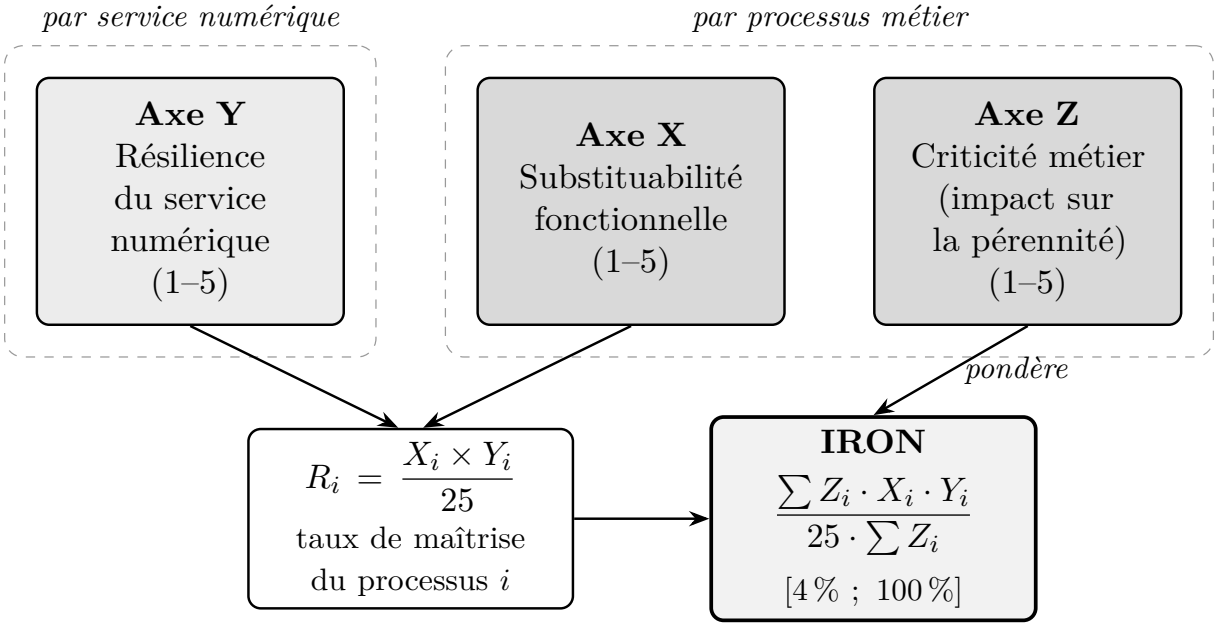

FIGURE 1 : Architecture du modèle IRON : trois axes convergent vers un score unique de robustesse organisationnelle. L'axe Y est une propriété du service numérique ; les axes X et Z sont des propriétés du processus métier.

IRON agrège ces trois axes en un score unique : plus le score est élevé, plus l'organisation est robuste face au numérique. Le score va de 4 % (aucun processus n'est substituable ni résilient) à 100 % (robustesse maximale théorique), sans calibrage sectoriel. Plus un processus est critique pour l'organisation (pérennité), plus sa maîtrise du risque numérique (substituabilité et résilience) pèse dans le score.

IRON s'inscrit dans une démarche large. En amont, l'organisation a pris conscience de la fragilité du numérique (fabrication, utilisation) et s'est engagée dans un travail d'identification de ses processus métier et de leurs dépendances. IRON intervient après cette phase : il quantifie la robustesse à partir d'un inventaire existant. En aval, le score produit alimente une stratégie de remédiation qui dépasse le périmètre du modèle. IRON est un instrument de mesure de la robustesse organisationnelle face à la dépendance numérique — pas un outil de conformité, ni de gestion du risque au sens classique, ni un guide de remédiation.

IRON ne remplace pas non plus les référentiels existants : il les complète en intégrant leurs résultats dans une mesure transversale. Une organisation certifiée ISO 27001 verra ses investissements de sécurité reflétés dans un score Y plus élevé ; une organisation ayant conduit un BIA au sens de l'ISO 22301 disposera déjà des éléments nécessaires à l'évaluation de l'axe Z.

IRON est aussi un outil de pilotage. Le score identifie les processus où l'effort d'amélioration est le plus rentable : ceux dont la criticité est élevée, mais dont la maîtrise du risque numérique peut être améliorée. Agir sur ces processus, puis re-mesurer, inscrit IRON dans une logique d'amélioration continue. La démarche opérationnelle complète — de l'état des lieux à la construction d'une stratégie de robustesse — est décrite dans Voyage vers la robustesse (Peccini 2026).

Ce livre blanc a donné la direction pour les axes X et Z, qui relèvent de l'analyse métier : identifier les processus, identifier leur dépendance numérique, évaluer leur substituabilité, mesurer leur criticité pour l'organisation. Restait à trouver la bonne approche pour l'axe Y : comment mesurer la résilience d'un 📖 service numérique de manière structurée, sans calibrage sectoriel ? Deux pistes ont été explorées — l'une par les indices de criticité matérielle (section 3), l'autre par les fondements de l'ingénierie de la résilience (section 4) — avant d'aboutir au modèle présenté en section 5.

1.5 Plan de l'article

L'article commence par un état de l'art des référentiels existants et de leurs lacunes par rapport à l'objectif d'IRON (section 2), puis examine l'approche par indices de criticité matérielle et les raisons pour lesquelles elle ne suffit pas à évaluer la robustesse organisationnelle (section 3). Les fondements théoriques du modèle sont ensuite posés (section 4), avant la description complète de la méthode : axes, grilles d'évaluation, formule et agrégation (section 5). Les propriétés du modèle — choix d'agrégation explicites, factorisation, scalabilité et limites explicites — sont établies en section 6. Enfin, une stratégie de validation progressive est proposée (section 7) et l'article conclut sur les perspectives (section 8). Les sections 2 à 4 établissent les fondements qui justifient chacun des choix du modèle ; le lecteur qui souhaite accéder directement à la méthode peut se

rendre en section 5.

2 État de l'art

2.1 Référentiels de sécurité et de continuité

Plusieurs référentiels encadrent aujourd'hui la gestion des risques numériques. Chacun apporte une contribution spécifique, mais aucun ne couvre l'ensemble du problème posé en introduction.

ISO 27001 — Sécurité de l'information

La norme ISO 27001:2022 structure un système de management de la sécurité de l'information autour de 93 contrôles répartis en quatre thèmes (organisationnels, humains, physiques, technologiques). Elle vise à protéger la confidentialité, l'intégrité et la disponibilité de l'information — la triade Confidentialité, Intégrité, Disponibilité (Confidentiality, Integrity, Availability) (CIA). Son apport est considérable pour la gouvernance de la sécurité, mais elle évalue le système d'information en soi, indépendamment des processus métier qu'il supporte. Une organisation certifiée ISO 27001 sait que son SI est protégé ; elle ne sait pas ce qui se passe si, malgré cette protection, un service tombe.

ISO 22301 — Continuité d'activité

La norme ISO 22301:2019 organise la continuité d'activité à travers une analyse d'impact (Business Impact Analysis (BIA), formalisée par l'ISO 22317) qui identifie les processus critiques et leurs exigences de reprise (Hassel et Cedergren 2024). C'est le référentiel le plus proche de la question qu'IRON pose : il lie défaillance et impact métier. Mais le BIA reste un outil d'analyse qualitative ; il ne produit pas de score quantitatif de fragilité globale et ne croise pas la substituabilité fonctionnelle avec la résilience technique du service numérique.

NIST CSF — Cadre de cybersécurité

Le NIST Cybersecurity Framework 2.0 (2024) propose six fonctions : Govern, Identify, Protect, Detect, Respond, Recover. Il couvre le cycle complet de la cybersécurité, de la gouvernance à la reprise. Son universalité (tous secteurs, toutes tailles) et sa structure en niveaux de maturité en font un outil de référence. Cependant, comme l'ISO 27001, il évalue la posture de sécurité du SI, pas l'impact d'une défaillance sur la pérennité organisationnelle de l'organisation.

DORA — Résilience opérationnelle numérique

Le règlement européen DORA (2022/2554), entré en application en janvier 2025, impose aux entités financières des exigences de résilience numérique : tests de pénétration, gestion des prestataires TIC critiques, notification d'incidents. DORA est le premier référentiel réglementaire à explicitement lier risque numérique et continuité opérationnelle. Mais il est sectoriel (services financiers uniquement) et normatif (il impose des mesures, sans produire de score de 📖 robustesse).

Autres indices et initiatives

Le BCI Resilience Index évalue la maturité en continuité d'activité par auto-déclaration. Le WEF Cyber Resilience Index se concentre sur la posture cyber des organisations. Le « Mission Dependency Index » (English et Yunusa-Kaltungo 2022) mesure la dépendance d'une mission à ses systèmes de support, mais sans intégrer la 📖 substituabilité fonctionnelle ni la 📖 résilience technique. Aucun de ces indices ne croise les trois dimensions identifiées.

2.2 Travaux académiques sur la mesure de résilience

Au-delà des référentiels normatifs, la littérature académique propose des approches quantitatives de la résilience organisationnelle et numérique.

Hosseini, Barker et Ramirez-Marquez (Hosseini et al. 2016) classifient les mesures de résilience en deux grandes familles : les approches qualitatives (questionnaires, matrices de maturité) et les approches quantitatives (métriques basées sur la performance, modèles probabilistes, théorie des graphes). La majorité des métriques existantes portent sur la résilience d'un système technique ou d'une infrastructure, pas sur la résilience d'une *organisation* face à la défaillance de ses systèmes numériques. L'écart entre résilience technique et robustesse organisationnelle est un espace qu'IRON vise à combler.

Linkov et Kott (Linkov et Kott 2019) proposent une matrice de cyber-résilience croisant quatre domaines (physique, informationnel, cognitif, social) et quatre phases temporelles (préparer, absorber, récupérer, adapter). Cette matrice couvre un périmètre plus large qu'IRON — mais ne produit pas de score agrégé ni de pondération par la criticité métier. IRON intègre les dimensions physique et informationnelle dans les axes X et Y, la dimension cognitive à travers les compétences des équipes (substituabilité dans X, rapidité de rétablissement dans Y) et la dimension sociale dans l'axe Z (impact sur l'organisation).

Aven (Aven 2019) examine la frontière conceptuelle entre risque et résilience, et plaide pour des métriques de résilience distinctes des métriques de risque. IRON s'inscrit dans cette logique : il ne mesure pas le risque (probabilité × conséquence), mais la robustesse (capacité à résister aux conséquences, quelle que soit leur probabilité). Cette distinction est structurante pour le modèle : les axes X et Y évaluent des capacités, pas des probabilités.

Sur la construction méthodologique des indices composites, le *Handbook on Constructing Composite Indicators* de l'OCDE (OECD/JRC 2008) établit un cadre de référence : normalisation, pondération justifiée, choix d'agrégation explicite, analyse de sensibilité. IRON respecte les trois premiers critères (échelle commune 1–5, pondération par la criticité Z, agrégation hybride justifiée) mais l'analyse de sensibilité formelle relève de la validation empirique (section 7).

2.3 Lacunes identifiées

L'analyse des référentiels normatifs et des travaux académiques révèle trois angles morts convergents.

Évaluation du SI, pas de l'organisation

Tous les référentiels évaluent le système d'information : ses contrôles (ISO 27001), sa capacité de reprise (ISO 22301), sa posture de sécurité (NIST CSF), sa résilience opérationnelle (DORA). Aucun ne part du 📖processus métier pour demander : *ce processus peut-il fonctionner sans ce* 📖*service numérique* ? La 📖substituabilité fonctionnelle — l'existence et la 📖maturité opérationnelle d'alternatives — est absente.

Impact mesuré en termes techniques, pas en termes de pérennité

Le BIA de l'ISO 22301 évalue l'impact d'un arrêt, mais en termes opérationnels (durée d'interruption maximale tolérable, objectif de reprise). Il ne lie pas explicitement cet impact aux dimensions qui déterminent la survie de l'organisation : continuité opérationnelle, conformité réglementaire, réputation. Or c'est le croisement de ces dimensions — la 📖criticité métier — qui distingue un incident mineur d'une crise existentielle.

Pas de score unique de fragilité

Chaque référentiel produit des résultats dans son propre format : niveau de maturité (NIST CSF), conformité binaire (ISO 27001), analyse qualitative (BIA), conformité réglementaire (DORA). Aucun ne produit un score unique et quantitatif permettant à une organisation d'évaluer sa fragilité numérique globale et de suivre sa progression dans le temps.

2.4 Positionnement d'IRON

IRON ne remplace aucun de ces référentiels : il les complète en intégrant leurs résultats dans une mesure transversale.

Une organisation certifiée ISO 27001 disposera d'éléments directement exploitables pour évaluer l'axe Y. Une organisation ayant conduit un BIA au sens de l'ISO 22301

TABLE 1 : Couverture des dimensions par les référentiels existants et par IRON.

Référentiel	X — Substituabilité	Y — Résilience	Z — Criticité
ISO 27001	—	✓	—
ISO 22301	—	✓	(partiel)
NIST CSF	—	✓	—
DORA	—	✓	(partiel)
MDI	—	—	✓
IRON	✓	✓	✓

aura déjà identifié ses processus critiques, ce qui alimente l'axe Z. IRON valorise les investissements existants ; il ne demande pas de repartir de zéro.

La différence fondamentale est que les référentiels existants évaluent les moyens mis en œuvre (contrôles, procédures, conformité), tandis qu'IRON évalue le résultat : que se passe-t-il si, malgré ces moyens, un service numérique tombe ? C'est un renversement de perspective : non plus *que faisons-nous pour protéger ?*, mais *que se passe-t-il si la protection échoue ?* (LOCH et al. 1992)

3 L'approche par indices de criticité matérielle

Avant de proposer IRON, il est nécessaire d'examiner une approche alternative : l'évaluation de la fragilité numérique par des indices portant pour partie sur la chaîne d'approvisionnement matérielle dans le cadre de l'axe Y, la résilience du numérique. Cette approche, explorée dans le cadre du projet FabNum (PECCINI 2025), produit des résultats importants pour la sensibilisation ou les prises de décision, mais se révèle inadaptée à l'évaluation organisationnelle. Comprendre pourquoi permet de justifier le changement de paradigme qui fonde IRON.

3.1 Le projet FabNum : rendre visible la fragilité structurelle

Le projet FabNum a développé quatre indices pour quantifier la fragilité de la chaîne d'approvisionnement du numérique :

- **IHH** (indice de Herfindahl-Hirschman) : mesure la concentration des producteurs à chaque maillon de la chaîne (extraction, traitement, fabrication, assemblage) ;
- **IVC** (indice de vulnérabilité concurrentielle) : capte la pression intersectorielle sur les mêmes ressources (numérique, véhicules électriques, défense, énergies renouvelables) (BHUWALKA et al. 2022) ;
- **ICS** (indice de capacité de substitution) : évalue la faisabilité technique et économique du remplacement d'un minerai critique ;

- **ISG** (indice de sensibilité géopolitique) : intègre le contexte politique des pays producteurs (Santillán-Saldivar et al. 2021).

Ces indices démontrent de manière quantifiée que la chaîne d'approvisionnement du numérique est structurellement fragile : oligopoles de fabrication (TSMC concentre plus de 60 % de la fonderie mondiale de semi-conducteurs), concentration géographique des minerais critiques (International Energy Agency 2025), tensions de marché croissantes entre secteurs concurrents (Kosajan et al. 2025). L'IVC, en particulier, constitue une contribution originale en captant la dynamique de pression intersectorielle que les indices classiques de criticité ne mesurent pas.

3.2 Limites pour l'évaluation organisationnelle

Malgré ces apports, l'approche par indices de criticité matérielle se heurte à trois limites fondamentales lorsqu'on cherche à l'utiliser pour évaluer la 📖robustesse d'une organisation.

Mesurer les causes, pas la capacité à y faire face

Les indices FabNum mesurent la probabilité qu'une perturbation survienne dans la chaîne d'approvisionnement : concentration, tensions de marché, risques géopolitiques. Ils répondent à la question « que peut-il arriver ? » mais pas à « que se passe-t-il si cela arrive ? ». Or c'est la seconde question qui détermine l'impact sur une organisation donnée. Deux entreprises exposées aux mêmes risques supply chain peuvent avoir des niveaux de 📖robustesse très différents si l'une dispose d'alternatives fonctionnelles et l'autre non.

Un périmètre partiel de l'axe Y

FabNum ne couvre que le volet matériel de la résilience numérique : chaîne d'approvisionnement en minerais et composants, fabrication de composants et assemblage de produits finaux. Or l'axe Y d'IRON englobe la totalité de la résilience du service numérique sur l'ensemble de ses couches (matériel, logiciel, hébergement, services tiers). Pour couvrir Y par des indices de criticité, il aurait fallu assembler d'autres outils fondés sur des principes similaires (concentration des éditeurs logiciels, oligopoles d'hébergement, dépendances aux services cloud), chacun avec sa propre méthodologie et ses propres sources de données, sans garantie de cohérence entre eux.

Une dépendance externe et une complexité d'interprétation

Intégrer des indices comme ceux de FabNum dans le calcul d'IRON créerait une dépendance à un outil tiers : l'organisation serait liée à la disponibilité, la fréquence de mise à jour et la pérennité de chaque fournisseur d'indices. Les données sous-jacentes

(USGS, IEA, rapports de marché) sont difficiles d'accès, opaques et publiées avec un à deux ans de retard. De plus, la traduction d'un IHH ou d'un ISG en score de résilience organisationnelle ne va pas de soi : ces indices mesurent une exposition structurelle, pas une capacité de réponse. Cette difficulté d'interprétation se démultiplierait avec chaque outil supplémentaire nécessaire pour couvrir les autres volets de Y.

3.3 Repositionnement : de la sensibilisation à l'évaluation

L'approche par indices n'est pas inutile : elle est mal positionnée par rapport au besoin. Elle excelle dans un rôle que les référentiels de la section 2 ne remplissent pas : démontrer concrètement, chiffres à l'appui, que le numérique repose sur une base matérielle fragile. C'est un travail de sensibilisation essentiel, sans lequel les organisations n'ont pas de raison de s'engager dans une démarche de 🕮 robustesse.

En termes de classification, les indices FabNum relèvent de l'approche Safety-I : identifier ce qui peut mal tourner, cause par cause. IRON, en revanche, doit adopter une approche Safety-II : mesurer la capacité de l'organisation à continuer de fonctionner lorsqu'une perturbation survient, quelle qu'en soit la cause. Cette distinction, formalisée par Hollnagel (Hollnagel 2014), est fondamentale : on ne peut pas être exhaustif sur les causes (le Cygne Noir de Taleb est par définition imprévisible (Taleb 2007)), mais on peut évaluer la capacité de réponse.

Les indices FabNum conservent donc deux rôles :

1. **Sensibilisation** : rendre visible la fragilité structurelle du numérique pour motiver l'engagement dans une démarche IRON ;
2. **Éclairage des solutions** : un IHH élevé sur les composants mémoire oriente vers la 🕮 diversification (famille B de l'axe Y), un IVC élevé renforce l'importance du stock (🕮 redondance, famille A). Les indices répondent à « sur quoi concentrer mes efforts ? », pas à « quel est mon score ? ».

Ils ne participent donc pas au calcul d'IRON. La section suivante présente les fondements théoriques sur lesquels repose le modèle d'évaluation centré sur l'organisation.

4 Fondements théoriques

La section précédente a montré que les indices de criticité matérielle ne pouvaient pas fonder l'axe Y d'IRON. Les axes X et Z, qui relèvent de l'analyse métier, disposaient déjà d'une direction de travail issue de (Peccini 2026). L'axe Y — comment mesurer la 🕮 résilience d'un 🕮 service numérique — restait à construire. Cette section pose les fondements théoriques qui permettent de le faire, en mobilisant cinq piliers issus de

disciplines distinctes : biologie, cybernétique, sciences de gestion, sécurité de l'information et ingénierie de la résilience.

4.1 Robustesse et résilience : un choix terminologique

IRON mesure la robustesse de l'organisation, pas sa résilience. Ce choix n'est pas anodin : chaque terme désigne une propriété de nature différente, portée par un sujet différent.

La **résilience** est une propriété technique du système numérique : sa capacité à résister aux perturbations (pannes, cyberattaques, crises) et à revenir à un état fonctionnel après l'incident (Peccini 2026). Elle est réactive et limitée — limitée par la dépendance du système à des ressources externes (énergie, matériaux, infrastructures) sur lesquelles il n'a pas de contrôle direct.

La **robustesse** est une propriété organisationnelle : la capacité d'une organisation à maintenir ses fonctions essentielles de manière stable et viable face aux défaillances du numérique, en créant les conditions pour ne pas tomber (Hamant 2023 ; Peccini 2026). Elle est préventive et repose sur l'hétérogénéité des solutions, la redondance des moyens et le maintien d'alternatives — y compris faiblement technologiques.

Cette distinction est structurante pour IRON. L'indice mesure la robustesse de l'*organisation* — sa capacité à maintenir ses processus métier malgré la défaillance d'un service numérique. Pour cela, il intègre dans l'axe Y la résilience *technique* de chaque service numérique : ses capacités de redondance, de diversification, de protection et de rapidité de rétablissement. La robustesse organisationnelle dépend donc, entre autres, de la résilience technique des services qui la supportent. Mais elle ne s'y réduit pas : l'axe X mesure précisément ce qui relève de l'organisation et non du système — la capacité des équipes à opérer sans le service défaillant.

4.2 Le Viable System Model : une définition universelle de l'organisation

Pour être applicable à toute organisation — entreprise, hôpital, collectivité, association… — IRON a besoin d'une définition de l'organisation qui ne dépende ni du secteur, ni de la taille, ni du statut juridique. Le Viable System Model (VSM) de Beer fournit cette définition (Beer 1984).

Le Viable System Model (VSM) identifie cinq sous-systèmes nécessaires et suffisants pour qu'une organisation soit viable :

1. les **opérations** : les activités qui produisent la valeur ;
2. la **coordination** : la gestion des interactions entre opérations ;

3. le **contrôle** : la surveillance de la performance ;
4. l'**intelligence** : l'adaptation à l'environnement ;
5. la **politique** : l'identité et la direction.

Ces cinq fonctions existent dans toute organisation viable, quelle que soit sa forme. Un hôpital a des opérations (soins), une coordination (planification des blocs), un contrôle (qualité), une intelligence (veille sanitaire) et une politique (direction). Une PME industrielle aussi, avec d'autres contenus, mais la même structure.

IRON exploite cette universalité : l'unité d'analyse n'est pas un département ou un système technique, mais un 🕮 processus métier — une activité qui concourt à l'une de ces cinq fonctions. Toute organisation en possède ; toutes sont évaluables de la même manière.

4.3 La pérennité comme continuum

Quand un 🕮 processus métier s'arrête, quel est l'impact sur l'organisation ? Pour répondre, il faut un modèle de ce que signifie « impact sur l'organisation ». Ce modèle repose sur le concept de 🕮 pérennité organisationnelle organisationnelle : une propriété non binaire qui se déploie sur un continuum.

La pérennité n'est pas un état binaire (l'organisation existe ou non) : c'est un continuum à plusieurs niveaux (Mignon 2009 ; Marrewijk et Werre 2003) :

1. **survie** : l'organisation évite la disparition ;
2. **permanence** : elle maintient son activité dans le temps ;
3. **durabilité** : elle s'adapte aux changements de son environnement ;
4. **soutenabilité** : elle intègre les dimensions sociales et environnementales ;
5. **longévité** : elle perdure sur plusieurs générations ;
6. **hyperlongévité** : elle traverse les siècles en se réinventant.

Trois inducteurs déterminent la position d'une organisation sur ce continuum : l'*efficacité opérationnelle*, la *cohérence de mission* et la *capacité organisationnelle*. Une défaillance numérique peut affecter chacun d'entre eux : un arrêt de production touche l'efficacité, une violation de données compromet la cohérence de mission (confiance, réputation), un manquement réglementaire réduit la capacité organisationnelle (sanctions, restrictions d'activité).

IRON traduit ces inducteurs en trois dimensions de 🕮 criticité métier : opérationnelle (O), réglementaire (Reg) et réputationnelle (Rep). La dimension financière, souvent citée dans les analyses de risque, n'apparaît pas comme dimension séparée. Dans la majorité

des cas, elle est la traduction monétaire d'un impact opérationnel, réglementaire ou réputationnel — l'intégrer créerait un double comptage systématique. Ce choix a une limite : certains incidents numériques produisent un impact financier primaire sans impact significatif sur les trois dimensions retenues (fraude par usurpation d'identité numérique, paiement de rançon sans interruption durable). L'évaluateur doit en avoir conscience et, le cas échéant, relever la criticité du processus concerné via la dimension opérationnelle.

4.4 Le renversement épistémologique : des causes aux conséquences

Les référentiels de la section 2et les indices de la section 3 partagent une même logique : identifier ce qui peut mal tourner (menaces, vulnérabilités, concentrations). Cette approche se heurte à un obstacle fondamental : l'espace des causes est infini. Le Cygne Noir de Taleb est par définition l'événement que personne n'avait anticipé (Taleb 2007). On ne peut pas être exhaustif sur les causes.

IRON renverse la perspective en s'appuyant sur une observation de Loch, Carr et Warkentin : les conséquences d'une perturbation sont indépendantes de ses sources, de ses auteurs et de leurs intentions (Loch et al. 1992). Le principe est que les conséquences d'une perturbation sont stables indépendamment de ses causes. Qu'un serveur tombe à cause d'une cyberattaque, d'un incendie, d'une panne matérielle ou d'une mise à jour défectueuse, les conséquences sur le 📖service numérique se ramènent aux mêmes catégories.

Ce principe posé, il faut identifier l'espace fini dans lequel ces conséquences s'expriment. Pour les services numériques, c'est la triade 📖CIA, stabilisée par trois décennies de pratique normative (ISO 27001, NIST SP 800-53) : disponibilité, intégrité, confidentialité — trois dimensions, chacune un continuum entre le fonctionnement nominal et la perte totale. IRON n'évalue donc pas *pourquoi* un service peut tomber, mais *ce qui se passe quand il tombe*. Ce renversement — des causes infinies aux conséquences finies — est ce qui rend le modèle opérable.

En termes de classification, ce renversement peut être rapproché du passage de Safety-I à Safety-II formalisé par Hollnagel (Hollnagel 2014) : l'un focalise sur les causes d'échec, l'autre sur la capacité à fonctionner dans des conditions variables.

Ce renversement ne se limite pas à l'axe Y — il se propage aux trois axes du modèle. Pour l'axe X, au lieu de « quels scénarios d'interruption ce processus pourrait-il subir ? » (causes infinies), on demande « que se passe-t-il pour ce processus si le service tombe ? » — l'espace des réponses est fini. Pour l'axe Z, au lieu de « quels risques menacent cette organisation ? », on demande « que se passe-t-il pour l'organisation si ce processus s'arrête ? ». La structure est parallèle sur les trois axes : chacun substitue un espace de conséquences fini et évaluable à un espace infini de causes.

4.5 Le cadre 4R de la résilience

Comment évaluer la capacité d'un service numérique à résister aux perturbations ? Le cadre 4R de Bruneau et al., développé pour la résilience sismique des communautés, fournit une taxonomie des capacités de réponse (Bruneau et al. 2003) :

- **Robustness** (résistance) : capacité à absorber le choc sans dégradation ;
- **Redundancy** (redondance) : existence de composants de secours ;
- **Resourcefulness** (réponse) : capacité à mobiliser des ressources pour gérer la crise ;
- **Rapidity** (rapidité de rétablissement) : vitesse de retour à un fonctionnement acceptable.

IRON transpose ce cadre au domaine numérique en quatre familles de solutions :

- **A** — **Redondance** : dupliquer les composants critiques (serveurs miroirs, sauvegardes, sites de repli) ;
- **B** — **Diversification** : utiliser des composants de nature différente pour éviter les défaillances de mode commun (multi-fournisseur, multi-cloud, logiciel alternatif) ;
- **C** — **Protection** : réduire la probabilité ou l'impact des perturbations (pare-feu, chiffrement, contrôle d'accès) ;
- **D** — **Rapidité de rétablissement** : minimiser le temps de rétablissement (PRA testé, équipe d'astreinte, procédures de bascule).

Ces quatre familles sont une réorganisation originale, inspirée du cadre 4R mais adaptée au contexte numérique. La Redundancy de Bruneau est scindée en deux familles : A pour les composants internes, B pour les dépendances externes — distinction essentielle dans un écosystème numérique où la diversification des fournisseurs constitue un levier spécifique. La Robustness — capacité structurelle à absorber un choc — ne se transpose pas au niveau du service numérique : le numérique ne peut pas être robuste au sens de Hamant, car il dépend de ressources et d'infrastructures fragiles sur lesquelles il n'a pas de prise (Peccini 2026). C'est précisément cette robustesse que l'indice IRON mesure au niveau de l'*organisation*.

Au niveau du service, la famille C — Protection — prend une place complémentaire : elle regroupe les mesures qui réduisent la probabilité ou l'impact des perturbations, complétant les trois autres familles pour couvrir l'ensemble des leviers de résilience technique. La Rapidity inspire la famille D. La Resourcefulness — la capacité à mobiliser des ressources humaines et organisationnelles — n'apparaît pas comme une famille distincte, mais elle est intégrée dans les grilles d'évaluation (section 5) : les critères de qualification incluent

explicitement les capacités humaines — effectifs disponibles, compétences, soutenabilité des équipes — tant pour la substituabilité que pour la résilience. Le score Y d'IRON évalue la maturité opérationnelle de ces quatre familles pour chaque service numérique, en appliquant le principe du maillon faible : la résilience globale est déterminée par la famille la plus faible.

4.6 La triade CIA comme espace des conséquences

Le renversement épistémologique (section 4.4) pose que l'espace des conséquences d'une perturbation sur un service numérique se réduit à trois dimensions :

- **Disponibilité** : le service est-il accessible quand on en a besoin ?
- **Intégrité** : les données et traitements sont-ils fiables et non altérés ?
- **Confidentialité** : les données sont-elles accessibles uniquement aux personnes autorisées ?

Chacune de ces dimensions est un continuum, pas un état binaire. Un service peut être partiellement disponible (dégradé), partiellement intègre (quelques données corrompues) ou partiellement confidentiel (fuite limitée). Les grilles d'évaluation de l'axe Y (section 5) déclinent chaque famille de solutions selon ces trois dimensions, créant une matrice d'exhaustivité qui garantit qu'aucun angle de fragilité n'est oublié.

L'articulation entre ces cinq piliers se résume ainsi : le VSM définit *ce qu'on évalue* (des processus métier universels), la pérennité définit *contre quoi on mesure l'impact* (un continuum à trois inducteurs), le renversement épistémologique définit *comment on aborde le problème* (par les conséquences, pas les causes), le cadre 4R définit *comment on structure les solutions* (quatre familles), et la triade CIA définit *l'espace dans lequel on évalue la fragilité* (trois dimensions finies). La section suivante assemble ces éléments en un modèle opérationnel.

5 Le modèle IRON

Cette section assemble les fondements de la section 4 en un modèle opérationnel. Chaque élément théorique trouve sa traduction concrète : le VSM fonde l'unité d'analyse, la pérennité structure l'axe Z, le renversement épistémologique oriente l'axe Y, le cadre 4R organise les familles de solutions et la triade CIA garantit l'exhaustivité de l'évaluation.

5.1 Architecture générale

L'unité d'analyse d'IRON est le processus métier : un ensemble d'activités concourant à un résultat identifiable pour l'organisation et utilisant au moins un service

numérique. Ce choix découle du VSM : tout processus, dans toute organisation, peut être rattaché à l'un des cinq sous-systèmes de Beer.

Chaque processus est évalué sur trois axes indépendants, chacun noté de 1 à 5 :

- **X** — la substituabilité fonctionnelle numérique : le processus peut-il fonctionner sans son service numérique ? (1 = aucune alternative, 5 = alternative équivalente et pratiquée)
- **Y** — la résilience numérique : le service numérique est-il capable de résister à une perturbation ? (1 = aucune mesure, 5 = résilience maximale)
- **Z** — la criticité métier métier : quel est l'impact sur l'organisation si ce processus s'arrête ? (1 = impact négligeable, 5 = impact existentiel)

Les axes X et Y mesurent la maîtrise de la dépendance numérique : les alternatives dont dispose l'organisation (X) et la résilience de ses services (Y). L'axe Z est le pondérateur métier : il détermine combien les scores X et Y comptent pour chaque processus. Un processus peut être faiblement substituable (X bas) mais peu critique (Z bas), ou inversement. Un service peut être très résilient (Y élevé) tout en supportant un processus critique sans alternative (Z élevé, X bas). C'est le croisement des trois qui révèle la robustesse réelle.

Prérequis : cartographie des dépendances. L'évaluation IRON suppose un inventaire préalable des processus métier, des service numériques qui les supportent et de la matrice de dépendance qui les relie. Sans cette cartographie, on ne sait pas *quoi* évaluer. L'inventaire doit identifier, pour chaque service, ses composants principaux, ses fournisseurs et le type d'hébergement (interne, SaaS, hybride) — informations indispensables à l'évaluation des familles A (redondance) et B (diversification) de l'axe Y. Cette phase d'inventaire est formalisée dans la démarche opérationnelle (Peccini 2026).

5.2 Axe X — Substituabilité numérique

L'axe X évalue la substituabilité fonctionnelle du service numérique qui supporte le processus : le processus peut-il continuer de fonctionner si ce service tombe ?

L'évaluation croise deux dimensions :

- la **substituabilité** (S) : existence d'une alternative au service numérique ;
- la **maturité** (M) : degré de préparation effective de cette alternative.

L'alternative au service numérique défaillant peut être de nature variée : un autre service numérique (basculement vers un logiciel concurrent ou un système de secours), un dispositif technique non numérique (formulaire papier, outil mécanique, procédure

manuelle outillée), ou une prise en charge purement humaine (traitement oral, intervention manuelle, compétence métier exercée sans support technique). Ce qui compte n'est pas la nature de l'alternative, mais sa qualité et sa tenabilité — et la capacité des équipes à l'opérer.

La substituabilité se décline en quatre niveaux :

S0 **Aucune alternative** : le processus s'arrête purement et simplement.

S1 Alternative **dégradée et non tenable** dans la durée : les équipes peuvent se débrouiller temporairement, mais le service est dégradé et la situation va s'effondrer (personnel détourné d'autres tâches, retards cumulatifs, compétences insuffisantes en nombre).

S2 Alternative **dégradée mais tenable**, ou **équivalente mais non tenable** : soit le service est dégradé mais les équipes savent le maintenir indéfiniment (facturation manuelle plus lente mais maîtrisée), soit le service est maintenu à niveau équivalent mais au prix de ressources non soutenables (mobilisation d'un prestataire externe facturé à l'heure, astreinte permanente d'une équipe réduite).

S3 Alternative **équivalente et tenable** durablement : les équipes maîtrisent une alternative qui permet au processus de fonctionner normalement sans le numérique concerné.

La distinction entre « dégradé mais tenable » et « équivalent mais non tenable » (tous deux S2) est importante : le premier est une béquille permanente — visible, stable, gérable ; le second est un sprint — le service semble maintenu mais des ressources sont consommées ailleurs et la situation finira par s'effondrer.

La 📖 maturité opérationnelle de l'alternative se décline en trois niveaux :

M0 **Théorique** : l'alternative existe sur le papier, dans un PCA ou dans la tête de quelqu'un, mais n'a jamais été testée.

M1 **Testée régulièrement** : l'alternative a été validée lors d'un exercice de crise ou d'un test régulier.

M2 **Pratiquée au quotidien** : l'alternative coexiste avec le numérique en permanence (double circuit actif).

Le croisement S × M produit le score X :
S0 (aucune alternative) n'apparaît pas dans la grille : une alternative inexistante ne peut être ni testée ni pratiquée. Le score est toujours 1.

La grille suit une diagonale 1-3-5 : plus l'alternative est bonne (S) et plus elle est validée (M), plus le score monte. Un cas limite mérite attention : S1/M0 obtient 1, car

TABLE 2 : Grille $S \times M$ (scores pour les axes X et Y).

	M0 (théorique)	**M1** (testée)	**M2** (pratiquée)
S1 (dég. + non ten.)	1	2	3
S2 (dég. ou non ten.)	2	3	4
S3 (équivalente)	3	4	5

une alternative à la fois dégradée, non tenable et jamais testée est fictive — dans les faits, elle n'existe pas. C'est un choix conservateur assumé : en l'absence de tout test, on ne peut pas distinguer une procédure réellement mobilisable d'une déclaration d'intention. Le critère M est précisément conçu pour capturer cette distinction ; assimiler S1/M0 à S0 en est la conséquence logique, au prix d'une sensibilité réduite en bas d'échelle. À l'autre extrémité, S1/M2 = 3 peut surprendre : pourquoi la pratique quotidienne d'une situation intrinsèquement non soutenable améliore-t-elle le score ? Parce que la pratique réduit le temps de réaction, révèle plus tôt le point de rupture et permet à l'organisation de planifier la transition — elle ne rend pas la situation tenable, mais elle en maîtrise la dégradation.

L'évaluation est guidée par un arbre de décision scénarisé. Le scénario déclencheur est : *« ce service numérique s'arrête complètement »*.

1. **Le processus métier peut-il continuer ?** Non → S0 = 1. Oui → question suivante.
2. **À quel niveau de service ?** Équivalent ou la dégradation mineure n'entache en rien la capacité à produire le service → S3 (évaluer M). Dégradé ou non tenable → question suivante.
3. **L'alternative est-elle à la fois dégradée et non tenable ?** Oui → S1 (évaluer M). Non : l'alternative est soit dégradée, mais tenable, soit non dégradée, mais non tenable → S2 (évaluer M).

Des questions complémentaires qualifient la maturité : l'alternative est-elle mise en œuvre au quotidien ? A-t-elle été testée lors d'un exercice ? Le personnel sait-il l'utiliser ? A-t-elle déjà été utilisée lors d'un incident réel ? Ces questions factuelles réduisent le biais d'auto-évaluation : la réponse est vérifiable, pas subjective.

5.3 Axe Y — Résilience numérique

L'axe Y est le cœur méthodologique d'IRON. Il évalue la résilience de chaque service numérique : sa capacité à résister aux perturbations affectant sa disponibilité, son intégrité ou sa confidentialité.

Évaluation par service numérique, pas par processus

Un même service numérique peut supporter plusieurs processus métier. Un ERP, par exemple, supporte la gestion commerciale, la comptabilité et la gestion des stocks. Évaluer l'axe Y une fois par service, puis réutiliser le score pour chaque processus qui en dépend, évite la redondance d'évaluation et garantit la cohérence. C'est le principe de *factorisation*, détaillé en section 6.

Quatre familles de solutions

L'axe Y s'appuie sur les quatre familles issues du cadre 4R (section 4) :

- **A** — **Redondance** : composants dupliqués (serveur miroir, sauvegarde, site de repli) ;
- **B** — **Diversification** : composants de nature différente (multi-fournisseur, multi-cloud, systèmes d'exploitation distincts) ;
- **C** — **Protection** : mesures préventives (pare-feu, chiffrement, contrôle d'accès, mise à jour) ;
- **D** — **Rapidité de rétablissement** : capacité de rétablissement (PRA testé, équipe d'astreinte, procédures de bascule).

Pour chaque famille, l'évaluation utilise la même grille S × M que l'axe X (tableau 2), mais appliquée aux sous-composants du service numérique. Chaque sous-composant est évalué avec un arbre de décision propre à la famille, puis le maillon faible (score le plus bas) détermine le score de la famille. Les sous-composants minimaux à considérer sont :

A — Redondance : traitement (serveurs, instances), stockage (disques, réplication), réseau (liens, routeurs), énergie (onduleurs, groupes électrogènes), données (sauvegardes, site de reprise).

B — Diversification : fournisseur cloud ou hébergement, logiciel système, logiciel applicatif, données (sites, juridictions, formats), services tiers (DNS, CDN, CA), compétences.

C — Protection : contrôle d'accès, sécurité réseau, sécurité des postes, sécurité applicative, chiffrement, gestion des correctifs, sensibilisation.

D — Rapidité : détection (monitoring, alerting), réponse (procédures d'incident, astreinte), reprise (PRA, restauration, bascule), test (exercices de reprise).

Ces listes sont indicatives : chaque organisation les adapte à son contexte. Une startup full-cloud n'évalue pas les mêmes sous-composants qu'une usine avec SCADA, mais la grille est la même.

Arbres de décision par famille

Arbre A — Redondance. Pour chaque sous-composant :

1. Ce sous-composant dispose-t-il d'un équivalent capable de prendre le relais en cas de défaillance ? Non → S0 = 1. Oui → question suivante.

2. Lorsque cet équivalent prend le relais, le service rendu est-il équivalent ou dégradé ? La situation est-elle tenable dans le temps ? Dégradé et non tenable → S1. Dégradé ou non tenable (exclusif) → S2. Équivalent et tenable → S3 (évaluer M).

Arbre B — Diversification. Pour chaque dépendance externe :

1. Cette dépendance repose-t-elle sur un seul fournisseur, une seule technologie ou un seul chemin ? Oui → S0 = 1. Non → question suivante.

2. Si le fournisseur ou la technologie principale devient indisponible, le service rendu par l'alternative est-il équivalent ou dégradé ? La situation est-elle tenable ? Dégradé et non tenable → S1. Dégradé ou non tenable (exclusif) → S2. Équivalent et tenable → S3 (évaluer M).

Arbre C — Protection. Pour chaque aspect à protéger :

1. Une mesure de protection est-elle en place ? Non → S0 = 1. Oui → question suivante.

2. Cette protection couvre-t-elle l'ensemble du périmètre concerné ? Résiste-t-elle à une sollicitation soutenue ? Partielle et non tenable → S1. Partielle ou non tenable (exclusif) → S2. Complète et tenable → S3 (évaluer M).

La famille C se distingue des trois autres : elle évalue une mesure préventive, pas une alternative de reprise. La grille $S \times M$ s'y applique néanmoins, à condition d'expliciter la correspondance. La *couverture du périmètre* joue le rôle de la qualité du service rendu : une protection partielle est l'équivalent d'un service dégradé. La *résistance à une sollicitation soutenue* joue le rôle de la tenabilité : une protection qui s'effondre sous charge prolongée est l'équivalent d'une alternative non tenable. La combinaison des deux critères détermine le niveau S :

- S1 : protection partielle et non résistante — un contrôle d'accès qui ne couvre qu'une partie des utilisateurs et dont les règles ne sont plus maintenues ;
- S2 : protection partielle mais résistante (un chiffrement rigoureux mais limité aux données les plus sensibles), ou protection complète mais non résistante (un pare-feu couvrant tout le périmètre mais dont les règles ne sont plus à jour) ;
- S3 : protection complète et résistante dans la durée.

La dimension M évalue la vérification effective de la mesure : M0 = jamais auditée, M1 = testée par un audit ou un pentest régulier, M2 = surveillée et maintenue en continu. La protection est une mesure active et continue, pas une alternative qu'on bascule — mais la question reste la même : existe-t-elle (S) et est-elle vérifiée (M) ?

Arbre D — Rapidité. Pour chaque aspect du service :

1. Une procédure de détection et de restauration est-elle définie ? Non → S0 = 1. Oui → question suivante.

2. Cette procédure permet-elle une reprise complète ou seulement partielle ? Le délai de reprise est-il compatible avec les besoins métier ? Reprise partielle et délai incompatible → S1. Reprise partielle ou délai incompatible (exclusif) → S2. Reprise complète dans les délais → S3 (évaluer M).

La famille D est aussi le lieu où se mesurent les **compétences numériques** nécessaires au rétablissement. Une procédure de reprise n'a de valeur que si des personnes compétentes savent l'exécuter — diagnostiquer la panne, restaurer les données, basculer sur le site de secours, révoquer les accès compromis. Les questions de maturité (M) intègrent cette dimension : qui sait exécuter cette procédure ? Combien de personnes en sont capables ? Que se passe-t-il si elles sont absentes ? Une procédure testée par une seule personne qui a quitté l'organisation est de facto retombée à M0. La rapidité de rétablissement dépend autant des compétences humaines que des dispositifs techniques — et le critère M capture cette réalité.

Dans les quatre arbres, la maturité opérationnelle M se qualifie de la même manière que pour l'axe X : M0 (théorique), M1 (testée régulièrement), M2 (pratiquée au quotidien). La règle S1/M0 = 1 s'applique également : une mesure dégradée, non tenable et jamais testée est fictive.

Grille d'exhaustivité

Chaque famille est déclinée selon les trois dimensions de la triade CIA, créant une matrice qui garantit l'exhaustivité de l'évaluation :

TABLE 3 : Matrice d'exhaustivité : familles de solutions × dimensions CIA.

	Disponibilité	**Intégrité**	**Confidentialité**
A — Redondance	cluster, site de repli	réplication, RAID	chiffrement des copies
B — Diversification	multi-cloud	formats ouverts	multi-fournisseur
C — Protection	pare-feu, WAF	contrôle d'accès	chiffrement, MFA
D — Rapidité	PRA, bascule auto.	restauration	révocation d'accès

Cette grille n'est pas un questionnaire : c'est un outil de vérification. L'évaluateur parcourt chaque cellule pour s'assurer qu'aucun angle de fragilité n'a été oublié. Les exemples du tableau sont indicatifs ; chaque organisation les adapte à son contexte. Deux cellules méritent une clarification. La cellule A/Confidentialité (chiffrement des copies) traduit le fait qu'une copie de secours est un nouveau point d'exposition : la redondance crée mécaniquement un besoin de protection de la copie elle-même. La cellule B/Intégrité (formats ouverts) ne relève pas de la résilience technique au sens habituel, mais d'un choix d'architecture de données : l'usage de formats propriétaires crée une dépendance au fournisseur pour lire ses propres données, ce qui est bien un enjeu de diversification.

Composants non contrôlés : inversion de perspective

Un service numérique inclut souvent des composants que l'organisation ne contrôle pas : un service SaaS, une API tierce, un réseau opérateur. Pour ces composants, l'évaluation ne porte pas sur la résilience du fournisseur (que l'organisation ne peut ni mesurer ni influencer), mais sur la résilience de l'organisation *face à* la défaillance du fournisseur. La question n'est pas « mon fournisseur est-il fiable ? » mais « que se passe-t-il pour moi si mon fournisseur tombe ? ». C'est une application directe du renversement épistémologique : évaluer les conséquences, pas les causes.

Risque systémique exogène

Certains risques échappent au périmètre d'une organisation isolée : un fournisseur commun à tout un secteur (comme CrowdStrike avant juillet 2024), une dépendance transitive enfouie dans la chaîne logicielle. IRON reconnaît explicitement cette limite : le 📖 risque systémique exogène n'est pas évaluable au niveau d'une organisation et ne fait pas partie du score. Il relève d'une analyse sectorielle ou nationale, comme celle que les indices FabNum (section 3) peuvent alimenter.

Agrégation par maillon faible

Le score Y d'un service numérique est déterminé par le principe du 📖 maillon faible : la résilience globale est celle de la famille la plus faible.

L'agrégation se fait en deux temps :

1. **Intra-famille** : pour chaque famille (A, B, C, D), le score est le *minimum* des scores des sous-composants — le sous-composant le moins résilient détermine le score de la famille.

2. **Inter-familles** : le score Y du service est le *minimum* des scores des quatre familles — la famille la plus faible détermine la résilience globale.

Ce choix est conservateur : il suffit d'une seule famille défaillante pour que le service soit fragile. Un service parfaitement redondant ($A = 5$) mais sans aucune protection ($C = 1$) obtient un $Y = 1$. Les incidents de la section 1 illustrent ce principe : chez OVHcloud, l'absence de redondance externalisée ($A = 1$) a suffi à détruire des données, indépendamment de la qualité des protections ; chez les organisations touchées par CrowdStrike, l'absence de diversification ($B = 1$) a suffi à les paralyser, malgré leurs investissements en sécurité ; à Daejeon, l'absence de bascule automatique ($D = 1$) a paralysé 647 services malgré l'existence de sites de repli. Dans chaque cas, une seule famille défaillante a déterminé l'issue.

Le score Y doit donc être lu à deux niveaux : le score agrégé est un **signal d'alerte** (un $Y = 1$ signifie qu'au moins une famille est défaillante et que le service est fragile), le profil détaillé (A, B, C, D) est le **diagnostic** (il identifie quelle famille est défaillante et où investir). Un service ayant $A=5, B=5, C=5, D=1$ et un service ayant $A=1, B=1, C=1, D=1$ obtiennent le même signal ($Y=1$), mais leurs diagnostics — et donc leurs plans d'action — sont radicalement différents.

5.4 Axe Z — Criticité métier

L'axe Z évalue l'impact qu'aurait l'arrêt d'un 📖 processus métier sur la 📖 pérennité organisationnelle de l'organisation. Il traduit les trois inducteurs de la pérennité en dimensions mesurables :

- **O** — impact **opérationnel** : l'arrêt du processus empêche-t-il l'organisation de délivrer ses produits ou services ?
- **Reg** — impact **réglementaire** : l'arrêt du processus met-il l'organisation en infraction ?
- **Rep** — impact **réputationnel** : l'arrêt du processus porte-t-il atteinte à l'image de l'organisation auprès de ses parties prenantes ?

L'évaluation de chaque dimension porte sur les conséquences *ultimes* de l'arrêt du processus, pas sur ses conséquences directes seules. Dans le 📖 VSM, les sous-systèmes sont interconnectés : l'arrêt d'un processus peut entraîner l'arrêt d'autres processus qui en dépendent. L'évaluateur ne doit pas considérer le processus en vase clos : si l'arrêt de la gestion commerciale entraîne celui de la facturation, puis de la trésorerie, c'est l'impact de cette cascade complète qui détermine le score Z de la gestion commerciale. Les interdépendances entre 📖 processus métier ne font donc pas l'objet d'un mécanisme de propagation séparé : elles sont absorbées dans l'évaluation de l'axe Z de chaque processus amont. Dans une organisation complexe, ces cascades peuvent traverser plusieurs niveaux ; l'évaluation de Z pour un processus amont devrait être conduite avec des personnes

connaissant l'ensemble de la chaîne aval, pas seulement le processus évalué. Sans cette précaution, le risque de sous-évaluation systématique de Z pour les processus amont est réel : l'évaluateur qui ne connaît que son processus immédiat ignore les conséquences en cascade. Ce mécanisme garantit le découplage entre les axes Y et Z : l'axe Y est évalué par service numérique, l'axe Z par processus métier. Si un même service supporte dix processus dont certains ont des cascades complexes, l'évaluateur de Y n'a pas besoin de connaître ces cascades — elles sont entièrement absorbées dans les scores Z des processus concernés.

Pourquoi pas de dimension financière ?

La dimension financière est absente parce qu'elle est transverse. Une perte de chiffre d'affaires est toujours la conséquence d'un impact opérationnel (production arrêtée), réglementaire (amende, suspension d'activité) ou réputationnel (perte de clients). L'intégrer comme dimension séparée créerait un double comptage : l'impact serait compté une fois dans sa dimension causale et une seconde fois dans la dimension financière.

Pondération non linéaire

Chaque dimension est évaluée sur quatre niveaux : pas d'impact (0), marginal (1), significatif (4), menaçant (10). La progression est non linéaire : l'écart entre « marginal » et « significatif » est plus grand qu'entre « pas d'impact » et « marginal », et l'écart entre « significatif » et « menaçant » est plus grand encore. Ce choix reflète la réalité : quatre gênes marginales ($4 \times 1 = 4$) équivalent à une dégradation significative isolée ($1 \times 4 = 4$), ce qui est juste ; mais elles ne pèsent jamais autant que deux dégradations significatives ($2 \times 4 = 8$). Un seul « menaçant » (10) dépasse toute combinaison de « significatifs » — une menace existentielle sur une dimension suffit.

Les valeurs 0, 1, 4, 10 sont contraintes par des choix interprétatifs explicites, adossés aux seuils de conversion du tableau 5. Un score brut ≥ 10 doit correspondre à « au moins une dimension menaçante » (ce qui impose la valeur 10 pour le niveau menaçant). Un score brut de 4 doit marquer l'entrée dans la zone d'impact significatif (ce qui impose la valeur 4 pour le niveau significatif). La valeur 1 pour le niveau marginal est le minimum non nul. Toute autre progression respectant ces contraintes (par exemple 0, 1, 5, 10) décalerait les seuils sans changer la logique ; les valeurs retenues sont celles qui produisent les correspondances les plus lisibles entre score brut et interprétation qualitative.

Agrégation en score Z

Le score brut de criticité est la somme des trois dimensions : $Z_{\text{brut}} = O + \text{Reg} + \text{Rep}$, ce qui donne une valeur entre 0 et 30. Ce score brut est ensuite converti en score Z entre 1 et 5 par une table de correspondance :

TABLE 4 : Niveaux de pondération pour chaque dimension de l'axe Z.

Dimension	**Pas d'impact**	**Marginal**	**Significatif**	**Menaçant**
Opérationnel (O)	0	1	4	10
Réglementaire (Reg)	0	1	4	10
Réputationnel (Rep)	0	1	4	10

TABLE 5 : Conversion du score brut de criticité en score Z.

$Z_{\mathbf{brut}}$	**Score Z**	**Interprétation**
0	1	Aucun impact
1	2	Un marginal isolé
2–4	3	Plusieurs marginaux ou un significatif isolé
5–9	4	Un significatif accompagné ou plusieurs significatifs
≥ 10	5	Au moins un menaçant

Les seuils correspondent à des ruptures qualitatives explicitement motivées. Un score brut de 1 signifie exactement un marginal isolé (score 2) ; dès 2, on entre dans la zone significative (score 3). Un score brut ≥ 10 signifie qu'au moins une dimension est menaçante — un seul « menaçant » suffit à placer le processus au niveau de criticité maximal (score 5).

Questionnaire scénarisé

Comme pour l'axe X, l'évaluation repose sur un scénario déclencheur suivi d'un arbre de décision par dimension. Le scénario est : *« ce processus métier s'arrête complètement »*. L'arrêt complet est le cas limite conservateur : il borne le score Z par le haut et simplifie l'évaluation. Les axes X et Y modélisent la dégradation graduellement parce qu'ils évaluent des *solutions* (qui peuvent être partielles) ; l'axe Z évalue un *impact organisationnel*, et le scénario du pire est le plus reproductible. Pour chacune des trois dimensions, l'évaluateur répond à trois questions en cascade :

Dimension opérationnelle — *Capacité à produire le service, le produit ou à remplir la mission.*

1. L'arrêt de ce processus affecte-t-il la capacité de l'organisation à produire son service, son produit ou à remplir sa mission ? Non $\rightarrow$ poids $= 0$. Oui $\rightarrow$ question suivante.

2. L'organisation peut-elle continuer à fonctionner sans mesure particulière, avec une gêne mineure ? Oui $\rightarrow$ poids $= 1$ (marginal). Non $\rightarrow$ question suivante.

3. L'organisation peut-elle encore remplir sa mission fondamentale sur cette dimension ? Oui, mais en mode dégradé et la situation s'aggrave $\rightarrow$ poids $= 4$ (significatif). Non, la mission est compromise $\rightarrow$ poids $= 10$ (menaçant).

Dimension réglementaire — *Droit d'exister et d'opérer.*

1. L'arrêt de ce processus crée-t-il un risque de non-conformité réglementaire ou de perte de légitimité ? Non → poids = 0. Oui → question suivante.

2. Ce risque est-il mineur (écart corrigeable sans conséquence, observation sans sanction) ? Oui → poids = 1 (marginal). Non → question suivante.

3. L'organisation risque-t-elle de perdre ce qui l'autorise à exister ou à opérer ? Non, mais sanctions, mises en demeure ou perte partielle de prérogatives → poids = 4 (significatif). Oui (retrait de licence, perte de mandat, dissolution) → poids = 10 (menaçant).

Dimension réputationnelle — *Capital de confiance des parties prenantes.* L'évaluation se fait sous hypothèse de divulgation : l'impact est estimé comme si l'incident devenait public, indépendamment de la probabilité que cela se produise.

1. L'arrêt de ce processus affecte-t-il la confiance des parties prenantes (clients, citoyens, donateurs, partenaires) ? Non → poids = 0. Oui → question suivante.

2. L'impact est-il temporaire et facilement réparable (incident mineur, gêne passagère) ? Oui → poids = 1 (marginal). Non → question suivante.

3. La confiance des parties prenantes essentielles est-elle durablement compromise ? Partiellement, avec un effort de rétablissement nécessaire → poids = 4 (significatif). Oui, perte de confiance majeure mettant en cause la pérennité → poids = 10 (menaçant).

Le score brut est la somme des trois poids, convertie en score Z par le tableau 5.

5.5 Formule IRON

Pour chaque processus métier i, le produit $X_i \times Y_i$ mesure sa *maîtrise du risque numérique* : combinaison de la substituabilité du processus et de la résilience du service qui le supporte. La criticité métier Z_i détermine combien cette maîtrise pèse dans le score global : plus un processus est critique, plus son niveau de maîtrise influence l'indice.

Le *taux de maîtrise* de chaque processus est :

$$R_i = \frac{X_i \times Y_i}{25}$$

Il varie de $\frac{1}{25}$ (aucune substituabilité, aucune résilience) à 1 (substituabilité et résilience maximales).

L'indice IRON agrège ces taux en un score unique, pondéré par la criticité :

$$\text{IRON} = \frac{\sum_{i=1}^{n} Z_i \cdot R_i}{\sum_{i=1}^{n} Z_i} = \frac{\sum_{i=1}^{n} Z_i \cdot X_i \cdot Y_i}{25 \cdot \sum_{i=1}^{n} Z_i}$$

IRON est la moyenne des taux de maîtrise, pondérée par la criticité métier de chaque processus. Cette formule a trois propriétés immédiates :

1. Z ne contribue pas directement au score — il détermine *combien* le taux de maîtrise de chaque processus compte ;
2. améliorer X ou Y sur un processus peu critique (Z_i faible) ne change quasiment rien au score global ;
3. la priorité d'action est limpide : améliorer X ou Y là où Z est maximal.

Règle de lecture. Le score IRON agrégé ne doit jamais être interprété seul. Deux processus ayant le même produit $X \times Y$ peuvent refléter des réalités différentes : un processus faiblement substituable ($X = 1$) adossé à un service résilient ($Y = 4$) n'est pas dans la même situation qu'un processus substituable ($X = 4$) adossé à un service fragile ($Y = 1$), même si leur taux de maîtrise est identique. Le score global doit être lu conjointement avec les profils détaillés : scores X par couple (processus, service), scores Y par famille (A, B, C, D) et par sous-composant, scores Z par dimension (O, Reg, Rep). La démarche opérationnelle (Peccini 2026) détaille les règles de lecture et d'analyse des résultats.

Bornes

Le score IRON est borné entre 4 % et 100 % :

- **4 %** (robustesse minimale) : tous les $X_i = 1$ et $Y_i = 1$. Aucun processus n'est substituable, aucun service numérique n'est résilient. L'organisation est exposée à toute perturbation.
- **100 %** (robustesse maximale théorique) : tous les $X_i = 5$ et $Y_i = 5$. Chaque service numérique dispose de solutions matures dans les quatre familles, et chaque processus a une alternative équivalente et pratiquée.

Le plafond de 100 % est théoriquement accessible mais pratiquement inatteignable : il supposerait, pour chaque sous-composant de chaque service numérique, une solution équivalente, tenable et pratiquée en permanence dans les quatre familles. Le risque résiduel

incompressible empêche d'atteindre la perfection — mais l'objectif d'IRON est de mesurer la progression, pas d'atteindre un absolu.

5.6 Illustration

Pour rendre le modèle concret, considérons cinq processus métier fictifs, évalués sur les trois axes :

Id	Description	X_i	Y_i	Z_i
P1	Non substituable, résilience moyenne, critique	1	3	4
P2	Substituabilité basse, bonne résilience, peu critique	2	5	2
P3	Bonne substituabilité, résilience faible, très critique	4	2	5
P4	Excellente substituabilité, bonne résilience, criticité moyenne	5	4	3
P5	Substituabilité et résilience moyennes, critique	3	2	4

TABLE 6 : Cinq processus métier fictifs évalués sur les axes X, Y et Z.

La figure 2 cartographie ces processus sur le plan $X \times Y$. Le dégradé de couleur indique le taux de maîtrise $R_i = X_i \times Y_i/25$: du rouge (4 %, aucune maîtrise) au vert (100 %, maîtrise maximale). La taille de chaque cercle est proportionnelle à la criticité Z_i. Les processus les plus préoccupants sont les gros cercles en zone rouge : critiques et mal couverts.

La figure 3 ajoute la dimension verticale : chaque processus s'élève à la hauteur de sa contribution $Z_i \times X_i \times Y_i/25$. Plus la tige est haute, plus le processus contribue positivement au score IRON global.

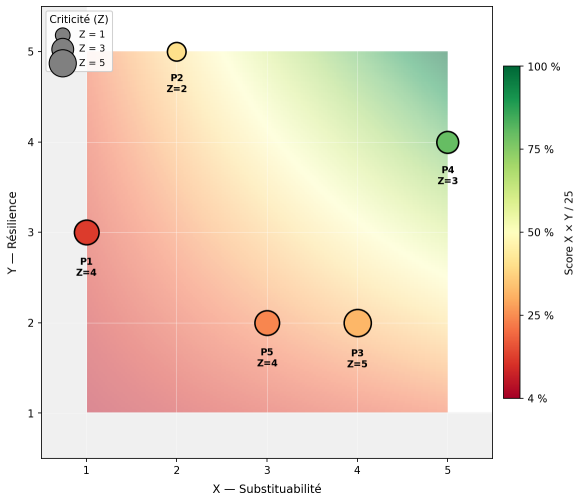

FIGURE 2 : Cartographie des processus ($X \times Y$).

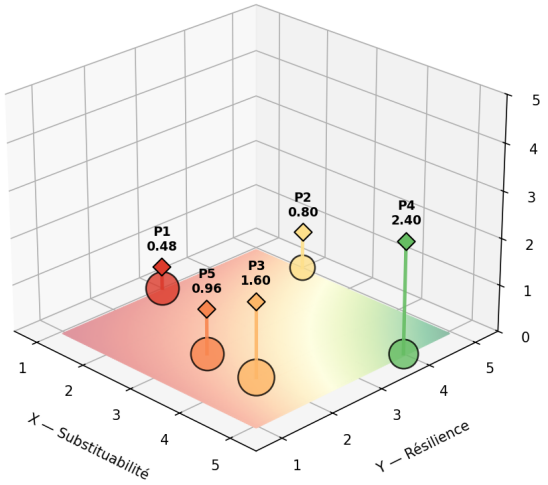

FIGURE 3 : Score IRON par processus ($Z \times X \times Y/25$).

Calcul de l'indice

Le taux de maîtrise et la contribution pondérée de chaque processus sont :

Id	X_i	Y_i	Z_i	$R_i = \frac{X_i \times Y_i}{25}$	$Z_i \times R_i$
P1	1	3	4	0,12	0,48
P2	2	5	2	0,40	0,80
P3	4	2	5	0,32	1,60
P4	5	4	3	0,80	2,40
P5	3	2	4	0,24	0,96
Total			**18**		**6,24**

TABLE 7 : Calcul détaillé de l'indice IRON pour les cinq processus.

$$\text{IRON} = \frac{\sum Z_i \cdot R_i}{\sum Z_i} = \frac{6{,}24}{18} \approx 34{,}7\,\%$$

Ce score de 34,7 % signale une robustesse à améliorer. La lecture conjointe des deux figures montre où agir : P1 (gros cercle rouge, tige basse) est le processus le plus exposé — critique ($Z = 4$), peu substituable ($X = 1$) et moyennement résilient ($Y = 3$). P3, malgré une bonne substituabilité, souffre d'une résilience faible qui limite sa contribution. P4, en revanche, illustre un processus bien maîtrisé : sa tige haute montre qu'il tire le score vers le haut.

6 Propriétés du modèle

Le modèle IRON possède plusieurs propriétés structurelles qui méritent d'être explicitées : elles ne résultent pas de choix de conception ad hoc, mais découlent de la structure même du modèle. Cette section les établit, puis identifie les limites explicites du modèle.

6.1 Choix d'agrégation explicites, sans calibrage sectoriel

IRON ne requiert aucun paramètre sectoriel à calibrer : ni pondération par secteur d'activité, ni seuil ad hoc, ni coefficient d'ajustement. En revanche, le modèle repose sur des choix d'agrégation explicites — le minimum pour l'axe Y, le produit pour $X \times Y$, les poids non linéaires de l'axe Z, la normalisation par 25 — qui sont des décisions de modélisation argumentées (voir ci-après et section 8), non des constantes universelles. Leur stabilité devra être vérifiée par l'analyse de sensibilité prévue dans la stratégie de validation (section 7).

Le produit comme mesure naturelle

Le produit $X \times Y$ mesure naturellement la maîtrise du risque numérique pour un processus. Il combine la substituabilité (l'organisation peut-elle se passer du service ?) et la résilience (le service peut-il résister aux perturbations ?). La compensation est impossible : un service très résilient ($Y = 4$) mais irremplaçable ($X = 1$) reste un risque, car si la résilience échoue, il n'y a pas de recours.

Pondération inter-processus sans arbitraire

La formule utilise Z_i (criticité métier) comme poids. Ce n'est pas un choix arbitraire : c'est une conséquence logique du modèle. Les processus les plus critiques pour la 📖 pérennité organisationnelle pèsent davantage dans le score. Un processus à faible impact ($Z = 1$) pèse 5 fois moins qu'un processus existentiel ($Z = 5$).

Universalité sectorielle

L'absence de paramètres sectoriels est une propriété, pas un appauvrissement. La spécificité sectorielle émerge naturellement des réponses :

- un hôpital a des processus à fort impact réglementaire (Z élevé sur Reg) — cela ressort automatiquement de l'arbre de décision Z ;
- dans une usine à lignes de production automatisées, les opérateurs ne savent plus faire manuellement — l'arbre de décision X produit un score S0 ou S1, donc X bas, sans que l'évaluateur ait besoin de savoir que « l'industrie est dépendante du numérique » ;

- une collectivité territoriale a des obligations de continuité de service public (Z élevé sur O) — même mécanisme.

Les listes de sous-composants à évaluer pour l'axe Y s'adaptent à l'infrastructure réelle de l'organisation : une startup full-cloud n'évalue pas les mêmes éléments qu'une usine avec SCADA, mais la grille $S \times M$ reste la même. Le fondement théorique de cette universalité est triple : le VSM de Beer définit l'organisation indépendamment du secteur (section 4), le concept de 📖pérennité organisationnelle s'applique à toute organisation viable, et la triade CIA — stabilisée par trois décennies de pratique normative internationale — s'applique à tout service numérique quelle que soit l'infrastructure.

6.2 Factorisation algébrique

La formule IRON $= \frac{\sum(Z_i \times X_i \times Y_i)}{25 \times \sum Z_i}$ se réécrit :

$$\text{IRON} = \frac{1}{25} \times \frac{\sum(Z_i \times X_i \times Y_i)}{\sum Z_i}$$

IRON est la moyenne des produits $X_i \times Y_i$, pondérée par la criticité Z_i, et normalisée par le maximum théorique 25. Cette réécriture révèle trois propriétés :

1. Z ne contribue pas directement au score — il détermine *combien* le taux de maîtrise de chaque processus compte ;
2. améliorer X ou Y sur un processus peu critique (Z_i faible) ne change quasiment rien au score global ;
3. la priorité d'action est limpide : améliorer X ou Y là où Z est maximal.

Les bornes confirment la cohérence : si tous les $X_i = 5$ et $Y_i = 5$ (robustesse maximale), IRON $= 100\,\%$; si tous les $X_i = 1$ et $Y_i = 1$ (aucune substituabilité, aucune résilience), IRON $= 4\,\%$. Le plafond de $100\,\%$ est théoriquement accessible, mais pratiquement inatteignable : il supposerait une perfection dans les quatre familles de résilience pour chaque service, et une alternative équivalente et pratiquée pour chaque processus.

6.3 Factorisation de l'évaluation

La factorisation algébrique a un corollaire opérationnel : l'effort d'évaluation peut être considérablement réduit sans perte de précision.

Factorisation de Y par service numérique

X et Z sont des propriétés du 📖processus métier : chaque processus a sa propre 📖substituabilité fonctionnelle et son propre impact. Mais Y est une propriété du 📖service

numérique : la résilience de l'ERP ne dépend pas du processus qui l'utilise. Si 50 processus s'appuient sur 12 services numériques, on fait 12 évaluations Y au lieu de 50. Si un service améliore sa résilience, tous les processus dépendants en bénéficient automatiquement dans le score.

Priorisation par Z

La factorisation algébrique montre que les processus à Z_i faible pèsent peu dans le score. La priorité d'évaluation est donc donnée aux processus à criticité élevée. On peut obtenir un IRON fiable en évaluant X et Y sur une fraction des processus : ceux dont la criticité Z est la plus élevée.

Illustration : l'effet de levier de la criticité

Le principe de Pareto s'applique naturellement à la criticité métier : dans la plupart des organisations, une minorité de processus concentre la majorité du poids dans le score IRON. L'exemple suivant illustre ce mécanisme.

Soit une organisation de 10 processus, répartis comme suit : 1 processus à $Z = 5$, 2 à $Z = 4$, 2 à $Z = 3$, 2 à $Z = 2$ et 3 à $Z = 1$. La somme des criticités vaut $\sum Z_i = 26$, dont les 3 processus les plus critiques ($Z \geq 4$) totalisent 13 — exactement la moitié du poids total.

Partons d'un état initial où tous les processus ont $X_i = 1$ et $Y_i = 1$ (aucune substituabilité, aucune résilience) :

$$\text{IRON}_0 = \frac{\sum(Z_i \times 1 \times 1)}{25 \times 26} = \frac{26}{650} = 4\,\%$$

Supposons qu'on dispose des ressources pour améliorer 3 processus à $X = 5$ et $Y = 5$ (maîtrise maximale). Deux stratégies s'offrent :

Stratégie A — cibler les 3 processus les plus critiques $(Z = 5, 4, 4)$:

$$\text{IRON}_A = \frac{5 \times 25 + 4 \times 25 + 4 \times 25 + 3 + 3 + 2 + 2 + 1 + 1 + 1}{650} = \frac{338}{650} \approx 52\,\%$$

Stratégie B — cibler les 3 processus les moins critiques $(Z = 1, 1, 1)$:

$$\text{IRON}_B = \frac{5 + 4 + 4 + 3 + 3 + 2 + 2 + 1 \times 25 + 1 \times 25 + 1 \times 25}{650} = \frac{98}{650} \approx 15\,\%$$

Le même effort — 3 processus portés à la maîtrise maximale — améliore la robustesse réelle de l'organisation bien davantage dans la stratégie A que dans la stratégie B, et le score IRON le reflète : 52 % contre 15 %. La pondération par Z oriente naturellement l'effort vers les processus critiques, sans qu'aucun paramètre supplémentaire ne soit nécessaire.

Évaluation progressive

Les deux mécanismes précédents se combinent en une démarche progressive :

1. inventaire des processus métier et de leurs service numériques ;
2. évaluation rapide de Z pour tous les processus (9 questions par processus) ;
3. identification des services numériques critiques (ceux supportant les processus à Z_i élevé) ;
4. évaluation X et Y des processus et services critiques ;
5. calcul d'un IRON partiel — déjà exploitable ;
6. extension progressive aux processus restants.

À chaque étape, l'organisation dispose d'un score exploitable dont la précision augmente. Il n'est pas nécessaire d'attendre l'évaluation complète pour agir. La démarche opérationnelle détaillée est décrite dans (Peccini 2026).

6.4 Scalabilité multi-niveaux

La granularité d'IRON s'adapte à la taille de l'organisation sans modification du modèle :

- une PME (10–50 processus) procède par évaluation directe ;
- une ETI ou grande entreprise (50–200 processus) évalue par lots, en priorisant par Z ;
- un groupe multi-sites calcule un IRON par entité, puis agrège au niveau supérieur avec la même formule.

Le score reste cohérent entre organisations de tailles différentes car la formule normalise : le dénominateur $25 \times \sum Z_i$ s'ajuste automatiquement au nombre et à la criticité métier des processus. Une PME avec 10 processus bien maîtrisés peut obtenir un meilleur IRON qu'un grand groupe avec 200 processus fragiles.

6.5 Agrégation hybride structurelle

Le modèle combine deux logiques d'agrégation à des niveaux différents, chacune là où elle est pertinente :

- **maillon faible intra-service** : au sein de l'axe Y, $Y = \min(\text{familles})$. Une seule famille défaillante suffit à rendre le service fragile. C'est cohérent avec la réalité : un ransomware qui chiffre des données sans sauvegarde exploitable est catastrophique,

peu importe la qualité de la protection périmétrique. Ce choix est conservateur : deux services ayant $A=5, B=5, C=5, D=1$ et $A=1, B=1, C=1, D=1$ obtiennent le même $Y=1$, alors que leurs profils de risque diffèrent radicalement. La perte d'information est assumée : le score agrégé est un indicateur de robustesse, pas un diagnostic complet. Le profil détaillé (A, B, C, D) reste disponible pour l'analyse qualitative et l'identification des axes d'amélioration — et c'est lui qui guide l'action. Un service ayant $A=5, B=5, C=5, D=1$ a le même score $Y=1$ qu'un service ayant $A=1, B=1, C=1, D=1$, mais son *coût de progression* est radicalement différent : dans le premier cas, une seule famille est à améliorer ; dans le second, tout est à construire. Le min signale l'urgence (une famille défaillante suffit à rendre le service fragile), le profil détaillé guide la réponse. Une alternative moins conservatrice (moyenne harmonique, par exemple) atténuerait cet écrasement, mais introduirait une compensation partielle entre familles — or c'est précisément cette compensation que le principe du maillon faible exclut ;

- **produit intra-processus** : $X \times Y$ garantit qu'une seule dimension catastrophique ne peut pas être compensée par l'autre ;
- **moyenne pondérée inter-processus** : $\sum(Z_i \times X_i \times Y_i)/(25 \times \sum Z_i)$ est appropriée car les processus sont relativement indépendants — la défaillance d'un processus n'entraîne pas mécaniquement celle des autres. L'accumulation de processus fragiles dégrade bien le score global.

L'asymétrie entre ces logiques est structurellement justifiée. Au sein d'un service numérique, les quatre familles de résilience ne sont pas indépendantes face à un incident : une seule famille défaillante suffit à provoquer la perte du service, quel que soit le niveau des trois autres — les incidents de la section 1 le confirment. Le minimum traduit cette réalité : la compensation entre familles n'a pas de sens physique. En revanche, les processus métier d'une organisation sont relativement indépendants : la défaillance de la gestion commerciale ne provoque pas mécaniquement celle de la comptabilité (et lorsqu'une cascade existe, elle est absorbée dans le score Z du processus amont, section 5.4). La moyenne pondérée est donc appropriée : un processus bien maîtrisé ne compense pas un processus fragile au sens causal, mais il contribue positivement à la robustesse globale de l'organisation — qui est bien une propriété agrégée. Un processus mal maîtrisé reste identifiable dans le profil détaillé, indépendamment du score global.

Cette architecture résout le dilemme classique entre agrégation additive (qui permet la compensation) et multiplicative (qui est trop pénalisante globalement), sans introduire de seuils arbitraires.

6.6 Réduction de la subjectivité

IRON ne prétend pas éliminer toute subjectivité : l'évaluation repose sur le jugement d'un évaluateur humain. Mais le modèle réduit structurellement les biais par trois mécanismes.

Le critère M comme anti-déclaratif

La grille $S \times M$ distingue explicitement trois niveaux de maturité opérationnelle : théorique (M0), testée (M1), pratiquée (M2). Une organisation qui affirme disposer de redondance mais ne l'a jamais testée obtient M0 — un score bas, quel que soit son auto-évaluation. L'écart entre ce qui est déclaré et ce qui est vérifié est capturé structurellement.

Des questions factuelles

Les arbres de décision des trois axes posent des questions sur des faits observables, pas sur des perceptions : « L'arrêt entraîne-t-il un arrêt de production ? » (axe Z), « Ce sous-composant dispose-t-il d'un équivalent capable de prendre le relais ? » (axe Y). La marge d'interprétation est réduite par rapport à des évaluations de type « notez votre culture de résilience de 1 à 5 ».

Commensurabilité des échelles

Les axes X et Y partagent la même grille $S \times M$: les scores 1–5 ont la même signification dans les deux axes (1 = aucune solution, 5 = solution équivalente et pratiquée). L'axe Z utilise une construction différente (trois dimensions, pondération non linéaire, somme convertie) mais aboutit à la même échelle 1–5. Le produit $X \times Y$ a donc un sens : il combine deux évaluations de robustesse sur une échelle commune. Et Z pondère ce produit selon l'importance du processus.

6.7 Limites explicites

IRON a des limites qu'il convient de poser clairement plutôt que de laisser découvrir.

Dépendances transitives

IRON évalue la résilience d'un service numérique face aux conséquences d'une défaillance, pas l'inventaire exhaustif de ses dépendances. Le renversement épistémologique (section 4.4) contourne le problème : peu importe que la dépendance soit un driver réseau ou un agent de sécurité que personne n'avait identifié, les conséquences sur le service tombent toujours dans les mêmes catégories (disponibilité, intégrité, confidentialité) et les

solutions sont les mêmes (familles A, B, C, D). Néanmoins, un inventaire des services numériques par processus métier reste un prérequis opérationnel : il faut savoir à quoi appliquer l'évaluation, même si cet inventaire n'a pas besoin de descendre jusqu'aux dépendances transitives profondes.

Photographie à instant T

IRON produit une photographie de la robustesse à un instant donné. Les scores évoluent avec les changements d'architecture, de fournisseurs ou de processus. Plutôt qu'une fréquence fixe de réévaluation, le modèle se prête à une réévaluation par événement : ajout ou retrait d'un service numérique, changement organisationnel majeur, modification d'architecture, incident significatif. Seuls les processus affectés par le changement sont recalculés, et le score global se met à jour automatiquement. L'intégration dans les cycles existants (revue de direction, audit ISO, obligations DORA) reste à formaliser dans le guide opérationnel (Peccini 2026).

Reproductibilité inter-évaluateurs

Le modèle réduit la subjectivité par des questions factuelles et le critère M (section 6), mais il ne garantit pas que deux évaluateurs indépendants produisent des scores identiques pour la même organisation. Les sources de divergence sont principalement deux : la connaissance des cascades inter-processus (deux évaluateurs avec des connaissances différentes des dépendances aval attribueront des scores Z différents au même processus) et l'appréciation de la maturité M (la frontière entre « testée » et « pratiquée » peut varier selon l'évaluateur). Cette variance inter-évaluateurs est un prérequis à toute utilisation longitudinale : si les scores changent davantage en fonction de l'évaluateur que de l'état réel de l'organisation, le suivi de progression perd son sens. La reproductibilité fait l'objet d'un protocole de test dans la stratégie de validation (section 7).

Angle mort sur l'impact financier primaire

L'axe Z évalue la criticité selon trois dimensions — opérationnelle, réglementaire, réputationnelle — et exclut la dimension financière pour éviter le double comptage (section 4). Ce choix est justifié dans la majorité des cas, mais il crée un angle mort : certains incidents numériques produisent un impact financier direct sans impact significatif sur les trois dimensions retenues. Une fraude par usurpation d'identité numérique (Business Email Compromise) peut entraîner une perte financière majeure sans interruption opérationnelle, sans infraction réglementaire et sans atteinte réputationnelle — si l'incident n'est pas divulgué. Un paiement de rançon rapide suivi d'une reprise immédiate produit le même schéma. Dans ces cas, le score Z du processus concerné peut sous-estimer sa criticité réelle. L'évaluateur doit en avoir conscience et, le cas échéant, relever la criticité via la

dimension opérationnelle. Un indicateur complémentaire — un drapeau signalant un impact financier primaire directement lié au numérique et non déductible des dimensions O, Reg ou Rep — est envisagé comme développement futur, sans complexifier le score principal ni réintroduire le double comptage.

Auto-évaluation et suivi de progression

IRON est conçu comme un outil d'auto-évaluation et de suivi de progression, pas comme un classement entre organisations. Deux organisations qui obtiennent le même score ne sont pas « aussi robustes » : elles ont des profils de risque différents, des processus différents, des contextes différents. Le score IRON est un indicateur interne : il identifie les processus où l'effort d'amélioration est le plus rentable et mesure la progression dans le temps.

7 Validation

Un modèle théorique n'acquiert de crédibilité que par la démonstration de sa validité. Mais la validité n'est pas monolithique : Plusieurs niveaux de validité peuvent être distingués, dont certains sont démontrables sans données empiriques (Cook et Campbell 1979). Cette section établit d'abord la validité structurelle du modèle, puis teste sa cohérence sur des cas rétrospectifs, avant de proposer une stratégie de validation progressive.

7.1 Validité structurelle

La validité structurelle s'évalue à deux niveaux : le modèle couvre-t-il le domaine qu'il prétend mesurer (validité de contenu), et ses mesures captent-elles ce qu'elles prétendent capter (validité de construit) ?

Validité de contenu

Les trois axes d'IRON couvrent les trois dimensions identifiées comme angles morts des référentiels existants (section 2) :

- l'axe X (substituabilité fonctionnelle) comble l'absence de prise en compte des alternatives fonctionnelles — une dimension que ni l'ISO 27001, ni le NIST CSF, ni DORA n'évaluent ;
- l'axe Y (résilience) transpose le cadre 4R de Bruneau et al. (Bruneau et al. 2003) au domaine numérique, en évaluant les quatre familles de solutions (A, B, C, D) selon la triade CIA ;

- l'axe Z (📖 criticité métier) ancre l'impact dans le continuum de 📖 pérennité organisationnelle, à travers trois inducteurs (opérationnel, réglementaire, réputationnel).

Chaque axe est fondé sur un cadre normatif ou académique reconnu. La couverture du domaine est démontrable par construction, sans données empiriques.

Cohérence interne

Trois propriétés du modèle établissent sa cohérence interne :

1. la grille $S \times M$ distingue explicitement ce qui est déclaré de ce qui est vérifié : une solution théorique (M0) obtient un score inférieur à une solution testée (M1), elle-même inférieure à une solution pratiquée (M2). Le critère M est un anti-déclaratif structurel (section 6) ;

2. les axes X et Y partagent la même grille $S \times M$ et la même échelle 1–5, ce qui rend le produit $X \times Y$ sémantiquement fondé : il combine deux évaluations de même nature sur une échelle commune ;

3. l'axe Z utilise une construction différente (arbre de décision à trois dimensions) mais aboutit à la même échelle 1–5, ce qui garantit la commensurabilité avec le produit $X \times Y$ qu'il pondère.

Ces propriétés relèvent de la cohérence interne du modèle, pas de la validité de construit au sens strict de Cook et Campbell (Cook et Campbell 1979). Celle-ci supposerait de démontrer que les mesures captent effectivement les construits théoriques visés — par exemple, que le score Y corrèle avec les résultats d'un audit ISO 27001 (convergence), ou qu'IRON se comporte différemment d'un simple audit de conformité (discriminance). La validité de construit reste donc à établir empiriquement ; elle fait partie des objectifs de la phase 2 de la stratégie de validation.

7.2 Cohérence rétrospective

La validité apparente (face validity) se teste en appliquant le modèle à des incidents documentés : les scores produits sont-ils cohérents avec l'impact observé ? Quatre cas de l'introduction (section 1) permettent ce test. Chacun met en lumière un mécanisme différent du modèle.

CrowdStrike, juillet 2024 — la diversification absente

Pour Delta Air Lines, le processus de réservation et d'embarquement dépendait d'un service numérique fonctionnant sur un système d'exploitation unique (Windows) avec un agent de sécurité unique (Falcon).

- $X = 1$: aucune alternative au service numérique de réservation ;
- $Y = 1$: la famille B (📖 diversification) obtient un score de 1 (mono-OS, mono-agent), et $Y = \min(\text{familles})$;
- $Z = 5$: impact existentiel (500 millions de dollars de pertes, flotte clouée au sol).

Le taux de maîtrise vaut $R = 1 \times 1/25 = 4\,\%$ — le minimum possible. Ce résultat est cohérent avec l'impact observé.

Contre-exemple : une compagnie aérienne exploitant une flotte mixte Linux/Windows, avec des agents de sécurité de fournisseurs différents, aurait obtenu $B \geq 3$ (diversification existante). Son score Y aurait été supérieur, et l'incident n'aurait touché qu'une fraction de ses systèmes. Avec $B \geq 3$ et $Y \geq 3$, le taux de maîtrise aurait atteint au moins $R = 1 \times 3/25 = 12\,\%$ — trois fois supérieur au cas Delta. La famille B capture exactement ce mécanisme.

OVHcloud Strasbourg, mars 2021 — la redondance absente

Pour les organisations hébergées sur SBG2 sans sauvegarde externalisée :

- $X = 1$: aucune alternative au service hébergé ;
- $Y = 1$: la famille A (📖 redondance) obtient un score de 1 (aucune sauvegarde hors site, aucun site de repli), et $Y = \min(\text{familles})$;
- Z variable, mais élevé pour les organisations ayant perdu des données définitivement.

Le modèle identifie correctement le point de défaillance : c'est l'absence de 📖 redondance (famille A) qui a rendu la destruction physique irréversible. Les organisations disposant de sauvegardes externalisées ($A \geq 3$) ont restauré leurs données en quelques jours.

NIRS Daejeon, septembre 2025 — la concentration et la lenteur

Pour les services gouvernementaux hébergés sur le site unique de Daejeon :

- $X = 1$: aucun basculement automatique, aucune alternative opérationnelle ;
- $Y = 1$: la famille A obtient un score de 1 (concentration sur un site unique), la famille D (📖 rapidité de rétablissement) obtient un score de 1 (plus de quatre semaines de rétablissement), et $Y = \min(\text{familles})$;
- $Z = 5$: services gouvernementaux critiques (services postaux, vérification d'identité, géolocalisation des appels d'urgence).

Le taux de maîtrise vaut $R = 4\,\%$. Deux familles défaillantes simultanément (A et D) confirment le principe du 📖 maillon faible : même si les familles B et C avaient été excellentes, le score Y resterait à 1.

Municipalité suédoise, 2021 — la substituabilité comme filet de sécurité

Holmström et Große documentent le cas d'une municipalité suédoise frappée par un rançongiciel (Holmström et Grosse 2025). Les systèmes numériques sont paralysés, mais la municipalité maintient ses services : elle avait conservé des procédures papier alternatives, connues des équipes mais non exercées en routine.

- $X = 4$: l'arbre de décision X produit ce score en trois réponses — le processus peut-il continuer sans le numérique ? Oui. À quel niveau de service ? Équivalent (S3). L'alternative est-elle pratiquée ? Connue et disponible, mais non exercée régulièrement (M1). D'où S3/M1 = 4 ;
- $Y = 1$: le rançongiciel a réussi, la 📖protection (famille C) et la 📖rapidité de rétablissement de reprise (famille D) étaient insuffisantes ;
- $Z = 4$: services publics avec obligations de continuité.

Le taux de maîtrise vaut $R = 4 \times 1/25 = 16\,\%$ — quatre fois supérieur au cas CrowdStrike, malgré une résilience technique tout aussi faible. La différence tient entièrement à la 📖substituabilité fonctionnelle : l'axe X a compensé la défaillance de l'axe Y. C'est exactement la logique du produit $X \times Y$: deux dimensions indépendantes, dont chacune peut atténuer les conséquences d'une faiblesse de l'autre.

Contre-exemple : sans les procédures papier conservées, la municipalité se serait trouvée dans la même situation que Delta Air Lines — $X = 1$, $Y = 1$, $R = 4\,\%$. L'écart entre les deux scénarios ($R = 16\,\%$ contre $R = 4\,\%$) tient à un seul axe : la substituabilité. Inversement, si la municipalité avait investi dans la résilience technique (familles C et D renforcées, $Y \geq 3$), le rançongiciel n'aurait pas paralysé ses systèmes et l'alternative papier n'aurait pas été nécessaire — $R = 4 \times 3/25 = 48\,\%$. Le modèle capture les deux chemins vers la robustesse : l'investissement numérique (axe Y) et le maintien d'alternatives fonctionnelles (axe X). La municipalité suédoise illustre le second ; les recommandations de la phase d'analyse devraient l'orienter vers le premier pour réduire sa fragilité structurelle.

Ce cas sert aussi de test de spécificité : les trois cas précédents montrent qu'IRON produit des scores bas quand l'organisation succombe (sensibilité), celui-ci montre qu'il produit un score plus élevé quand l'organisation résiste grâce à sa substituabilité (spécificité). Le modèle ne se contente pas de confirmer les échecs — il distingue les profils de robustesse. Ce cas illustre la thèse centrale d'IRON : la 📖robustesse d'une organisation ne dépend pas seulement de la résilience de ses services numériques, mais aussi de sa capacité à fonctionner sans eux.

7.3 Stratégie de validation progressive

La validation empirique complète d'IRON — corrélation entre les scores et les impacts réels d'incidents — nécessite des données longitudinales qui n'existent pas encore. Plutôt

que d'attendre une validation complète avant tout déploiement, une stratégie progressive permet de renforcer la crédibilité du modèle par étapes.

Phase 1 — Cas rétrospectifs

Appliquer IRON à 5–10 incidents documentés publiquement et vérifier que les scores produits sont cohérents avec l'impact observé. Les quatre cas de cette section en constituent une première illustration. Cette phase ne nécessite aucune coopération d'organisations : les informations sont publiques. Elle devrait inclure des cas symétriques — organisations ayant traversé un incident sans dommage majeur grâce à une bonne substituabilité ou résilience — pour tester la spécificité du modèle, pas seulement sa sensibilité. Elle établit la validité apparente du modèle.

Phase 2 — Pilotes volontaires

Évaluer 3 à 5 organisations volontaires, de tailles et de secteurs différents, pour tester l'opérationnalité de la méthode : durée d'évaluation, clarté des questions, reproductibilité des scores entre évaluateurs. Les volontaires bénéficient d'un diagnostic gratuit — incitation suffisante pour constituer un premier panel.

Cette phase inclut un test de reproductibilité inter-évaluateurs : pour au moins deux organisations, deux évaluateurs indépendants conduisent l'évaluation séparément, puis les scores sont comparés axe par axe et processus par processus. Les divergences identifient les questions ambiguës ou les points où la connaissance de l'organisation influence le résultat. Cette phase teste également la validité de construit : le score Y corrèle-t-il avec la maturité mesurée par d'autres référentiels (ISO 27001, NIST CSF) ? Le score Z est-il cohérent avec un BIA existant ? Ces tests de convergence établiraient que les axes mesurent bien ce qu'ils prétendent mesurer. La commensurabilité des échelles — comment traduire un niveau de maturité ISO 27001 ou un résultat de BIA en valeur comparable à un score IRON sur 1–5 — devra être résolue comme prérequis de ces tests.

Phase 3 — Suivi longitudinal

Suivre les organisations évaluées sur une période de 2 à 5 ans et observer si les incidents subis corrèlent avec les scores IRON : les processus à faible taux de maîtrise sont-ils effectivement ceux qui causent le plus de dommages lors d'une perturbation ? Cette phase est la plus exigeante mais la plus probante. Elle établirait la validité prédictive du modèle. Les critères de significativité statistique — corrélation minimale, taille de l'échantillon, nombre d'incidents nécessaires — devront être définis avant son lancement.

Chaque phase produit des résultats exploitables indépendamment des suivantes. Le modèle peut être déployé et amélioré itérativement sans attendre la validation complète —

c'est l'approche standard en recherche appliquée, où la rigueur structurelle précède la confirmation empirique.

8 Discussion et conclusion

8.1 Contributions

Cet article a présenté IRON, une méthode d'évaluation de la robustesse des organisations face au numérique. Ses contributions se résument en cinq points.

1. **Un croisement inédit.** À notre connaissance, IRON est le premier indice à croiser, au niveau du processus métier, la substituabilité numérique (X), la résilience des services numériques (Y) et la criticité métier (Z) en un score unique. Les référentiels et indices recensés (section 2) traitent ces dimensions séparément ; IRON les intègre dans une mesure transversale.

2. **Une universalité sans paramètre sectoriel.** Fondé sur le VSM de Beer pour la définition de l'organisation, sur le continuum de pérennité organisationnelle pour la mesure de l'impact, et sur le cadre 4R de Bruneau et al. pour la structuration des solutions, le modèle s'applique à toute organisation — entreprise, hôpital, collectivité, association — sans calibrage sectoriel. La spécificité de chaque organisation émerge des réponses, pas des paramètres (section 6).

3. **Un renversement épistémologique appliqué.** En appliquant à l'évaluation organisationnelle le principe établi par Loch et al. (Loch et al. 1992) — les conséquences d'une défaillance sont indépendantes de ses causes —, IRON contourne le problème de l'espace infini des menaces et rend le modèle opérable (section 4).

4. **Un coût d'évaluation maîtrisé.** La factorisation par service numérique et la priorisation par criticité permettent d'obtenir un score exploitable en évaluant une fraction des processus. Pour une PME de 10 processus, l'effort représente environ 20 questions par processus — une journée, pas un audit de plusieurs semaines.

5. **Une complémentarité avec l'existant.** IRON ne remplace aucun référentiel : il consomme leurs résultats. Une certification ISO 27001 se reflète dans un score Y plus élevé ; un BIA au sens de l'ISO 22301 alimente directement l'axe Z. Les investissements existants sont valorisés, pas dupliqués.

8.2 Choix méthodologiques et objections

Sept objections méthodologiques méritent une réponse explicite. Les trois premières portent sur la construction des scores, les quatre suivantes sur les cadres théoriques

mobilisés.

Multiplication d'échelles ordinales

Les échelles 1–5 des axes X et Y sont ordinales : la « distance » entre les niveaux n'est pas garantie égale. La théorie classique de la mesure interdit les opérations arithmétiques sur des données ordinales (Cox 2008). Le produit $X \times Y$ serait donc mathématiquement non fondé si les scores étaient de simples auto-évaluations de type Likert. Ce n'est pas le cas : les scores IRON sont construits par une grille à deux dimensions ($S \times M$) dont la progression reflète des ruptures qualitatives explicites (S0 → S1 = passage de « rien » à « quelque chose », S2 → S3 = passage de dégradé à équivalent ; M0 → M1 → M2 = progression de théorique à pratiqué). La grille est la même pour les deux axes, ce qui rend le produit sémantiquement fondé : il combine deux évaluations de même nature sur une échelle commune. L'objection reste pertinente pour l'axe Z, dont la construction (somme convertie de trois dimensions 0/1/4/10) est différente ; mais Z n'entre pas dans un produit — il pondère une moyenne, opération moins exigeante sur le plan de la théorie de la mesure.

Sensibilité aux choix d'agrégation

La littérature sur les indices composites montre que les choix de normalisation, de pondération et d'agrégation peuvent produire des résultats significativement différents (OECD/JRC 2008). Le choix du minimum pour agréger les familles A/B/C/D dans l'axe Y, du produit $X \times Y$ plutôt qu'une somme ou une moyenne harmonique, et de la moyenne pondérée par Z sont des décisions qui influencent le score final. Chacune est justifiée sémantiquement : le minimum reflète le principe du maillon faible (un service sans sauvegarde est fragile, quel que soit son niveau de protection) ; le produit traduit l'indépendance et la complémentarité des axes X et Y (chacun peut compenser partiellement l'autre) ; la pondération par Z concentre l'attention sur les processus critiques. Mais la justification sémantique ne dispense pas de la vérification empirique : une analyse de sensibilité formelle — que se passe-t-il si le minimum est remplacé par une moyenne harmonique ? si le produit est remplacé par une somme pondérée ? les classements de processus changent-ils substantiellement ? — relève de la phase 2 de la validation (section 7). En l'absence de cette analyse, la stabilité des classements de processus selon les choix d'agrégation reste une limite actuelle du modèle. Cette analyse fait partie des tests prévus sur les pilotes volontaires.

Biais d'auto-évaluation

Toute méthode fondée sur l'auto-évaluation est exposée aux biais de désirabilité sociale et de surestimation des compétences (Podsakoff et al. 2003). Les organisations

les moins résilientes sont précisément celles qui risquent de surévaluer leurs capacités. IRON atténue ce risque par trois mécanismes : le critère M distingue structurellement ce qui est déclaré (M0) de ce qui est testé (M1) ou pratiqué (M2) ; les arbres de décision posent des questions sur des faits observables, pas sur des perceptions ; et le renversement épistémologique force l'évaluateur à raisonner sur des conséquences concrètes plutôt que sur une « culture de résilience » auto-déclarée. Ces mécanismes ne suppriment pas le biais — seule une évaluation externe le ferait — mais ils le réduisent structurellement. Le test de reproductibilité inter-évaluateurs prévu en phase 2 de la validation (section 7) permettra d'en mesurer l'ampleur résiduelle.

Évaluation par les conséquences, pas par les menaces

IRON évalue les conséquences d'une défaillance, pas ses causes. Cox (Cox 2008) argue qu'une évaluation ignorant les menaces ne peut pas guider l'allocation des ressources défensives. L'objection est pertinente dans un cadre de gestion des risques, mais IRON ne prétend pas être un outil de gestion des risques : c'est un indice de robustesse. Il mesure la capacité d'une organisation à résister aux perturbations numériques, quelle que soit leur origine. L'analyse des menaces relève d'autres référentiels (ISO 27005, EBIOS RM) dont les résultats alimentent l'axe Y — les mesures de protection (famille C) et de détection/réponse (famille D) sont précisément les réponses aux menaces identifiées. IRON consomme les résultats de l'analyse des menaces sans la dupliquer.

Ce renversement est parfois associé au passage de Safety-I à Safety-II formalisé par Hollnagel (Hollnagel 2014). Leveson critique cette dichotomie, arguant que l'ingénierie de la sécurité n'a jamais été limitée à l'approche causale que Hollnagel attribue à Safety-I (Leveson 2020). La critique est pertinente en ingénierie des systèmes ; elle ne touche pas IRON, dont le renversement épistémologique s'ancre dans Loch et al. (Loch et al. 1992), pas dans Safety-II. L'observation que les conséquences d'une défaillance sont indépendantes de ses causes précède Safety-II de vingt ans et ne dépend pas de la validité de cette dichotomie.

Transposition du cadre 4R au domaine numérique

Le cadre 4R de Bruneau et al. (Bruneau et al. 2003) a été conçu pour la résilience sismique des communautés. Cette approche d'ingénierie physique a pour limite structurelle d'évaluer la robustesse des configurations existantes, pas la capacité d'un système à se reconfigurer sous pression. La critique porte sur la quatrième dimension du cadre original — la *Resourcefulness*, la capacité à mobiliser des ressources nouvelles. IRON redistribue cette dimension implicitement dans les quatre familles (section 4), ce qui constitue effectivement une perte : la capacité adaptative d'une organisation — son aptitude à inventer des solutions inédites en situation de crise — n'est pas mesurée par le modèle. C'est une limite

assumée : IRON mesure la robustesse (capacité à résister avec les moyens en place), pas l'adaptabilité (capacité à improviser). Cette distinction est mobilisée par Aven (Aven 2019) ; IRON se positionne du côté de la robustesse.

Usage du Viable System Model

Le VSM de Beer est critiqué pour offrir une image simplifiée de l'organisation, fondée sur une analogie organique qui peut induire des diagnostics erronés (Jackson 1988). IRON n'utilise pas le VSM comme outil de diagnostic organisationnel : il en emprunte uniquement la *définition* de l'organisation. Les cinq sous-systèmes de Beer (opérations, coordination, contrôle, intelligence, politique) servent à justifier que tout 🕮processus métier, dans toute organisation, peut être identifié et évalué — c'est une condition d'universalité, pas un modèle de fonctionnement. Les critiques portant sur les limites du VSM comme outil de diagnostic — sa difficulté à capturer les dynamiques de pouvoir, les dimensions culturelles ou la viabilité financière — sont légitimes mais hors du périmètre de l'usage qu'IRON en fait. En revanche, la difficulté pratique à délimiter les cinq sous-systèmes dans une organisation réelle peut produire des inventaires de processus variables selon l'évaluateur ; cette variabilité est testée par le protocole de reproductibilité inter-évaluateurs prévu en phase 2 (section 7).

La triade CIA comme grille de conséquences

La triade 🕮CIA (Confidentialité, Intégrité, Disponibilité) est critiquée en sécurité de l'information pour son incomplétude : elle ne couvre pas explicitement l'authentification, la non-répudiation ni la *privacy*. IRON n'utilise pas la triade CIA comme cadre de sécurité exhaustif : il l'utilise comme grille de structuration des *conséquences observables* d'une défaillance numérique. Quand un service tombe, trois choses se produisent : il n'est plus accessible (Disponibilité), ses données peuvent être corrompues (Intégrité), ses données peuvent être exposées (Confidentialité). Les dimensions jugées manquantes — authentification, non-répudiation, accountability — sont des *mécanismes* qui se manifestent comme des atteintes à C, I ou D : un défaut d'authentification est une atteinte à la confidentialité (accès non autorisé) ou à l'intégrité (modification non autorisée). La triade CIA est donc un choix de modélisation des conséquences, historiquement situé et largement adopté, pas une affirmation sur la complétude du cadre de sécurité dans toutes ses dimensions.

8.3 Limites et travaux futurs

Trois limites appellent des travaux complémentaires.

Validation empirique

La validité structurelle et la cohérence rétrospective sont établies (section 7), mais la validation prédictive — les scores IRON corrèlent-ils avec les impacts réels d'incidents futurs ? — reste à démontrer. La stratégie progressive proposée (cas rétrospectifs, pilotes volontaires, suivi longitudinal) trace un chemin réaliste, mais les phases 2 et 3 nécessitent du temps et des partenariats.

Labels d'interprétation

Le score IRON est un pourcentage entre 4 % et 100 %, mais le modèle ne définit pas de seuils d'interprétation validés : à partir de quel score une organisation est-elle « suffisamment robuste » ? La réponse dépend du contexte — un hôpital et une association n'ont pas les mêmes exigences. Définir des seuils définitifs supposerait des données empiriques qui n'existent pas encore. En l'état, IRON est un outil de progression : c'est l'évolution du score dans le temps qui compte, plus que sa valeur absolue.

À titre indicatif et en attendant la validation empirique, quatre zones d'interprétation peuvent guider la lecture :

Table 8 : Grille provisoire d'interprétation du score IRON.

Score IRON	**Zone**	**Interprétation indicative**
4–20 %	Fragilité critique	La majorité des processus critiques sont exposés ; une perturbation numérique met en cause la pérennité.
20–40 %	Fragilité significative	Des leviers existent mais restent insuffisamment activés ; les processus les plus critiques manquent de maîtrise.
40–70 %	Robustesse en progression	Les processus critiques commencent à être maîtrisés ; l'effort doit se poursuivre sur les services à Y faible.
70–100 %	Robustesse avancée	Maîtrise étendue ; l'enjeu est le maintien dans le temps et la vigilance sur les évolutions d'architecture.

Ces zones sont **provisoires** : elles seront affinées par les retours des pilotes volontaires (phase 2 de la validation, section 7). Elles ne doivent pas être utilisées pour des décisions binaires (certification, éligibilité contractuelle, tarification assurantielle) ; ce type d'usage supposerait des seuils validés empiriquement, qui constituent un prolongement nécessaire.

Risque systémique

IRON mesure la robustesse d'une organisation individuelle. Il ne capture pas le risque systémique : la dépendance de milliers d'organisations à un même fournisseur, un même

système d'exploitation ou un même agent de sécurité. L'incident CrowdStrike (section 1) illustre cette dimension : chaque organisation touchée avait un problème de diversification (famille B), mais la concentration du risque à l'échelle mondiale relève d'une logique collective que l'indice d'une organisation seule ne peut pas refléter. Au niveau individuel, IRON détecte bien le problème : chaque organisation dépendante obtient $B = 1$. Ce que l'indice ne peut pas mesurer, c'est l'impossibilité d'entraide sectorielle quand toutes les organisations partagent simultanément la même fragilité. Cette dimension appelle des travaux à un autre niveau d'analyse — distinct de la topologie de la robustesse interne à une organisation, traitée ci-après.

8.4 Topologie de la robustesse organisationnelle

IRON évalue chaque processus indépendamment. Cette propriété garantit la simplicité et la reproductibilité du modèle, mais elle soulève une question légitime : que se passe-t-il lorsque plusieurs processus partagent une même ressource de substitution ?

Certaines dépendances partagées sont déjà captées par le modèle. Si tous les services numériques d'une organisation reposent sur un fournisseur cloud unique, chacun obtient $B = 1$ (diversification minimale), donc $Y = 1$ par le principe du minimum. Le score IRON reflète correctement la fragilité systémique, service par service, sans mécanisme supplémentaire.

La situation est structurellement différente pour les alternatives non numériques évaluées par l'axe X. Qu'il s'agisse de personnes, de procédures papier, d'équipements mécaniques ou de prestataires externes, la capacité de substitution est évaluée processus par processus — mais la disponibilité *simultanée* d'une même alternative pour plusieurs processus n'est inscrite nulle part dans les données IRON. Prenons l'exemple d'une équipe capable de basculer en mode manuel : son score X est identique que cette équipe serve un seul processus ou dix. Ce n'est pas un oubli de la formule : c'est une information qui n'existe qu'au niveau du contexte organisationnel global, pas au niveau du processus.

Cette asymétrie révèle deux stratégies de robustesse distinctes. Une organisation dont les scores Y dominent pratique une *robustesse distribuée* : chaque service numérique embarque sa propre résilience (sauvegardes, redondance, diversification), indépendamment des autres. Une organisation dont les scores X dominent pratique potentiellement une *robustesse centralisée* qui devient fragile sous charge simultanée lorsque les alternatives reposent sur les mêmes ressources mutualisées. À score IRON égal, ces deux profils n'offrent pas la même garantie en situation de crise généralisée.

IRON fournit les données nécessaires pour poser cette question : un profil X-dominant sur les processus critiques est un signal que l'évaluateur doit interpréter avec sa connaissance du contexte opérationnel. Mais le modèle ne répond pas seul — l'exercice de crise multi-scénarios reste indispensable pour évaluer la contention des alternatives partagées. La

topologie de la robustesse organisationnelle — cartographie de la structure de la robustesse (distribuée, centralisée, mixte) et de ses points de fragilité sous charge — constitue un programme de recherche complémentaire sur l'interprétation des données, et n'est pas en soi une lacune du score. La démarche opérationnelle (Peccini 2026) intégrera une étape d'identification des concentrations d'alternatives partagées lors de la phase d'analyse des résultats.

8.5 Perspectives

Trois prolongements sont envisagés.

Le premier est un **guide opérationnel** (en cours de rédaction), destiné aux praticiens : de l'inventaire des processus métier à la construction d'une stratégie de robustesse, en passant par les questionnaires détaillés pour chaque axe. Ce guide est le complément nécessaire du présent article, qui pose le modèle sans détailler sa mise en œuvre. Le présent article, le guide opérationnel et le livre blanc (Peccini 2026) forment un ensemble cohérent : le livre blanc pose le contexte stratégique et la problématique, l'article formalise le modèle, le guide décrit la mise en œuvre. Les éléments fondateurs mobilisés par l'article (substituabilité, pérennité, renversement épistémologique) sont développés dans le livre blanc, dont la seconde version intégrera le guide opérationnel et référencera le présent article. Les trois documents sont conçus pour être lus indépendamment, mais se complètent.

Le deuxième est une **synthèse décideur**, condensant les enjeux et les résultats d'IRON en un format accessible aux dirigeants qui ne liront ni l'article ni le guide. La compréhension des enjeux par les décideurs est un prérequis au déploiement : sans elle, les ressources nécessaires à l'évaluation ne seront pas mobilisées.

Le troisième est une **plateforme d'évaluation** permettant aux organisations de conduire leur auto-évaluation IRON de manière guidée. Cette plateforme constituerait elle-même un cas d'application du modèle : en tant que service numérique, elle devrait obtenir un score Y élevé — ce qui imposerait de résoudre le paradoxe de l'outil numérique utilisé pour mesurer le risque numérique. Le modèle est indépendant de son support : la formule peut être résolue sur papier ou sur un tableur. Mais un outil dédié faciliterait le suivi de progression et la factorisation des évaluations par service numérique.

Remerciements

L'auteur remercie [Prénom Nom] pour sa relecture attentive d'une version antérieure de cet article et ses remarques sur les choix de modélisation, la cartographie des dépendances et le positionnement du modèle.

Glossaire

criticité métier Mesure de l'impact qu'aurait l'arrêt d'un processus métier sur la pérennité de l'organisation, évaluée selon trois dimensions : opérationnelle, réglementaire et réputationnelle. 6, 10, 15, 19, 29, 36, 41

diversification Famille de solutions (B) consistant à utiliser des composants de nature ou d'origine différente pour éviter les défaillances de mode commun. 13, 14, 17, 19, 22, 42

maillon faible Principe d'agrégation selon lequel la fragilité globale d'un service numérique est déterminée par son composant le moins résilient. 18, 22, 25, 42

maturité opérationnelle Degré de préparation effective d'une alternative ou d'une solution de résilience : théorique (M0), testée ponctuellement (M1) ou pratiquée régulièrement (M2). 10, 18, 20, 24, 38

processus métier Unité d'analyse d'IRON : ensemble d'activités concourant à un résultat identifiable pour l'organisation et utilisant au moins un service numérique. 4, 8, 10, 14, 15, 18, 19, 22, 26, 29, 34, 36, 37, 39, 48

protection Famille de solutions (C) consistant à mettre en place des mesures préventives réduisant la probabilité ou l'impact des perturbations. 14, 17, 22, 37, 43

pérennité organisationnelle Capacité d'une organisation à maintenir durablement sa mission et ses activités. Continuum allant de la survie à la longévité. 6, 8, 15, 26, 33, 34, 41

rapidité de rétablissement Famille de solutions (D) consistant à minimiser le temps nécessaire pour retrouver un fonctionnement acceptable après une perturbation. 14, 17, 22, 42, 43

redondance Famille de solutions (A) consistant à dupliquer les composants critiques pour assurer la continuité en cas de défaillance d'un élément. 13, 14, 17, 19, 22, 38, 42

risque systémique exogène Risque lié aux dépendances transitives entre organisations (ex. : fournisseur commun à l'ensemble d'un secteur), non évaluable au niveau d'une organisation isolée et donc hors du périmètre d'IRON. 25

robustesse Capacité d'une organisation à maintenir ses fonctions essentielles de manière stable et viable face aux défaillances du numérique, en créant les conditions pour ne pas tomber. Nature préventive et organisationnelle : propriété de l'organisation, pas du système technique. 9, 12, 13, 14, 39, 43

résilience Capacité d'un système numérique à résister aux perturbations et à revenir à un état fonctionnel après l'incident. Nature réactive et technique : propriété du système, pas de l'organisation. 5, 6, 8, 9, 13, 14, 19, 21, 40

service numérique Ensemble cohérent de composants techniques (applications, infrastructures, données) fournissant une capacité identifiable à un ou plusieurs processus métier. 5, 7, 8, 10, 13, 14, 16, 17, 18, 19, 21, 34, 36, 38, 39

substituabilité fonctionnelle Capacité d'un processus métier à continuer de fonctionner en l'absence du service numérique qui le supporte, via une alternative manuelle ou technique. 5, 6, 8, 9, 10, 19, 34, 40, 43

Références

Aven, Terje (2019). « The Call for a Shift from Risk to Resilience : What Does It Mean ? » In : *Risk Analysis* 39.6, p. 1196-1203. DOI : 10.1111/risa.13247. URL : https://doi.org/10.1111/risa.13247.

BBC News (19 juill. 2024). *GPs, airports and banks in UK hit by IT outage*. URL : https://www.bbc.co.uk/news/articles/cp0823lz4j7o.

Beer, Stafford (1984). « The Viable System Model : Its Provenance, Development, Methodology and Pathology ». In : *Journal of the Operational Research Society* 35.1, p. 7-25. DOI : 10.1057/jors.1984.2. URL : https://doi.org/10.1057/jors.1984.2.

Bhuwalka, Karan et al. (2022). « Quantifying the drivers of long-term prices in materials supply chains ». In : *Journal of Industrial Ecology* 27.1. DOI : 10.1111/jiec.13355. URL : https://doi.org/10.1111/jiec.13355.

Bruneau, Michel et al. (2003). « A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities ». In : *Earthquake Spectra* 19.4, p. 733-752. DOI : 10.1193/1.1623497. URL : https://doi.org/10.1193/1.1623497.

Cook, Thomas D. et Donald T. Campbell (1979). *Quasi-Experimentation : Design and Analysis Issues for Field Settings*. Boston : Houghton Mifflin.

Cox, Louis Anthony Jr. (2008). « What's Wrong with Risk Matrices ? » In : *Risk Analysis* 28.2, p. 497-512. DOI : 10.1111/j.1539-6924.2008.01030.x. URL : https://doi.org/10.1111/j.1539-6924.2008.01030.x.

CrowdStrike (2024). *Channel File 291 Incident : Root Cause Analysis*. Rapp. tech. URL : https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf.

English, Lar et Akilu Yunusa-Kaltungo (2022). « A practical application of methodologies to determine asset criticality and work order prioritization ». In : *Engineering Reports* 4.12. DOI : 10.1002/eng2.12555. URL : https://doi.org/10.1002/eng2.12555.

Greenberg, Andy (2019). *Sandworm : A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York : Doubleday.

Hamant, Olivier (2023). *Antidote au culte de la performance : la robustesse du vivant*. Paris : Gallimard.

Hassel, Henrik et Alexander Cedergren (2024). « A framework for business continuity management in a multiactor context ». In : *Journal of Contingencies and Crisis Management* 32.2. DOI : 10.1111/1468-5973.12573. URL : https://doi.org/10.1111/1468-5973.12573.

Hollnagel, Erik (2014). *Safety-I and Safety-II : The Past and Future of Safety Management*. Farnham : Ashgate Publishing.

Holmström, Anton et Christine Grosse (2025). « Not All Heroes Wear Capes : Cyber Resilience of the Social Administration at a Swedish Municipality ». In : *Risk, Hazards & Crisis in Public Policy* 16.3. DOI : 10.1002/rhc3.70024. URL : https://doi.org/10.1002/rhc3.70024.

Hosseini, Seyedmohsen, Kash Barker et José Emmanuel Ramirez-Marquez (2016). « A review of definitions and measures of system resilience ». In : *Reliability Engineering & System Safety* 145, p. 47-61. DOI : 10.1016/j.ress.2015.08.006. URL : https://doi.org/10.1016/j.ress.2015.08.006.

International Energy Agency (2025). *Global Critical Minerals Outlook 2025*. Rapp. tech. Paris : IEA. URL : https://www.iea.org/reports/global-critical-minerals-outlook-2025.

Jackson, Michael C. (1988). « An Appreciation of Stafford Beer's 'Viable System' Viewpoint on Managerial Practice ». In : *Journal of Management Studies* 25.6, p. 557-573. DOI : 10.1111/j.1467-6486.1988.tb00047.x. URL : https://doi.org/10.1111/j.1467-6486.1988.tb00047.x.

Kosajan, Vorada, Zongguo Wen et Xiyuan Wang (2025). « Criticality assessment and management policy analysis of rare earth elements ». In : *Journal of Industrial Ecology* 29.1, p. 344-357. DOI : 10.1111/jiec.13601. URL : https://doi.org/10.1111/jiec.13601.

Leveson, Nancy G. (2020). *Safety III : A Systems Approach to Safety and Resilience*. Rapp. tech. MIT Technical Report. MIT Engineering Systems Lab. URL : http://sunnyday.mit.edu/safety-3.pdf.

Lines, Delta Air (10 oct. 2024). *Delta Air Lines Announces September Quarter 2024 Financial Results*. URL : https://ir.delta.com/news/news-details/2024/

Delta-Air-Lines-Announces-September-Quarter-2024-Financial-Results/default.aspx.

Linkov, Igor et Alexander Kott (2019). « Fundamental Concepts of Cyber Resilience : Introduction and Overview ». In : *Cyber Resilience of Systems and Networks*. Springer, p. 1-25. doi : 10.1007/978-3-319-77492-3_1. url : https://doi.org/10.1007/978-3-319-77492-3_1.

Loch, Karen D., Houston H. Carr et Merrill E. Warkentin (1992). « Threats to Information Systems : Today's Reality, Yesterday's Understanding ». In : *MIS Quarterly* 16.2, p. 173-186. doi : 10.2307/249574. url : https://doi.org/10.2307/249574.

Marrewijk, Marcel van et Marco Werre (2003). « Multiple Levels of Corporate Sustainability ». In : *Journal of Business Ethics* 44.2-3, p. 107-119. doi : 10.1023/A:1023383229086. url : https://doi.org/10.1023/A:1023383229086.

Mathews, Jessica (19 juill. 2024). *Doctors revert to pen and paper after CrowdStrike's outage hits hospitals*. url : https://fortune.com/2024/07/19/crowdstrike-outage-glitch-hospitals-healthcare-doctors-computer-systems/.

Mignon, Sophie (2009). « La pérennité organisationnelle. Un cadre d'analyse : introduction ». In : *Revue française de gestion* 35.192, p. 73-89. doi : 10.3166/rfg.192.75-89. url : https://shs.cairn.info/revue-francaise-de-gestion-2009-2-page-73?lang=fr.

Ministry of the Interior and Safety, Republic of Korea (2025). *Incendie du datacenter gouvernemental NIRS de Daejeon*. Incendie du 26 septembre 2025 détruisant 858 To de données et paralysant 647 services numériques gouvernementaux. url : https://www.koreaherald.com/article/10585116.

OECD/JRC (2008). *Handbook on Constructing Composite Indicators : Methodology and User Guide*. Paris : OECD Publishing. doi : 10.1787/9789264043466-en. url : https://doi.org/10.1787/9789264043466-en.

OVHcloud (2021). *Incendie du datacenter de Strasbourg (SBG2)*. Incendie du 10 mars 2021 détruisant le datacenter SBG2 et affectant 3,6 millions de sites web. url : https://next.ink/5148/ovhcloud-feu-se-declare-a-strasbourg-partie-site-detruit/.

Parametrix (24 juill. 2024). *CrowdStrike's Impact on the Fortune 500*. url : https://www.parametrixinsurance.com/reports-white-papers/crowdstrikes-impact-on-the-fortune-500.

Peccini, Stéphan (2025). *Base documentaire de l'application FabNum*. Licence CC-BY-NC-ND-4.0. url : https://fabnum-git.peccini.fr/FabNum/Fiches/.

— (2026). *Voyage vers la robustesse — Livre blanc. Construire une stratégie d'organisation pour pallier les risques induits sur le numérique face aux enjeux climatiques,*

géopolitiques, sociaux et technologiques. Rapp. tech. Infogreen Factory. URL : https://framagit.org/biens-communs/publications/voyage-vers-la-robustesse.

PODSAKOFF, Philip M. et al. (2003). « Common method biases in behavioral research : A critical review of the literature and recommended remedies ». In : *Journal of Applied Psychology* 88.5, p. 879-903. DOI : 10.1037/0021-9010.88.5.879. URL : https://doi.org/10.1037/0021-9010.88.5.879.

SANTILLÁN-SALDIVAR, Jair et al. (2021). « Design of an endpoint indicator for mineral resource supply risks in life cycle sustainability assessment : The case of Li-ion batteries ». In : *Journal of Industrial Ecology* 25.4, p. 1051-1062. DOI : 10.1111/jiec.13094. URL : https://doi.org/10.1111/jiec.13094.

SBS NEWS (19 juill. 2024). *CrowdStrike IT outage hits airports, banks, supermarkets as PM says Triple-0 unaffected*. URL : https://www.sbs.com.au/news/article/crowdstrike-it-outage-hits-airports-banks-supermarkets-as-pm-says-triple-0-unaffected/ezge7qp0g.

TALEB, Nassim Nicholas (2007). *The Black Swan : The Impact of the Highly Improbable*. New York : Random House.