PILOTER SA TRANSFORMATION NUMERIQUE AVEC LA METHODE MCRA (MACROCARTOGRAPHIE DES RISQUES PAR LES AUDITS)

PILOTING DIGITAL TRANSFORMATION USING THE "MACRO-MAPPING OF RISKS BY AUDITS" METHOD

Vincent Desroches
Agence nationale de la sécurité des systèmes d'information (ANSSI), Paris, France
Vincent.desroches@ssi.gouv.fr

Sébastien Delmotte
MAD-Environnement,
23, rue de la République
31560 Nailloux, France
delmotte@mad-environnement.com

Résumé *— Cette communication présente l'apport de la méthode MCRA (macrocartographie des risques par les audits) pour piloter un projet de transformation numérique et gérer les risques de l'ensemble de ses leviers stratégiques, organisationnels, humains, métiers, technologiques et environnementaux.*

Abstract *— This paper presents the contribution of the MCRA method (macro-mapping of risks by audits) to pilot a digital transformation project and manage the risks of all of its strategic, organizational, human, business, technological and environmental levers.*

Mots clés *— Transformation numérique ou digitale, Management des risques, méthode MCRA.*

Key words *— Digital transformation, Global risk management, MCRA method.*

I. INTRODUCTION

A. L'entreprise traditionnelle bousculée par le numérique

La transformation numérique ou digitale, terme aujourd'hui largement utilisé pour désigner le passage des entreprises aux technologies de l'information, est difficile à définir de manière simple tant sa nature est multidimensionnelle. Elle ne peut pas se résumer à la seule dimension technique par laquelle elle est souvent abordée. **La transformation numérique est politique, culturelle, sociale, économique…** Le numérique est une culture, et la révolution numérique est une rupture dans la manière dont nos sociétés produisent, utilisent et partagent les connaissances. Elle se caractérise par l'augmentation du pouvoir des individus, l'apparition de formes collectives nouvelles et originales (ex : communautés numériques, organisations du travail fondées sur la participation à des projets *open source* comme Github), et par la redistribution à l'échelle mondiale du pouvoir et de la valeur vers les acteurs qui contrôlent les plateformes de mise en réseau [1].

Elle trouve ses origines dans l'invention de l'informatique et de l'ordinateur, lesquels étaient initialement utilisés comme un instrument de calcul. La conception de l'informatique distribuée en réseau par les universitaires entre les années 1960 et 1990 a été guidée par les idées de la contre-culture des années 1970 prônant la liberté et la coopération, parallèlement à l'introduction du concept d'homme augmenté prôné par Doug Engelbart dans les années 1960 [2]. Mais Cardon [1] rappelle également que la naissance de l'informatique est inséparable de la stratégie de l'armée américaine qui financera, au travers l'ARPA devenue DARPA, le développement d'internet et inscrivant ainsi dans son ADN le contrôle. **Ainsi, la culture numérique actuelle est-elle née de la dualité entre liberté et contrôle**, mouvement libertaire et organisation militaire.

Cette tension se retrouve également dans l'organisation de l'entreprise dans le contexte actuel de la transformation numérique. Babinet [3] rappelle que l'organisation hiérarchisée de l'entreprise traditionnelle issue de la révolution industrielle trouve son origine dans le modèle militaire, le seul connu au début du XXème siècle comme permettant de gérer les ressources humaines, techniques et financières nécessaires pour atteindre les objectifs stratégiques décidés au sommet de l'organisation. L'entreprise numérique, à l'image des start-ups de la *Silicon Valley*, se veut quant à elle bâtie sur un modèle d'organisation horizontale, peu hiérarchisée et dont le centre de gravité est constitué d'individus hors-normes fortement impliqués dans des communautés où le savoir n'est plus centralisé au sein de petits groupes de spécialistes.

Le modèle économique de l'entreprise numérique est caractérisé par le « gratuit » dont les revenus majoritaires sont publicitaires, une offre globale et pléthorique, la désintermédiation, l'automatisation, la dématérialisation, des coûts de transaction réduits induisant une forte tension sur les prix proposés par les plateformes et une influence très forte des consommateurs sur l'image et par conséquent sur les orientations stratégiques de l'entreprise. **La question de**

la cinétique de cette mutation est importante : si l'entrée de l'informatique chez les particuliers et la mise en place d'internet s'est étalée sur plusieurs dizaines d'année, la dominance de l'économie numérique initiée dans les années 2000 s'est mise en place en l'espace d'une décennie : alors qu'en 2006, seule Microsoft faisait partie du top10 des capitalisations boursières, perdue au milieu des géants pétroliers et des mastodontes financiers, en 2016, 5 entreprises du numérique occupaient le classement dont 3 en tête. Le début des années 2010 a connu l'avènement des américains GAFA (Google, Apple, Facebook, Amazon) suivi par les NATU (Netflix, Air BNB, Tesla et Uber) et plus récemment encore de la vague chinoise des BATX (Baidu, Alibaba, Tencent et Xiaomi). L'offre numérique initiale ne propose pas seulement de nouveaux services, elle est venue directement concurrencer l'offre traditionnelle, comme c'est le cas pour les taxis Uber. On assiste ainsi à un déplacement rapide des centres d'attraction de la valeur et de nouveaux monopoles viennent remplacer les anciens en concentrant souvent encore plus de pouvoir.

Devant le déferlement de cette vague, **les entreprises traditionnelles n'ont d'autre choix que de devoir s'adapter très rapidement** (en quelques années) à cette nouvelle économie et à la nouvelle culture qui la supporte. C'est en leur sein qu'on retrouve la tension originelle du numérique, entre organisation hiérarchisée fondée sur le contrôle, et modèle collaboratif horizontal et distribué. **Les facteurs humains et organisationnels sont au cœur de cette transformation numérique** : dans la structure de l'organisation, les relations de pouvoir, le collectif et la culture d'entreprise, dans les comportements et les savoirs individuels et dans la conduite du changement.

B. Les clés de succès pour réussir une transformation numérique

L'entreprise traditionnelle est donc face à des choix de transformation associés à des opportunités fantastiques, mais aussi à des conséquences potentiellement désastreuses pour elle. Concrètement, elle doit définir une stratégie de transformation à court, moyen et long terme et accompagner sa mise en œuvre. C'est à cette fin que la fonction de **CTO (*Chief Transformation Officer*) / CDO (*Chief Digital Officer*)** a récemment vu le jour. C'est une fonction clé de l'organisation et de la réalisation de la transformation numérique mais elle ne doit pas porter à elle seule la responsabilité de son succès ou son échec [11].

Babinet [3] identifie cinq phases pour réussir la transformation numérique : arrêter un plan à long terme, créer un tableau de bord de la transformation digitale, organiser, former, détecter les talents. Fayon et al. [5] préconisent quant à eux d'agir sur 6 leviers de transformation associés à des indicateurs de suivi de maturité numérique : la stratégie, l'organisation, le personnel, l'offre, la technologie et innovation, l'environnement. Pour sa part, le Cigref (Club informatique des grandes entreprises françaises) propose une démarche de transformation associée à 7 critères [6] : la vision, l'appropriation, les technologies, les données, le pilotage, les méthodes et la transformation du métier. Ces différentes propositions se rejoignent sur les points fondamentaux, notamment : que **l'impulsion doit venir du top-management** qui doit définir **une stratégie, des objectifs et un cadre de gouvernance ;** qu'un **diagnostic du niveau de maturité** au regard des objectifs doit être réalisé à intervalle régulier afin de s'assurer notamment que l'ensemble des personnels adhère au projet de transformation et suit le mouvement. Chaintreuil [12] insiste pour sa part sur le **rôle central de la direction des ressources humaines** (DRH) comme courroie de transmission entre le comité exécutif de l'entreprise et le management intermédiaire, lui-même lien essentiel entre décisions stratégiques et opérationnelles. La DRH doit fournir à l'entreprise les conditions du succès de la transformation numérique : recrutement des bons profils, formations au numérique, création d'un cadre de travail collaboratif et agile, simplification ou réinvention des procédures de management et d'évaluation adaptées à l'entrée dans le monde du travail des générations hyperconnectées… Un tel management RH favorise l'appropriation de la culture numérique et est vecteur de la promotion de la marque « employeur » essentielle aujourd'hui à l'image.

Cependant, ces démarches de transformation ne proposent pas explicitement d'approche et d'outil formalisés pour analyser et gérer les risques associés à la transformation numérique. En effet, le modèle de *business* numérique n'est pas dénué de risques et reste fragile [4] : faible taux de réussite de la monétarisation des start-up, concurrence extrême pour prendre les positions dominantes, concurrence des professionnels par les particuliers, enjeux réglementaires, fiscaux, éthiques, cyber-sécuritaires… Sans oublier les enjeux technologiques : l'explosion de la quantité de **données** recueillies grâce aux réseaux et bientôt aux objets connectés concomitante à l'augmentation régulière de la puissance de calculs des microprocesseurs est à l'origine du « big data », qui associe stockage et exploitation à grande échelle des données à l'aide d'algorithmes puissants d'analyse et d'apprentissage regroupés sous le terme générique d' « IA ». D'autre part, le monde numérique est bâti sur des technologies avant tout physiques (*hardware*) dans un monde physique également source de dangers et de menaces (disponibilité des ressources primaires, événements dangereux naturels, sanitaires, sociaux, contrôle des infrastructures et équipements distribués géographiquement…). De par la nature multidimensionnelle d'un projet de transformation numérique et les incertitudes et « inconnaissances » relatives aux environnements dans lesquels il se déroule, **il semble nécessaire de fonder son pilotage par un management global des risques**, qui couvre l'ensemble des phases de transformation numérique, elle-même s'inscrivant dans la stratégie globale de l'entreprise. La gestion des **risques positifs**, associés aux opportunités et aux gains, est un préalable à la construction de la stratégie de transformation car elle en fournit en partie les raisons. La gestion des **risques négatifs**, associés aux dangers et menaces, est quant à elle un facteur clé de succès du processus de transformation en garantissant qu'il se déroule dans le domaine de risque acceptable au regard des objectifs et exigences de l'activité, mais aussi de l'appétence au risque. Une approche par les risques accroit également le **niveau de confiance et d'adhésion** dans les orientations prises et leurs mises en œuvre.

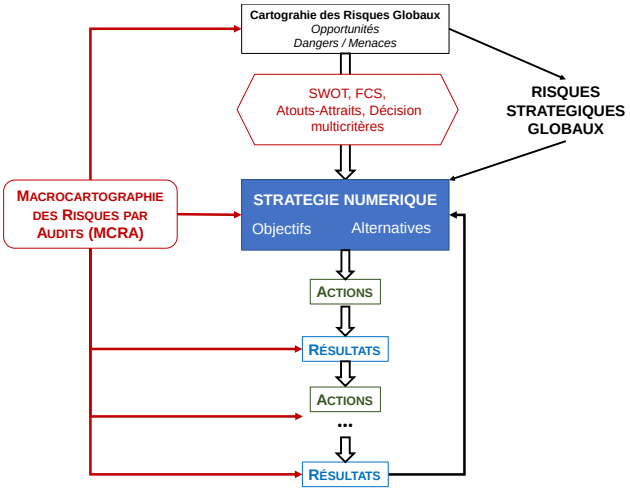

Fig. 1. Démarche globale de transformation numérique fondée sur l'approche par les risques

C. La démarche MCRA pour piloter sa transformation numérique

La macrocartographie des risques par audit (MCRA) est une méthode particulièrement bien adaptée à cette problématique. Développée dans les années 2000 au CNES (Centre national d'études spatiales), afin de visualiser un instantané des risques perçus dans une grande organisation spatialement distribuée, elle est fondée sur le recueil de la **perception des risques impactant les activités** d'une organisation, pour ensuite par regroupements successifs et application d'une fonction de transfert, évaluer et cartographier les risques au regard de l'échelle d'acceptabilité de la gouvernance [7,8,9] (Fig. 2). Pour ce faire, les responsables métier évaluent les risques impactant leur propre activité **sur la base d'un plan d'audits** qui repose sur la description des chaînes de valeur d'entreprise au travers à la fois de son modèle fonctionnel et de son modèle organisationnel. Ils évaluent également **l'importance de leur activité** dans la performance et les objectifs opérationnels globaux de l'entreprise. Ce paramètre d'importance permet de réaliser la transposition des risques entre les activités de base et la gouvernance d'entreprise, qui ont chacun leur propre référentiel d'acceptabilité (un risque perçu comme inacceptable au niveau d'une activité de base peut être acceptable à l'échelle de l'organisation et inversement). Il permet ainsi de donner une mesure de la **différence de perception des risques et valeurs** entre les activités de base et la gouvernance, symptôme d'un désalignement de vision et de divergences entre les niveaux stratégique et opérationnel/métier. La démarche est donc à la fois *top-down* car elle construit ses référentiels à partir de la définition des objectifs et exigences par la gouvernance et *bottom-up* car elle fait remonter la perception des risques des activités de base. De surcroît, **l'évaluation financière des risques** perçus est réalisée par le recueil de la perception des pertes associées aux risques et des efforts nécessaires pour les réduire. Au final, elle fournit à la gouvernance une **vision globale des risques et de leur financement** au niveau de l'organisation, mais aussi une **vision détaillée à tous ses niveaux**, indispensables pour construire une stratégie d'entreprise mais également pour suivre et ajuster à intervalle régulier sa mise en œuvre dans un contexte d'environnements incertains. Elle répond au standard de l'ISO31000 [10].

Dans un premier temps, la MCRA peut être appliquée classiquement pour dresser une **photographie des risques globaux** de l'entreprise afin d'identifier les différents axes de sa stratégie future, dont la stratégie numérique (Fig. 1). Ces résultats enrichissent les méthodes dédiées à l'analyse stratégique (SWOT, *Visioning*, Atouts-Attraits, FCS, Décision multicritères), utilisées pour définir la stratégie numérique (objectifs et choix entre les différentes alternatives). Dans un second temps et ensuite à fréquence optimisée, **en centrant les audits sur les leviers relatifs à la transformation numérique,** la MCRA permet de dresser l'état des lieux des risques liés aux transitions envisagées, et d'aider ainsi à l'anticipation des possibles freins au changement, des signaux faibles reflétant un non-alignement de la vision entre le *board* et les équipes opérationnelles, mais aussi des faiblesses structurelles ou vulnérabilités latentes qu'il conviendra de prendre en compte sur tout le cycle de la transformation numérique. La démarche MCRA donne les clés permettant au CTO/CDO :

- D'orienter ou conforter la stratégie de transformation envisagée ;
- De bâtir et suivre le plan d'actions de gestion des risques associé au plan de transformation en intégrant l'ensemble des chaînes de valeur de l'entreprise et de son écosystème ;
- D'orienter les investissements grâce à l'analyse financière des risques.

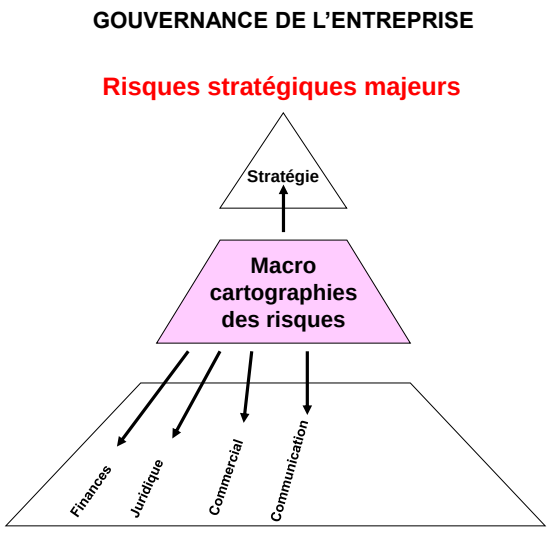

Fig. 2. Elaboration de la cartographie des risques

II. CONCEPTS PRELIMINAIRES DU RISQUE

La démarche MCRA s'appuie sur un socle méthodologique d'appréciation du risque dont on rappelle ici les concepts majeurs.

Le risque met en jeu deux notions. L'une, qualitative qui concerne son origine, à savoir l'exposition du système au danger par un événement contact, appelée situation dangereuse, qui, sous l'effet d'un événement amorce, peut se transformer en événement redouté avec des conséquences de différentes natures et importances en termes de préjudices ou de dommages, dépendantes des circonstances temps-

environnement (facteurs aggravants). L'autre, quantitative, est la « mesure » en termes de probabilité et de gravité de l'incertitude de la situation dangereuse ou de l'événement redouté [13,14].

Dans la pratique, **l'identification des risques** est faite en utilisant un ensemble d'outils méthodologiques traitant de façon complémentaire de la nature des événements et de leurs localisations spatiale et temporelle. L'évaluation des risques est faite, d'une part, sur l'incertitude de l'occurrence en utilisant une échelle d'index de vraisemblance (analyse qualitative ou semi-quantitative) ou de valeurs de probabilité (analyse quantitative) et, d'autre part, sur les conséquences en utilisant une échelle d'index de gravité ou de valeurs de pertes et d'efforts. La maîtrise des risques est associée directement aux actions de réduction et de contrôle faites sur les composantes du risque : la prévention regroupe les actions qui ont pour but de diminuer la probabilité d'occurrence du risque tandis que la protection regroupe les actions qui ont pour but de diminuer la gravité des conséquences.

Le processus de réduction des risques est fondé sur le concept de **criticité du risque** qui ne peut être mis en œuvre que lorsque la gouvernance du risque a préalablement fait la répartition de l'ensemble des risques de l'activité en trois zones correspondant à leur criticité suivant le principe ALARA (*As Low As Reasonably Achievable*), à savoir en :

1. Risque acceptable en l'état ;
2. Risque tolérable sous contrôle ;
3. Risque inacceptable.

La criticité du risque est le résultat d'une fonction de décision associée à une échelle de valeurs politique, éthique, religieuse, économique, qui pour chaque risque évalué associe ou non une action de réduction ou de contrôle. L'ensemble de ces zones est visualisé respectivement en vert, jaune et rouge sur le Tab.1.

TABLEAU 1. EXEMPLE D'ECHELLE DE CRITICITE

		Gravité				
		1	**2**	**3**	**4**	**5**
Vraisemblance	**5**	1	2	3	3	3
	4	1	2	3	3	3
	3	1	1	2	3	3
	2	1	1	2	2	3
	1	1	1	1	2	2

Enfin, à la notion d'acceptabilité du risque s'ajoute celle du **financement du risque**. Il est fondé :

- D'une part sur l'évaluation du bénéfice/perte, c'est-à-dire le rapport des gains potentiels liés à la présence d'une opportunité par rapport aux pertes potentielles liées à la présence d'un danger. Une telle évaluation nécessite d'aborder conjointement pour un même projet l'analyse des risques positifs et celle des risques négatifs ;
- D'autre part sur l'évaluation des pertes/surcoût, c'est-à-dire le rapport des pertes attendues si on ne fait rien et des coûts liés à la mise en œuvre d'actions de réduction des risques. La décision de traitement du risque est politique si les coûts sont supérieurs aux pertes et économiques si les pertes sont supérieures aux coûts.

III. PRINCIPES DE LA MCRA

Le processus de la MCRA est invariant quel que soit le domaine d'activité et le périmètre de l'étude, et son application se déroule en trois étapes (Fig. 3) : la préparation, la réalisation et la valorisation. Une démarche MCRA peut être menée au niveau d'une entreprise et de l'ensemble de ses processus globalement, ou bien d'un projet particulier (par exemple un projet de transformation numérique), ou bien d'un processus, sous-processus ou activité de base spécifique. Dans la suite du document, nous employons le terme générique de « projet ».

La première étape de préparation (tâche 1.1) débute par la réalisation de la cartographie des processus, sous-processus et activités de base de l'entreprise suivant le formalisme de l'ISO9001 : Management, Soutien, Réalisation [15].

Le plan d'audit est ensuite établi en sélectionnant les entités (par exemple le siège et les différents établissements) qui hébergent les sous-processus et activités contribuant au projet concerné (tâches 1.2 et 1.3) ; aux intersections des sous-processus et des activités sont identifiés des responsables métiers qui doivent être audités. **La cartographie des dangers** (tâche 1.4) est élaborée à partir de la liste des 27 dangers génériques standards [7,8,9] ou d'une base de connaissances contextualisée au projet. Elle constitue le socle de base des audits en ce sens qu'elle fournit une grille de lecture pour évaluer les critères de risques et de valeurs associés au projet (ex : juridique, réglementaire, financier, éthique, image, cybersécurité, facteur humain, performance économique, transformation du métier). La démarche MCRA étant par essence agile, il est possible de sélectionner un premier jeu de critères de risques-valeurs particulièrement prégnants que l'on souhaitera auditer en priorité, et de planifier plusieurs itérations successives permettant de traiter ensuite des critères jugés secondaires.

Enfin, **un questionnaire ouvert** accompagnant la grille d'évaluation des risques est élaboré afin de : (i) identifier les rôles et fonctions des personnes auditées ; (ii) évaluer le niveau de maturité d'une part vis-à-vis de la gestion des risques et d'autre part vis-à-vis de la transformation numérique ; (iii) préciser par des exemples concrets la nature des dangers et menaces perçus ou évalués ; (iv) mesurer le niveau d'adhésion à la stratégie numérique envisagée. L'ensemble de ces informations permet de compléter et d'interpréter les cartographies des risques de la MCRA.

Les éléments d'évaluation du risque utilisés pendant les audits sont : (i) l'échelle de gravité des conséquences des risques perçus au niveau des activités de base ; (ii) l'échelle de vraisemblance de ces risques ; (iii) l'échelle d'importance qui mesure la perception de l'importance de l'impact du danger sur le projet au travers de son impact sur les activités.

Les éléments de décision utilisés pour l'élaboration de la macrocartographie sont : (i) les référentiels de criticité du risque des activités de base et de la gouvernance du système ; (ii) la fonction de transfert des perceptions de risques entre le niveau des activités de base et le niveau de gouvernance du

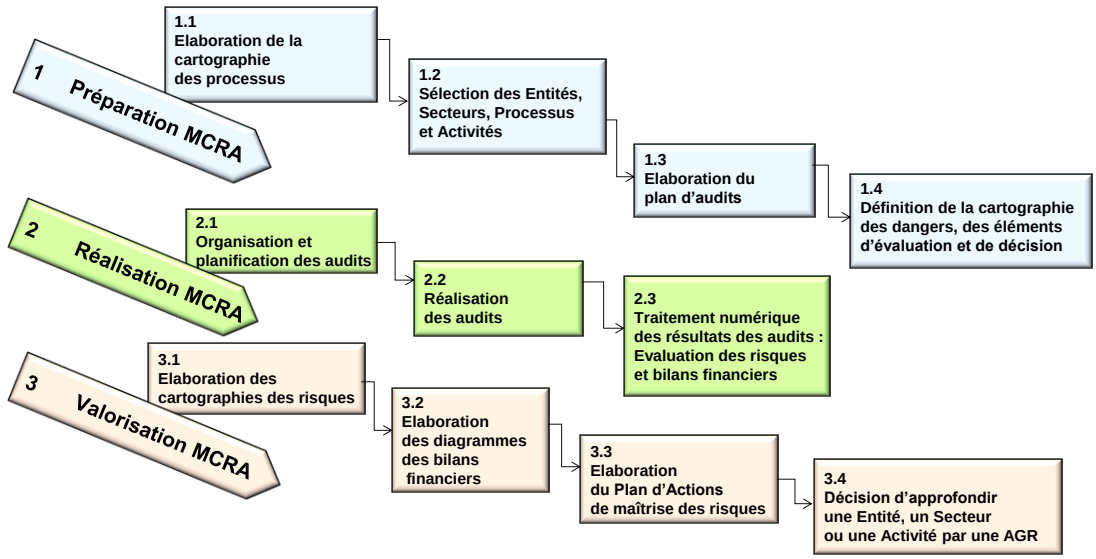

Fig. 3. Processus de la MCRA

projet, qui définit les niveaux de gravité et vraisemblance perçus au niveau du projet en fonction du facteur d'importance de l'activité. Elle traduit par exemple le fait qu'un risque peut être perçu comme ayant des conséquences graves au niveau d'une activité sans pourtant que celles-ci soient perçues comme graves au niveau de la gouvernance du projet, et inversement.

La première phase de préparation d'une MCRA est réalisée avec la gouvernance projet et fait appel aux études de qualité et de risques existantes, ainsi qu'au retour d'expérience (REX) en particulier pour l'élaboration de la liste des dangers et pour la définition des paramètres financiers.

La deuxième étape (tâches 2.1 à 2.3) concerne l'organisation et la planification des audits, suivies de leur réalisation puis du traitement numérique des résultats. Les audits sont fondés, comme évoqué ci-dessus, d'une part sur un questionnaire ouvert permettant d'évaluer le niveau de maturité de la gestion des risques dans l'activité auditée, et d'autre part sur la grille d'évaluation, pour chaque danger, des paramètres de gravité, de vraisemblance, d'importance, de perte et d'effort perçus. Lorsque plusieurs événements dangereux associés à un danger sont identifiés, c'est celui qui génère le risque le plus significatif qui doit être évalué. Ces données brutes fournissent les **cartographies des risques bruts perçus au niveau des activités**. Elles sont ensuite traitées numériquement.

Dans la troisième étape de valorisation, suivant une logique de regroupement décrite dans la Fig. 4 et dont l'algorithme est décrit dans [7,8,9], des cartographies des risques sont élaborées pour tous les niveaux de l'entreprise : sous-processus, processus, entités, secteurs et le projet lui-même. Les cartographies de l'importance perçue des dangers et des activités sont produites pour tous les niveaux de l'organisation. Enfin, les cartographies des pertes et des efforts et les diagrammes des bilans financiers sont également élaborés pour tous les niveaux.

La valorisation de l'ensemble de ces résultats aboutit à : (i) la hiérarchisation des risques majeurs pour le projet et l'identification des sous-processus et des secteurs les plus critiques ; (ii) l'analyse financière des risques par le calcul des rapports entre pertes et efforts à tous les niveaux ; (iii) l'élaboration d'un plan d'action de maîtrise des risques.

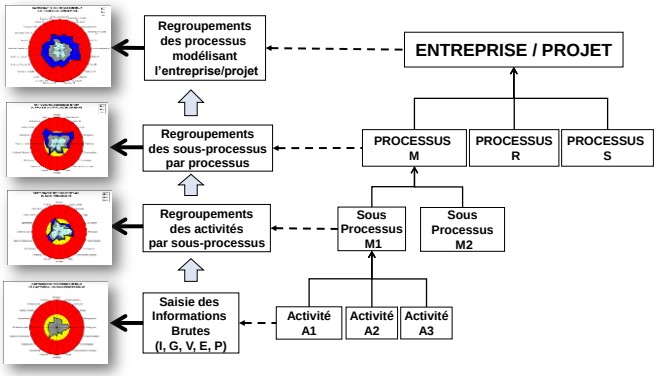

Fig. 4. Hiérarchisation des activités, sous-processus et processus dans l'organisation projet et logique d'évaluation. I : importance, G : Gravité, V : Vraisemblance, E : Effort, P : Perte.

IV. Application a un projet de transformation numerique

A. Cas d'étude

Le cas présenté illustre l'utilisation de la MCRA comme **outil de diagnostic des risques et de l'adhésion** dans le projet de transformation numérique d'une entreprise produisant des biens de consommation dans le domaine de la santé et du bien-être. Les axes stratégiques suivants ont été définis avec la gouvernance (SWOT, Vision, FCS, Atouts-Attraits) :

- Développer l'IA pour la R&D et l'aide à la conception de produits mieux adaptés aux profils client (individualisation du produit par gammes) ;
- Développer le profiling client : (i) en utilisant des outils d'analyse des réseaux sociaux ; (ii) en développant un outil SaaS sur le site Internet de l'entreprise pour guider le client dans la définition de son besoin et lui proposer les produits « *best match* » ;
- Implémenter un outil d'optimisation de la *supply-chain*

pour répondre en temps réel à la demande de produits individualisés par le client ;

- Développer la communication numérique de l'entreprise (réseaux sociaux, sponsoring et *branding* d'influenceurs et d'ambassadeurs digitaux, ciblage, *story telling*…) ;
- Développer une communication de crise.

Le plan d'audit (Tableau 2) a été défini avec la gouvernance, ainsi que les éléments d'évaluation des risques. 16 audits ont été menés auprès des responsables des sous-processus, dans 3 entités : le siège, le centre de R&D et une usine. Un premier diagnostic dont certains résultats sont illustrés ici a été réalisé au démarrage au projet.

TABLEAU 2. PLAN D'AUDITS

Plan d'audits			Structure et activités de l'entreprise										Nombre total d'activités auditées	
Entités →			1	1	1	1	1	1	2	2	3	3		
Processus	Sous-processus	Abrév / Secteurs	DG_DIR	DG_TD	DG_JUR	DG_RH	DG_COM	DG_FIN	DG_MA	C_RD	C_LAB	C_PROD	C_PROC		
Management (M)	Décision et organisation	M1	1											1	4
	Elaboration de la stratégie	M2		1										1	
	Programmation	M3		1										1	
	Maîtrise de la Qualité	M4	1											1	
Réalisation (R)	R&D	R1								1	1			2	4
	Production	R2										1	1	2	
Support (S)	Achats	S1		1										1	8
	Ventes	S2							1					1	
	Maîtrise de l'information	S3		1										1	
	Ressources humaines	S4				1								1	
	Ressources financières	S5						1						1	
	Sûreté et protection	S6	1											1	
	Communication externe	S7					1							1	
	Juridique	S8			1									1	
Nombre total d'audits par secteur			3	4	1	1	1	1	1	1	1	1	1		16
Nombre total d'audits par entité									12		2		2		
Nombre total de secteurs par entité									7		2		2		

B. Cartographie globale des risques

L'ensemble des cartographies dont sont issus les exemples présentés ici fournit un diagnostic complet des risques à tous les niveaux de l'entreprise. Ce diagnostic permet d'identifier :

- Les entités, activités et phases critiques du projet, en termes de risques perçus ou de faible adhésion, vis-à-vis de la stratégie de transformation numérique envisagée ;
- Les dangers et critères de valeurs qui sont à l'origine des risques les plus critiques, à tous les niveaux ;
- Les efforts perçus comme nécessaires pour réduire ces risques ou améliorer l'adhésion au projet ;
- Les risques résiduels résultant de la mise en œuvre des efforts perçus.

Ces cartographies fournissent non seulement les niveaux de risques moyens, mais aussi les risques minimum et maximum. Ces intervalles min-max représentent à la fois la dispersion des valeurs risque-adhésion des différentes activités ou phases du projet, mais aussi la dispersion des valeurs recueillies des paramètres lorsqu'une même activité est auditée plusieurs fois (si par exemple elle est répartie sur plusieurs sites). L'analyse de cette dispersion est tout aussi fondamentale que celle des valeurs moyennes et peut mettre en évidence des dysfonctionnements ou des perceptions hétérogènes d'un même danger, **hétérogénéité qui trahit souvent des problèmes de fonctionnement**.

Le tableau 3 présente les risques moyens globaux perçus par les 3 entités de l'entreprise. Les risques perçus comme inacceptables (rouges) sont :

- La cybersécurité (SIEGE). C'est la menace cyber qui est citée le plus souvent lors des audits. Elle est perçue comme importante car l'entreprise a subi ces dernières années plusieurs attaques informatiques dommageables : bien que ce risque ait déjà été pris en compte et fasse l'objet d'un plan d'amélioration continue, le projet de transformation numérique est considéré comme une source supplémentaire à la menace déjà existante. Les autres entités (R&D et USINE) le perçoivent comme relativement élevé également mais le risque moyen calculé reste dans la zone du tolérable. Cette différence de perception peut s'expliquer par le fait que les fonctions dédiées à la cybersécurité sont réalisées par le SIEGE ;
- La Transformation du métier et du système d'information, et la *Supply chain* (USINE). Il s'agit ici des risques perçus relatifs à la transformation digitale du système de production et de la réorganisation opérationnelle de la *supply-chain*. Le futur système n'a pas été encore spécifié et seuls les grands principes ont été présentés, ce qui génère un fort niveau d'incertitude pour la partie opérationnelle de l'activité. Par ailleurs, le système d'information utilisé actuellement en production est assez ancien mais considéré comme robuste et fiable et le changement (notamment le remplacement de l'ERP) est perçu comme source d'instabilité pour la production. Si le risque relatif à la transformation du métier et du SI est apprécié comme relativement élevé par les deux autres entités, la différence est plus importante pour le risque *supply chain* perçu comme beaucoup plus faible (tout en restant dans le tolérable) par la R&D et le SIEGE.

Le risque Ethique est perçu au sein de toutes les entités comme acceptable et c'est lui qui présente la valeur moyenne la plus faible. Il ne semble donc pas que la transformation à venir soit vue comme source de problèmes éthiques ; au contraire, les entretiens ont révélé que le ciblage marketing était perçu comme un accélérateur pour le commerce et la R&D. L'introduction de l'IA en recherche n'est pas perçue comme pouvant potentiellement remplacer les experts mais au contraire comme un outil augmentant leurs capacités d'innovation. Il ressort que les risques perçus comme faibles et acceptables reflètent ici une adhésion au projet.

On note des discordances de perception qui constituent des points d'attention particuliers pour la direction de projet et le CTO/CDO :

- Pour le risque Matériels et Equipements, perçu comme beaucoup plus élevé en R&D que dans les autres entités. Cela est lié aux incertitudes relatives aux capacités de calculs des systèmes de R&D, peu prises en compte par les autres entités, particulièrement le SIEGE ;
- Pour le risque Communication et Crises, perçu comme élevé par le SIEGE et l'USINE mais très faible par la R&D. Ce point est sensible pour les fonctions de management et pour la production, vraisemblablement car elles seront particulièrement impactées en cas de survenue d'une situation de crise consécutive à la transformation digitale envisagée, ce qui semble beaucoup moins le cas pour la R&D. Les incertitudes évoquées sont relatives à la forte dépendance future au système d'information qui, s'il

est défaillant ou attaqué, pourrait être à l'origine du blocage de la production.

TABLEAU 3. RISQUES MOYENS INITIAUX PERÇUS PAR ENTITE ET PAR DANGER. LORSQU'UNE CASE EST VIDE, CELA SIGNIFIE QUE LE RISQUE N'A PAS ETE EVALUE (NON CONCERNE OU IGNORANCE)

Risques Moyens initiaux moyens par entité et par danger		Entités de l'entreprise					
Dangers	Abrèv	SIEG	RD	USI	Max	Moy	Min
Environnements	ENV	6,5	9,0		9,0	7,7	6,5
Cybersécurité	CYB	12,5	12,0	10,5	12,5	11,7	10,5
Image	IMA	8,6	4,0		8,6	6,3	4,0
Client	CLI	9,5	7,5	10,5	10,5	9,2	7,5
Culture d'Entreprise	ENTR	8,2	8,8	6,0	8,8	7,6	6,0
Management	MAN	9,6	8,0	8,8	9,6	8,8	8,0
Stratégique	STR	8,0	6,0	12,0	12,0	8,7	6,0
Technologique	TECH	9,0	12,0	10,5	12,0	10,5	9,0
Communication et crises	CRIS	9,7	4,0	12,0	12,0	8,6	4,0
Ethique	ETH	6,0	3,0		6,0	4,5	3,0
Juridique	JUR	8,5	6,3	6,0	8,5	6,9	6,0
Financier	FIN	8,0	7,5	6,0	8,0	7,2	6,0
Commercial	COM	9,3	6,0	8,8	9,3	8,0	6,0
Matériels et équipements	MAT	5,3	10,5	7,5	10,5	7,8	5,3
Transformation du métier et du SI	SI	11,1	10,5	14,0	14,0	11,9	10,5
Projets et Etudes	PROJ	8,0	12,0	10,5	12,0	10,2	8,0
Supply-chain	SUPP	9,0	7,5	14,0	14,0	10,2	7,5
Facteur humain	FH	8,7	12,0	9,0	12,0	9,9	8,7
Max		12,5	12,0	14,0	14,0	11,9	10,5
Moy		8,6	8,1	9,7	10,5	8,6	6,8
Min		5,3	3,0	6,0	6,0	4,5	3,0

La figure 5 visualise la hiérarchisation des risques globaux par leur valeur moyenne et permet d'en établir un classement et une priorisation. Chaque item évalué lors des entretiens peut faire l'objet d'une analyse fine, à la fois quantitativement grâce à l'exploitation des évaluations et qualitativement en dépouillant les entretiens ouverts.

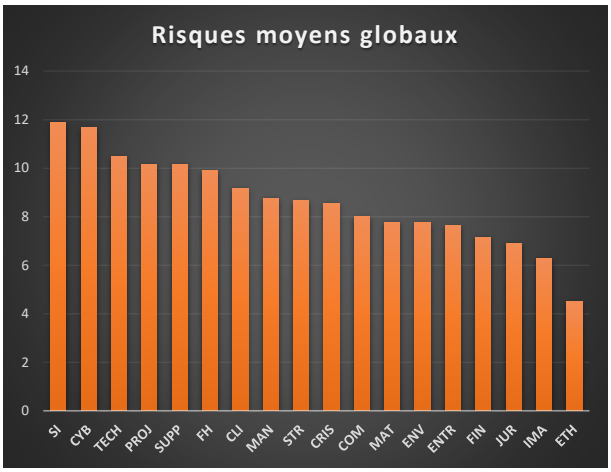

Fig. 5. Risques moyens globaux

Les cartographies des risques présentées dans la figure 6 (diagrammes de Kiviat) visualisent de manière synthétique les domaines de variations des risques perçus pour les risques initiaux (avant traitement) et résiduels (attendus après traitement). A ce stade, les risques résiduels présentés sont ceux attendus si les actions de traitement sont mises en œuvre, mais il conviendra de renouveler le processus de la MCRA afin de vérifier que ces objectifs de réduction ont été atteints. **Ainsi la MCRA est aussi un outil de suivi des indicateurs de la maîtrise de la transformation digitale.**

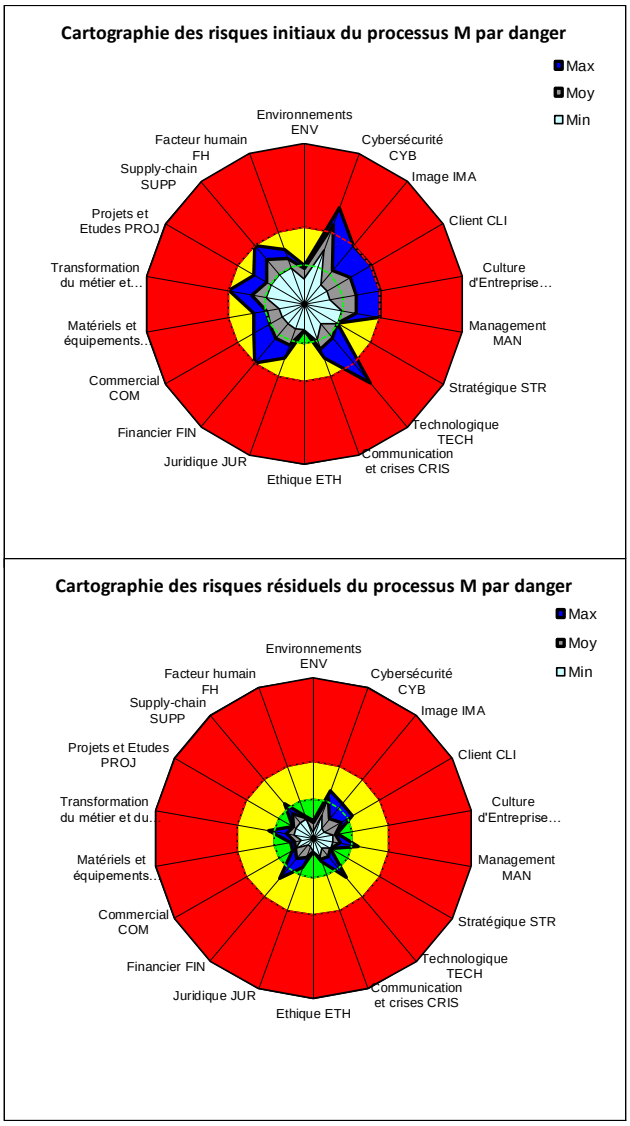

Fig. 6. Cartographie des risques initiaux (avant traitement) et résiduels (attendus après traitement) du processus de Management

La figure 7 présente les montants financiers cumulés des pertes associées aux risques non traités et des efforts perçus comme nécessaires pour traiter les risques. Les pertes perçues sont généralement supérieures aux efforts perçus, indiquant un bénéfice économique à traiter les risques. Seuls les risques relatifs aux aléas environnementaux correspondent à un rapport coût/risque déficitaire : cela est lié au fait qu'en absence de contrôle possible sur les environnements physiques, technologiques, écologiques, politiques…, la maitrise de ces risques est perçue comme coûteuse et hasardeuse. La MCRA fournit bien d'autres éléments d'analyse car l'ensemble des diagrammes est décliné : par processus, par sous-processus, par regroupement de sous-processus, par dangers, par regroupement de dangers, par entités, par activités et par audits. Tous les points de vue et points d'entrée de l'analyse peuvent être représentés.

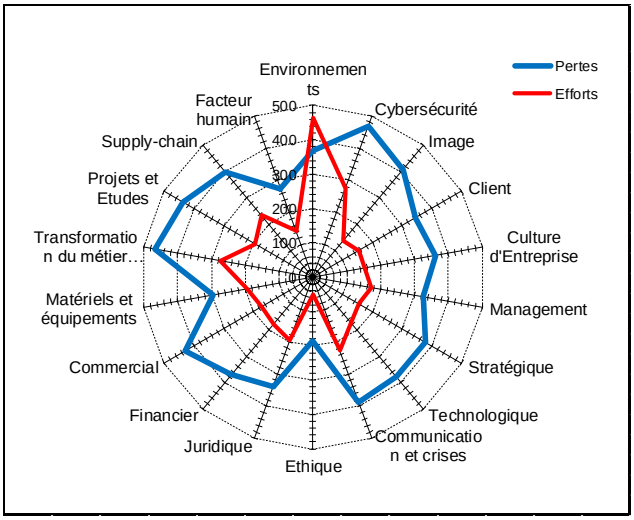

Fig. 7. Montants financiers cumulés pour les pertes associées aux risques perçus et pour les efforts perçus comme nécessaires pour les réduire

Le tableau 4 donne la vision globale des risques regroupés par **leviers de transformation** selon l'approche présentée dans [5].

TABLEAU 4. RISQUES MOYENS INITIAUX REGROUPES PAR LEVIERS DE TRANSFORMATION NUMERIQUE [5]

		Risques initiaux								
Risques Moyens des regroupements par danger		**Gravités initiales**			**Vraisemblances initiales**			**Risques Moyens initiaux**		
Catégories	**Abrèv**	**Max**	**Moy**	**Min**	**Max**	**Moy**	**Min**	**Max**	**Moy**	**Min**
Stratégie et Organisation	ST-ORG	3,84	2,94	1,81	4,13	2,83	2,00	15,9	8,3	3,6
Environnements	ENV	3,30	2,83	2,00	4,00	3,09	2,29	13,2	8,7	4,6
Personnel	PERS	4,00	3,09	2,00	3,46	2,64	2,00	13,9	8,2	4,0
Offre	OFF	3,78	2,81	2,00	4,18	2,87	2,00	15,8	8,1	4,0
Technologie et Innovation	TEC-INN	3,78	2,96	2,17	3,78	2,93	2,00	14,3	8,7	4,3

La démarche MCRA menée par le CTO/CDO met clairement en évidence que le projet envisagé est perçu comme audacieux et source de risques pour l'ensemble des leviers de la transformation digitale de l'entreprise (risque initial moyen dans le jaune pour tous les leviers). Les impacts potentiels sur la stratégie de l'entreprise et sur son organisation sont perçus par certains acteurs comme particulièrement élevés (risque initial max. dans le rouge) : le projet de transformation envisagé touchera le cœur de la vision stratégique historique de l'entreprise, il impactera significativement l'organisation des métiers et de la production, l'usage des systèmes numériques, mais aussi la nature de la relation commerciale avec les clients et usagers. La direction de l'entreprise et le CTO/CDO l'avaient identifié, mais pas avec une telle ampleur. D'autre part, il est intéressant de constater une dispersion importante du risque (Min, Max, Moy), qui traduit des différences de perceptions des risques et d'adhésion au projet importantes entre les acteurs audités, voire des antagonismes. Le CTO/CDO a constaté, en faisant une analyse fine des audits, une « fracture » latente d'une part générationnelle au sein des équipes et d'autre part géographique entre certains sites et services. Tous ces éléments recueillis lui ont permis d'identifier des points d'attention et axes d'efforts, et d'orienter le plan de transformation, notamment concernant les aspects suivants :

- Echelonnement du projet en commençant par l'axe de transformation ayant le meilleur ratio risque/adhésion/pertes/efforts (il s'agit de l'axe « développer l'IA pour la R&D et l'aide à la conception de produits mieux adaptés aux profils client ») ;
- Adaptation du plan de communication initial afin de prendre en compte de façon ciblée les perceptions de risques exprimées, particulièrement concernant les volets « Supply chain » et « Transformation métier/SI » ;
- Lancement d'une prestation d'accompagnement, par un cabinet spécialisé, du volet cybersécurité du projet compte-tenu des inquiétudes très vives exprimées sur ce sujet.

Une fois l'ensemble de ces résultats analysé et les risques hiérarchisés, **un plan d'action** de réduction des risques et de gestion des risques résiduels peut être élaboré. **Un tableau de bord** de suivi de réalisation des actions, de maîtrise des effets secondaires des actions et des coûts financiers d'avancement des actions facilite le management des risques. Enfin, le diagnostic au démarrage du projet doit être suivi d'une **réévaluation** des risques planifiée à intervalle régulier et intégré dans les outils de management de projet.

V. CONCLUSION

La démarche de macrocartographie des risques par les audits constitue un outil puissant pour piloter un projet de transformation d'entreprise sous l'angle de la **perception des risques** et de **l'adhésion au projet** entre le niveau de gouvernance et les différentes parties prenantes métiers. Son application à différentes étapes du projet fournit la mesure et le suivi de l'évolution de la transformation tout en faisant vivre explicitement le sujet auprès des acteurs en sollicitant à intervalle régulier leurs perceptions. Parce qu'elle adresse de façon agile et efficiente l'ensemble des leviers de la transformation (stratégie, organisation, ressources humaines, transformation des métiers et des SI, innovation et technologie, *supply chain*…), la méthode MCRA offre au *Chief Transformation ou Digital Officer* (CTO/CDO) une **vision « à 360° »** des risques et des enjeux de perception, ce qui lui permet d'orienter efficacement la transformation envisagée ; d'autre part, il peut concentrer les efforts et ressources sur les facteurs de risque les plus prégnants et sur les axes du projet pour lesquels une adhésion et une confiance fortes ont été exprimées.

La MCRA permet de **faire émerger les freins**, signaux faibles, divergences de visions, écarts de maturité entre les différentes entités et niveaux de l'entreprise concernant des dangers, préoccupations ou motivations inhérents au projet. En cela, elle est le support de la transition entre un état du système et de son environnement où la connaissance globale est constituée par la juxtaposition plus ou moins perméable de **connaissances individuelles** et un état où la connaissance globale devient **collective** et partagée. Elle permet ainsi de **créer de l'adhésion** et de préparer les équipes au changement car les questionnaires d'audits reflètent les enjeux, défis et objectifs que la gouvernance donne au projet. En ce sens, elle peut être utilisée pour orienter le plan de communication en agissant efficacement et de façon ciblée sur la sphère des perceptions. Associée aux méthodes usuelles d'analyse stratégique (SWOT, *Visioning*, Atouts-Attraits…), la MCRA contribue à **orienter**, **conforter** et **maîtriser les risques** d'une stratégie et d'un plan de transformation au travers de ses différents leviers. En effet, les critères de risques et de valeurs associés à ces derniers peuvent être facilement

intégrés dans la cartographie des dangers qui sert de socle d'évaluation lors des audits. Enfin, la MCRA inclut une analyse financière bénéfices/pertes/risques qui permet d'orienter et rationnaliser les **investissements** à mener pour les différentes phases et leviers du projet de transformation.

La démarche peut être **outillée**, elle est **capitalisable** et s'adapte pleinement aux cultures et modes de fonctionnement des entreprises. Les cartographies des risques et les analyses financières qui en sortent sont directement utilisables par les acteurs du management du risque et de la transformation numérique.

VI. REMERCIEMENTS

Nous remercions le *reviewer* de l'IMDR pour ses commentaires et suggestions constructifs.

REFERENCES

[1] Cardon D., 2019. Culture numérique. Paris : Presses de Sciences Po, 2019 — (Les Petites Humanités).

[2] Douglas C. Engelbart, 1962 Augmenting Human Intellect: A Conceptual Framework. SRI Summary Report AFOSR-3223 Prepared for: Director of Information Sciences, Air Force Office of Scientific Research, Washington DC.

[3] Babinet G., 2019. Transformation digitale : l'avènement des plateformes. Editions Le passeur.

[4] Michon A. et Hyppolite P.A., « Les géants du numérique. Magnats de la finance », novembre 2018, Fondation pour l'Innovation Politique. http://www.fondapol.org/etude/les-geants-du-numerique-1-magnats-de-la-finance

[5] Fayon D., Tartar M., 2019. Transformation Digitale 2.0 : 6 leviers pour parer aux disruptions. Pearson France.

[6] Cigref, 2018. Valeur économique des projets de transformation numérique pour l'entreprise, http://cigref.fr

[7] Desroches A., Déniel L., 2019. Macrocartographie des Risques par les Audits. Ed Lavoisier Hermes Science, ISBN 978-2-7462-4849-6.

[8] Delmotte S., Desroches A., 2015. Macro-Cartographie des Risques par Audit : Une méthode de diagnostic et de management global des risques d'entreprise. Congrès Qualita 2015 ; 17-19 mars 2015, Nancy.

[9] Desroches A, et al., 2010. Le management des risques des entreprises et de gestion de projet. Ed Hermes science.

[10] Norme ISO 31000:20018. Management du Risques – Principes et Lignes Directrices.

[11] Mignot O., 2019. La transformation digitale des entreprises : principes, exemples, mise en œuvre, impact social. Maxima, Paris.

[12] Chaintreuil J.N., 2015. RH & Digital : Regards collectifs de RH sur la transformation digitale. Diateino.

[13] Desroches A., N. Aguini, M Dadoun et S. Delmotte, 2016. L'Analyse globale des risques - Principes et pratiques, 2009, Seconde Edition, Ed Lavoisier Hermes science.

[14] Desroches A, 2013. Le management des risques par l'analyse globale des risques, Transfusion Clinique et Biologique, Volume 20, Issue 2, pp 198-210, ISSN 1246-7820.

[15] Norme ISO 9001:2008. Systèmes de management de la qualité.