

**APPROCHE INTÉGRÉE de PROTECTION de l'INFORMATION  
GSA5-MED2  
Les domaines engageants pour la performance pérenne**



**ISBN : 978-1989364109**

Première édition numérique gratuite publiée en mars 2019 par YLA Formation inc.,  
via:

**[www.share.institute](http://www.share.institute)**

**YVAN LAUZON, MBA**

## SOMMAIRE

L'Approche intégrée **GSA5-MED2** présente une démarche regroupant onze domaines (ou perspectives) distincts, trop souvent gérés totalement de façon isolée dans l'organisation, couvrant sept domaines de Management qui sont gérables au quotidien:

**GSA5** pour Gouvernance / Sécurité / Accès à l'information & Vie privée / Architecture / Assurance / Audit / Archivistique;

mais aussi, quatre domaines de Normativité (encadrement) :

**MED2** pour Morale / Éthique / Déontologie / Droit.

Cette Approche innovante peut servir à mieux considérer les importants enjeux & défis de ces onze domaines engageants pour la performance pérenne, permettant notamment de mieux couvrir :

l'Accès à l'information et la Protection des données-informations-connaissances; l'Analyse de l'environnement d'affaires dans un monde toujours changeant (ViCA-VUCA);

l'Analyse de son secteur d'affaires;

l'intelligence d'affaires (Bi)

l'Intelligence économique (concurrence, +++);

l'Intelligence collective pour FAIRE MIEUX, en faisant autrement, TOUS ENSEMBLE;  
la Gestion des connaissances collectives (Knowledge Management).

\* \* \*

**Pour obtenir votre copie imprimée :**

Consultez l'ÉDITEUR-DISTRIBUTEUR : **YLA FORMATION inc.**

C.P. 24006, CSP POINTES, MONTREAL, CANADA, H1A 4Z2

**[newmanagement2.0@gmail.com](mailto:newmanagement2.0@gmail.com)**

\* \* \*

**La deuxième édition de ce livre numérique (augmentée d'au moins 30%) sera payante, mais à faible coût, disponible dès juin 2019. Pour information : [www.share.institute](http://www.share.institute)**



### **Yvan Lauzon, MBA est Expert-conseil à l'international & Professeur contractuel**

Enseignant actuellement à l'Université du Québec (ENAP- UQ) différents cours en Gestion de projet (GP), en Gestion des ressources humaines dans un contexte technologique (eGRH), en Intelligence collective & Équipe de projet performante, de même qu'en Leadership dans les projets internationaux.

Depuis 1981, Yvan a occupé différents postes au sein d'organisations publiques & privées, notamment *Adjoint de sous-ministre associé* (Bureau du CIO) au gouvernement du Québec de 2006 à 2008. Yvan a agi durant 5 ans à titre de *Coordonnateur gouvernemental de la sécurité* et durant 2 ans comme *Directeur* au conseil d'administration de l'*Association sur l'accès et la protection de l'information* (AAPI) et *Coordonnateur* de GP-Québec (Gestion de projet) associé au PMI-Lévis Québec.

Yvan agit aussi à titre d'expert-conseil pour de grandes organisations internationales, notamment aux Nations-Unies (ONU-CEFACT, 1993-1996) et à l'OCDE (2006-2008).

Parallèlement, Yvan enseigne depuis 1987 dans des programmes de Maîtrise d'universités canadiennes & étrangères, dont : MAP (Administration publique), MBA (Affaires) & MGP (Gestion de projet, GP). Ces dernières années il a surtout enseigné : eGRH / Équipe de projet performante / Gestion de projet / Gestion des savoirs collectifs (KM) / Gouvernance / Intelligence collective / Leadership / Management TI.

Plus spécifiquement, Yvan a enseigné quelques années la Sécurité de l'information, d'abord en formation continue au Centre de recherche informatique de Montréal (CRIM), puis en cours universitaires à l'Université du Québec. Il a aussi enseigné la Gouvernance des ressources informationnelles (GRI) à l'Université de Sherbrooke.

D'autre part, Yvan a lancé et financé plusieurs initiatives multilingues gratuites visant le développement des compétences du personnel des organisations publiques, parapubliques et privées canadiennes et étrangères, dont: ([www.share.institute](http://www.share.institute)), ([www.climb.express](http://www.climb.express)), ([www.smartconference.ca](http://www.smartconference.ca)).

Finalement, Yvan réalise depuis février 2018 une Tournée internationale portant sur : ***Compétences requises en 2020 des Chefs de projets--Leaders et de leurs Gestionnaires.***

\* \* \*

*Le présent ouvrage a été lancé à Nantes (FRANCE) le 26 mars 2019, lors de la conférence  
**RFQM 2019** (Rencontres Francophones sur la Qualité et la Mesure)*

*This book was launched in Nantes (FRANCE) on March 26, 2019, during the conference  
**RFQM 2019** (Francophone Meetings on Quality and Measurement)*

*Este libro fue lanzado en Nantes (FRANCIA) el 26 de marzo de 2019, durante la conferencia  
**RFQM 2019** (Rencontres Francophones sur la Qualité et la Mesure).*

## DÉDICACE

Cet ouvrage est dédié à toutes les personnes de la francophonie qui suivent actuellement des cours en Management (BAA, MAP, MBA, ...) et/ou en Gestion de projet (MGP).

\* \* \*

## REMARQUES

1.. **GENRE** -- Le genre masculin est utilisé dans ce livre sans discrimination et dans le seul but d'alléger le texte.

2.. **ÉCRITURE** -- Les lettres majuscules et le caractère & (la perluète) sont abondamment utilisés ici simplement pour des fins pédagogiques, ne respectant pas toujours les règles d'écriture, des autorités linguistiques, la calligraphie ou les usages de plus de 125 millions de francophones.

3.. **DROITS d'AUTEUR** : Toute reproduction totale ou partielle est interdite, par quelque moyen que ce soit, sans une autorisation écrite d'Yvan Lauzon MBA, via ( gestionnaire2.0@gmail.com )

## Table des matières

INTRODUCTION.....	1
REMARQUE.....	2
SECTION 1 : La Performance pérenne débute par la Compétence.....	3
SECTION 2 : Activités organisationnelles.....	5
2.1 Modes de fonctionnement des organisations : Opérations courantes & Mode Projet .....	5
2.2 Typologie des projets.....	8
2.3 Chef de projet Leader .....	9
2.4 Confiance : Un prérequis essentiel aux affaires .....	11
SECTION 3 : Données + Informations + Connaissances + Compétences.....	12
3.1 Définition.....	12
3.2 Actifs informationnels & Ressources informationnelles.....	12
3.3 Propriétés & Typologies d'information.....	14
SECTION 4 : Approche intégrée couvrant 7 domaines de Management (GSA5) & 4 domaines de Normativité (MED2).....	16
4.1 Gouvernance .....	16
4.2 Sécurité .....	18
4.3 Accès à l'information & Protection de la vie privée .....	25
4.4 Architecture.....	28
4.5 Assurance .....	28
4.6 Audit.....	29
4.7 Archivistique.....	29
4.8 Morale.....	30
4.9 Éthique .....	30
4.10 Déontologie.....	31
4.11 Droit .....	31
SECTION 5 : Meilleures pratiques en Management : L'exemple des TIC .....	34
CONCLUSION & PROSPECTIVE .....	36
REMERCIEMENTS .....	37
ANNEXE_1.....	38
Référentiels des Meilleures pratiques en Management TIC .....	38

\* \* \*

## INTRODUCTION

Le présent ouvrage numérique gratuit est lancé le jour même d'un Atelier que je donne à Nantes (France) sur la Protection de l'information, dans le cadre d'un événement en Qualité et Métrologie, soit **RFQM 2019**.

Bien entendu, la *Protection de l'information* est souvent prise pour acquise, un peu comme les services publics. En effet, comme la distribution d'électricité, d'eau ou de gaz dans nos maisons, lorsque ça fonctionne bien, on ne les remarque même pas... Pourtant bon nombre de personnes s'y affèrent quotidiennement, pour nous offrir des services publics de qualité, sans failles.

\* \* \*

Le présent ouvrage de type « ESSAI LIBRE non scientifique » ne prétend à aucune exhaustivité, les onze sujets présentés ici étant particulièrement étendus et à grande portée (Scope & Range). Mais vous aurez certainement plaisir à parcourir ce livre de Management, riche en contenu innovant et facile à comprendre.

\* \* \*

La première section présente les composantes de la performance organisationnelle pérenne requises pour assurer la continuité des opérations et innover dans la façon de livrer des produits et services à des clients internes ou externes toujours plus exigeants.

La seconde section traite des principaux modes de fonctionnement des organisations post-modernes, soit le mode des Opérations courantes et le mode Projet. Cette section couvre également les compétences requises des Chefs d'équipes (ex : Chefs de projet) et aussi de la Confiance, véritable moteur des affaires.

La troisième section aborde les principales distinctions, propriétés et typologies des différentes composantes informationnelles de l'organisation, car il importe au départ de bien comprendre ce qu'il faut protéger, soit « le Quoi » et « le Pourquoi », avant d'y aborder « le Comment », dont les moyens techniques.

La quatrième section illustre les particularités des onze domaines de l'Approche intégrée de Protection de l'information GSA5-MED2, sept touchant des domaines gérables dits de Management (GSA5 pour Gouvernance / Sécurité / Accès à l'information & Vie privée / Architecture / Assurance / Audit / Archivistique), les quatre autres étant plutôt des encadrements normatifs, dits domaines de Normativité (MED2 pour Morale / Éthique / Déontologie / Droit).

Finalement, la cinquième section souligne l'importance pour les Corporations professionnelles ou autres Associations professionnelles de ces onze domaines plus engageants pour l'organisation, de se doter de code de conduite, de corpus de connaissances (BoK), de référentiel de meilleures pratiques (Best practices) et de méthodologie éprouvée. L'ouvrage renferme également une annexe touchant le Management TIC.

\* \* \*

Ce livre n'a pas été conçu spécialement pour une lecture continue, mais plutôt un parcours pas à pas; par exemple, à raison de deux ou trois sous-sections par jour (par ex. 2.1 à 2.3) --pour environ 20 à 30 minutes de lecture par jour-- sur 7 jours. Il est aussi possible de sauter une sous-section, puis d'y revenir un peu plus tard, chacune étant autonome.

Bonne lecture !  
**Yvan Lauzon MBA**

## REMARQUE

L'Approche **GSA5-MED2** ne doit pas être perçue comme 11 pièces contiguës s'imbriquant l'une dans l'autre dans un Puzzle, mais bien comme une mosaïque en 11 couches superposées, telle une Matrice graphique d'une Ville intelligente.



\* \* \*

## SECTION 1 : La Performance pérenne débute par la Compétence

### Contexte d'affaires actuel

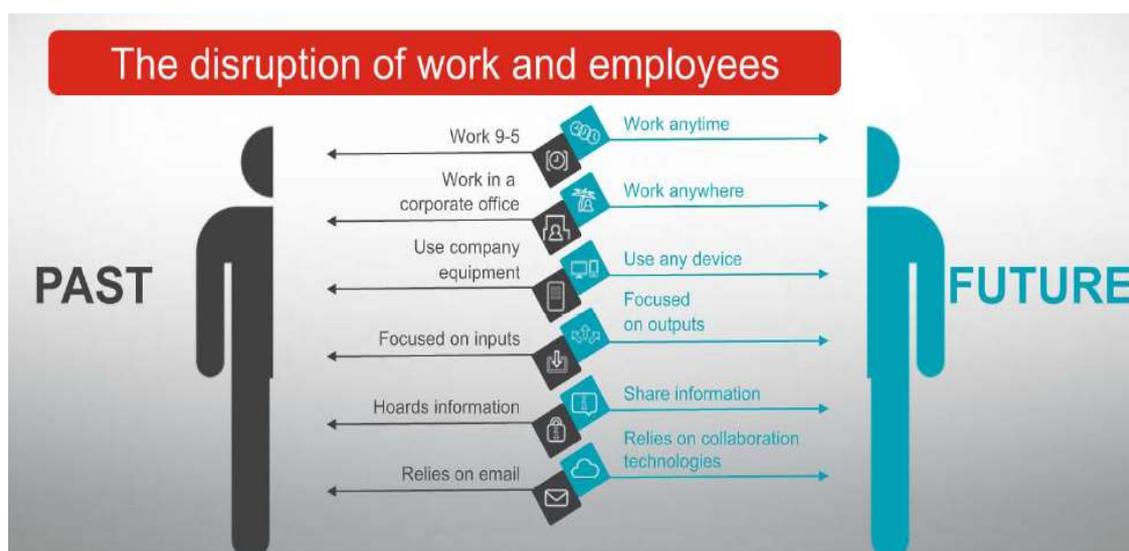
• Je débute toujours mes allocutions en salle par une description du Contexte d'affaires actuel, car pour évoluer l'organisation post-moderne doit tenir compte de l'environnement d'affaires actuel (tant interne, qu'externe) et les tendances d'évolutions prévisibles, tout en connaissant bien ses forces et faiblesses, mais aussi les opportunités et menaces (OM) technologiques et plus largement les OM d'affaires (FFOM ou SWOT).

• Voici quelques éléments de cet environnement externe, qu'il faut considérer, dans le cadre d'une Analyse étendue, genre "BIG PICTURE" :

- Complexification de la société : Enjeux & Défis, de plus en plus interdisciplinaires / Effet temporel / Contexte politique / Mouvement sociétaux (ex : Gilets jaunes), ...
- Environnement ViCA (en anglais VUCA) :  
*Volatilité (vitesse du changement...), Incertitude (pistes possibles d'évolution...), Complexité (interrelations entre les événements...), Ambiguïté (Interprétation des événements...).*
- Après douloureux de la Crise financière de 2008, qui s'est éternisée (2015 + ...).
- Crise des réfugiés, avec plus de 66 M de délocalisés, une première mondiale !
- Menaces terroristes & Cybercrime.
- Rééquilibrage des pouvoirs entre les Nations.
- Concentration de la richesse & Pauvreté persistante dans de grandes régions du monde.
- Pérennité remise en cause : Environnement.
- Projectification grandissante dans la Société (car on fonctionne de plus en plus en mode projet).

### Évolution du monde du travail

• Comme une image vaut mille mots ... (-;-), je vous laisse apprécier celle-ci :



SOURCE : The Future of Work : Attract New Talent, Build Better Leaders, and Create a competitive Organisation / Jacob Morgan 2014 (NOTA : Facilement retrouvable sur Internet, en texte intégral PDF)

## Plusieurs niveaux de Performance à considérer

• La Performance dans le monde du travail est un construit avec ses différents niveaux, un peu comme les poupées russes ou matriochkas, s'emboîtant l'une dans l'autre.

- INDIVIDUEL : La productivité individuelle est le Rendement, qui contribue à la performance individuelle, lorsqu'elle cadre bien avec les objectifs d'affaires ...
- COLLECTIF : Elle se retrouve dans le clan ou groupe, de même que dans les différents types d'équipes de travail, dont les équipes de projet ...
- ORGANISATIONNEL : Plusieurs sous-niveaux sont possibles : unité administrative, filiale ou encore succursale, l'organisation au grand complet, au niveau national ou même à l'international...
- MULTI-ORGANISATIONNEL : Plusieurs organisations de propriétaires différents sont impliquées (cas MANDATAIRE est l'entité qui agit au nom et/ou à la place d'une autre) ...

## Modèle de performance

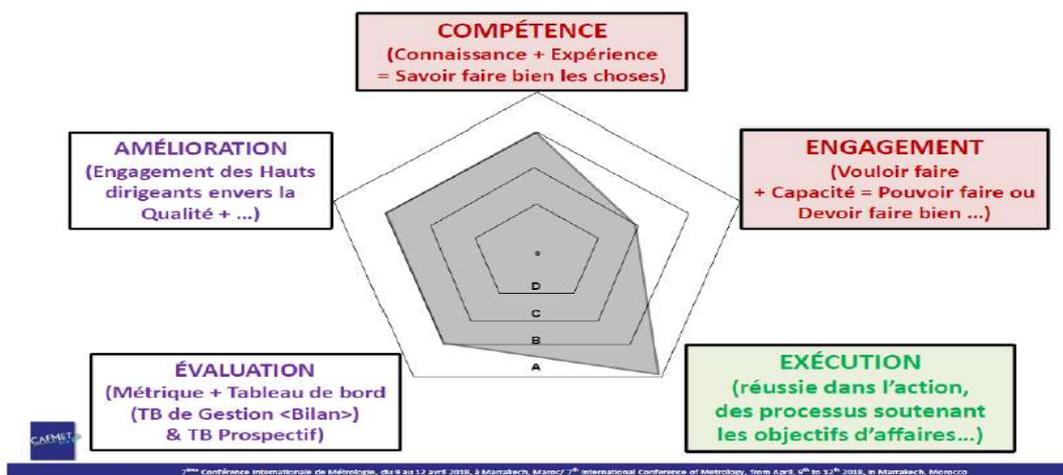
• Il est acquis que la performance organisationnelle est liée à l'atteinte des objectifs d'affaires et des intentions stratégiques (choix des options à privilégier+ manières de faire pour l'exécution + etc.). Bref, ce qui est fait, doit être relié à ce qui était demandé à l'origine par le « Grand patron » ... (-;-)

• J'ai eu l'occasion d'exposer au CAFMET 2018, tenu à Marrakech en avril 2018, un *Modèle innovant de performance*, avec cinq conditions concurrentes.

NOTA : La figure ci-dessous doit être lue dans le sens horaire (aiguilles d'une montre), en partant de midi.

### Modèle de PERFORMANCE – Yvan Lauzon MBA 2018

5 conditions pour générer une performance organisationnelle pérenne



Source : Lauzon, 2018

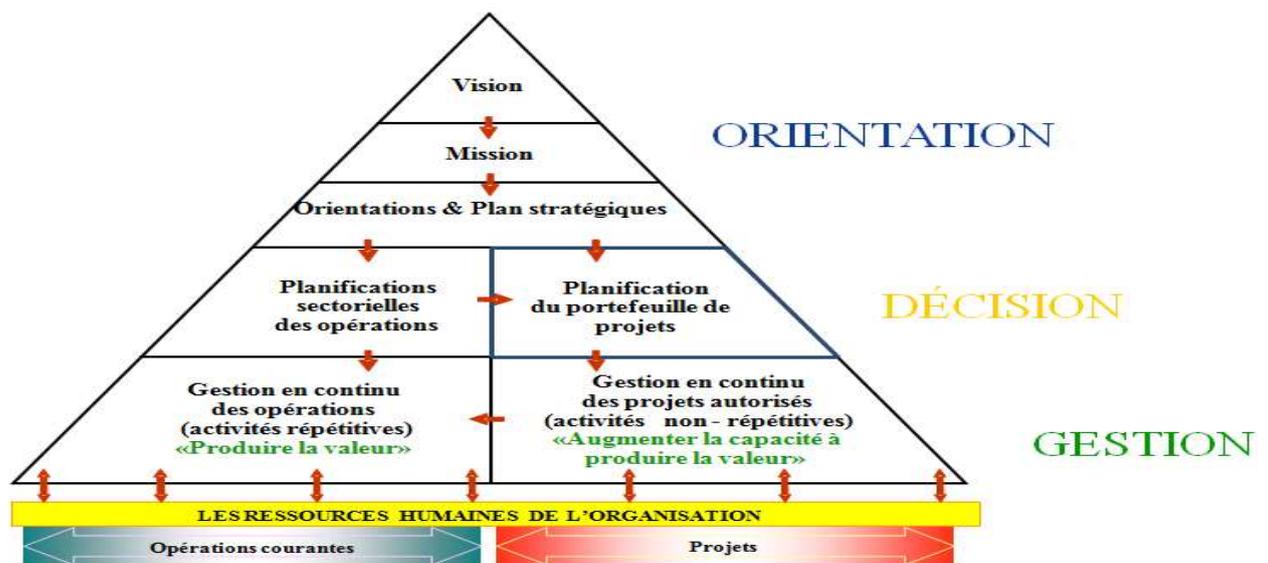
\* \* \*

## SECTION 2 : Activités organisationnelles

• Deux MODES de FONCTIONNEMENT cohabitent dans les organisations depuis le début des pyramides, avec des logiques différentes, ayant chacun des avantages et inconvénients:

\* **Mode des Opérations courantes** –ou– Activités courantes de travail (ex : les Conseillers en ressources humaines agréés, travaillant à la Direction des ressources humaines ou DRH) (ex : les Conseillers en marketing, travaillant à la vice-présidence Marketing), etc.

\* **Mode Projet**



### 2.1 Modes de fonctionnement des organisations : Opérations courantes & Mode Projet

• Naviguant dans un environnement de plus en plus volatil, incertain, complexe et ambigu (V-I-C-A) et dans un contexte de compétition globale et élargie, les organisations n'ont d'autre choix que d'assumer un Leadership accru, en adoptant du même coup de nouvelles façons de faire et des modes de travail éprouvés, comme le Mode Projet, tout en cherchant à être toujours plus performantes.

• En effet, les défis organisationnels sont nombreux et forts imposants : mobiliser leurs employés de 4 ou mêmes 5 générations distinctes de salariés, mieux coordonner les activités courantes de travail et celles reliées aux projets, livrer de façon optimisée des produits et services appréciés, augmenter leur flexibilité organisationnelle, apprendre rapidement et de différentes manières, et innover constamment.

#### Opérations courantes

• La plupart des organisations publiques et privées d'aujourd'hui sont encore organisées par « Fonctions d'affaires », composées d'entités qui se focalisent avant tout sur leurs objectifs propres, plutôt que sur ceux de l'ensemble de l'organisation. Par ex. la DRH s'intéresse d'abord aux objectifs et activités de la DRH, la VP Marketing au marketing, la VP Finance aux ... (vous l'aurez vite deviné !).

- Fortement décriée aujourd’hui, l’organisation par « Fonctions d’affaires » crée souvent de « véritables silos internes ». Cette organisation résulte pourtant de choix organisationnels historiquement fondés, en permettant de dédier des équipes à des enjeux importants, qui visent constamment l’excellence opérationnelle. Ce type d’organisation peut aussi favoriser la responsabilisation et l’implication de ses salariés, en répondant ainsi au besoin d’appartenance à un groupe précis, dont on partage aisément les codes de conduite, les us & coutumes, et la mission.

- Cependant, cette autonomie administrative s’accompagne souvent d’un certain cloisonnement ou « Effet de silos ». L’information circule peu au-delà des frontières du silo, les équipes ne savent pas très bien travailler ensemble, voire agissent parfois en rivales. Cela freine à la fois l’apprentissage et la capacité d’unir ses forces pour innover ou encore pour mener une stratégie d’affaires concertée ... Or ces atouts sont devenus essentiels de nos jours. C’est pourquoi de nombreux dirigeants ressentent le besoin de « Briser les silos », c’est-à-dire de conduire les entités à mieux coopérer & collaborer au service des ambitions partagées.

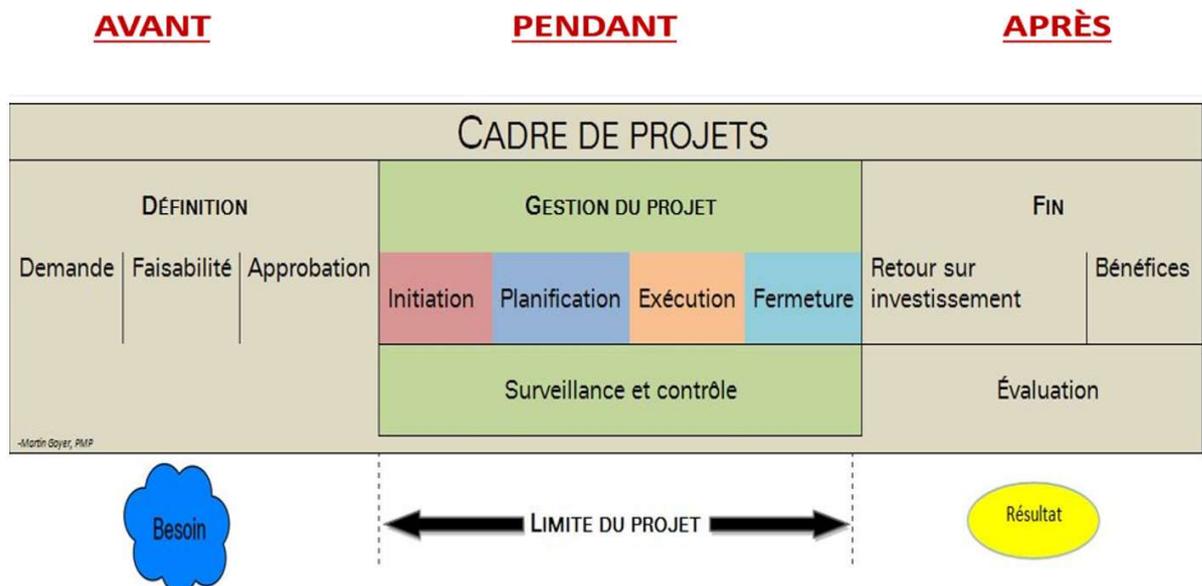
**Mode Projet**

- Le Mode Projet implique toujours la réalisation de projets. Un projet est une initiative temporaire réalisée en vue de créer un produit ou un service unique. Il s’agit donc d’un ensemble de ressources gérées comme un tout unique dans le temps, avec un début et une fin pré-annoncée. (Déf. PMI)

- Dans une organisation d’une certaine taille on retrouve également des Programmes de projets (à ne PAS confondre avec des Programmes de services) et des Portefeuilles de projets. Un Programme de projets est un groupe de projets conduits d’une façon coordonnée, afin d’en obtenir un résultat global que ne permettrait pas un management indépendant de chacun d’eux. Un Portefeuille de projets est un ensemble de projets et/ou de programmes de projets. (Déf. PMI).

- Les gens oublient souvent qu’avant le Projet, d’importantes activités ont eu lieu, notamment la recherche de financement dudit projet.

De même, la clôture du projet n’est pas la fin des activités, notamment dans les organisations publiques ...



Source : Goyer, 2013

## 12 critères d'évaluation des projets

- Dans mes deux plus récents ouvrages portant sur l'Intelligence collective, j'ai décrit douze critères d'évaluation des projets. Je reprends simplement ici la liste de ces critères, car des lacunes en matière de protection de l'information peuvent « faire foirer un projet de bien des façons », comme on dit chez nous!

- Outre les trois critères fondamentaux du **Triangle de fer du PMI**, résumé par **Q-C-D** :

- 1. Portée du Contenu & **Q**ualité
- 2. **C**oût (respect Budget-argent \$)
- 3. **D**élai (respect Budget-temps)

- Par définition (Déf. PMI), un écart négatif de plus de 10% aux prévisions initiales pour chacun de ces trois critères, conduit directement à l'échec de la performance du projet. En clair, le projet est qualifié d'échec. Pourtant la solution d'affaires résultante du projet peut être adéquate, voire même merveilleuse !

Par ex. l'Opéra de Sydney, figure emblématique de la Ville du même nom est un échec de projet bien connu et même indiscutable. Prévision initiale de budget-coût : 7 millions \$ AUD (5 M euros). Fin prévue pour 1963, terminée pourtant en 1973. Eh OUI, 10 ans plus tard, ce n'est pas une erreur typographique... (-)

- Nous pouvons aisément ajouter **neuf autres critères** :

- 4. Satisfaction du Commanditaire et du Maître d'ouvrage (MOA),

*le Commanditaire étant le "Sponsor"; alors que le Maître d'ouvrage est le Donneur d'ordre.*

- 5. Utilité du projet,

*soit le rapport entre les Objectifs initiaux du projet et les Besoins d'affaires (ayant fait naître ledit projet)*

- 6. Cohérence du projet,

*soit le rapport entre les Objectifs fixés et les Moyens affectés au dit projet.*

- 7. Pertinence du projet,

*soit le rapport entre le Besoin exprimé et les Objectifs assignés au Projet.*

- 8. Efficience du projet,

*soit le rapport entre les Moyens mobilisés et les Résultats obtenus.*

- 9. Efficacité du projet,

*soit le rapport entre les Objectifs initiaux du projet et les Résultats obtenus.*

- 10. Adéquation entre Besoins exprimés & Besoins réels,

*bien entendu, la prémisse de base est la Légitimité même du projet, s'appuyant sur des besoins réels)*

- 11. Impacts clients et ceux touchant les principales Parties prenantes (impactées ET impliquées);

*Passons donc de PESTE, en Analyse stratégique, à PESTEL et finalement à PESTELOD)*

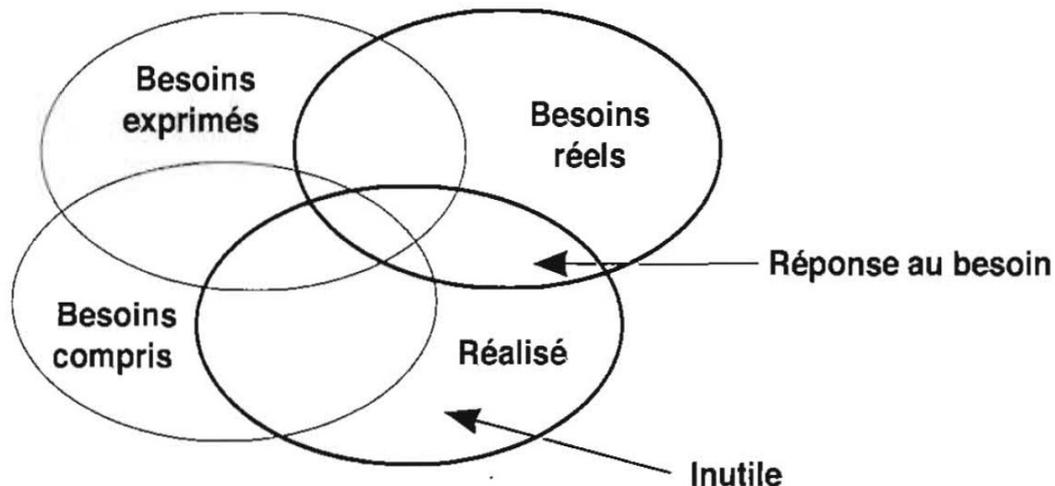
*(PESTELOD = 8 critères d'Analyse complémentaires : Politique / Économique / Social / Technologique / Environnement & développement durable / Légal & éthique / Organisationnel / Démographique)*

- 12. Préparons le futur, via un

*Apprentissage individuel / Apprentissage collectif / Innovation, ...)*

## Adéquation entre Besoins exprimés & Besoins réels : Légitimité du projet

- Lorsqu'on débute un projet on regarde les bénéfices attendus, face aux besoins exprimés, on identifie les grandes étapes, les activités, les livrables, les ressources requises, etc.
- J'aime bien cette figure, qui illustre très bien, que beaucoup d'activités de projet –même bien réalisées– ne serviront tout simplement à rien, car comme dit Peter Drucker, véritable *Gourou du management*:  
« Il n'y a rien de plus inutile que de faire efficacement ce qui ne devrait pas être fait du tout »



Source: ISBN : 978-2212556476.

\* \* \*

## 2.2 Typologie des projets

- Il existe de nombreuses typologies des projets, mais curieusement aucune ne semble poindre à l'horizon dans le cadre d'une norme internationale unique ...
- Voici quelques catégories, qui peuvent se retrouver dans l'une ou l'autre des catégorisations ou typologies retrouvées en entreprise, ou plus simplement sur Internet.
- MAINTENANCE & AMÉLIORATION INCRÉMENTALE (Continuité, encadrement, ...) / NOUVELLE SOLUTION d'AFFAIRES / TECHNOLOGIE NOUVELLE
- SECTEUR & SOUS-SECTEUR INDUSTRIEL (ex : Projet dans le secteur de la Construction) (ex : Projet dans le sous-secteur de la construction d'autoroutes, ...)
- TAILLE (distinction selon Budget-temps / Budget-Coûts / Ressource requise en RH internes & consultants)
- MONO-ORGANISATIONNEL / PLURI-ORGANISATIONNEL / ...
- SIMPLE / COMPLIQUÉ / COMPLEXE / INNOVATION de RUPTURE.

Voici quelques informations sur cette dernière liste :

- Projet simple : On peut prédire l'évolution du phénomène à l'étude, ses enjeux, ses impacts et conséquences probables, etc. Bref, les solutions possibles sont plutôt claires. Les procédures & directives, de même que les activités du projet, sont aussi assez limpides, voire faciles à suivre.  
Par ex : Peinturer votre bureau de 4 pièces.

- Projet compliqué : Forcément moins simple ... (-;-)  
Il faudrait peut-être alors songer à recourir à un (ou des) expert(s) ou spécialiste(s) de domaine.  
Pour comprendre le phénomène ou la situation visée, il est possible de décomposer les problèmes rencontrés, les options, les activités, etc. Par ex : Construire un nouvel avion.
- Projet complexe : Bien entendu, l'intensité de la complexité est plus grande, que dans les projets simples ou compliqués, mais le niveau d'incertitude l'est également, car souvent les projets de ce niveau de complexité font face à plus d'inconnus, que de connus. Les résultats possibles sont difficiles à évaluer, notamment en début de projet. Les comportements sont aussi difficilement prévisibles.
- Innovation de rupture (Disruptive Innovation).
- Il ne faut pas oublier ici le cas des projets chaotiques, voire à la dérive ...

\* \* \*

## 2.3 Chef de projet Leader

- Depuis près de 100 ans, la recherche tente de percer le secret des Leaders d'équipes de travail efficaces en examinant leurs traits de personnalité (par ex : intelligence, dominance, etc.), leurs comportements (ceux centrés sur la tâche, les relations...), l'ajustement du Leadership à la situation réelle, leur capacité de créer un climat de confiance et de servir de modèle à leurs collaborateurs, l'engagement ferme de ces derniers, même en période de stress prolongé ou même de crise, leurs capacités de changement rapide, et finalement, l'exercice d'un leadership compatible avec les projets.
- Les Leaders d'équipes efficaces savent utiliser leurs habilités politiques, comme l'influence interpersonnelle, le réseautage, la finesse sociale et la sincérité perçue. Ils savent également accroître le pouvoir personnel des membres de leurs équipes en créant des conditions gagnantes où le travail en équipe a du sens pour eux, leurs présentent des défis stimulants et importants pour l'organisation, mais qu'ils se sentent capables de relever, en leur laissant une certaine autonomie, mais tout en les encadrant (habilitation psychologique ET habilitation structurelle).
- Ces Leaders d'équipes efficaces savent aussi créer une équipe gagnante, avec des gens qui performant bien ensemble, et ce, notamment lorsque l'intelligence collective est nécessaire pour diagnostiquer, résoudre des problèmes, réfléchir en équipe, concevoir en équipe (co-construction), apprendre en équipe, ou encore, explorer les alternatives en terrain inconnu.
- En réponse à une question d'un apprenant, lors d'une formation en salle, j'ai identifié mon propre choix de onze compétences-clés TOP-NIVEAU des Chefs de projet LEADER, soit ceux qui réussissent mieux que la moyenne des Chefs de projet :

*Adaptabilité / Agréable, sympathique & aidant / Clairvoyant (anticipation correcte) / Convaincant (persuasif) / Courageux dans la prise de décision et l'action Empathique / Discernement / Forte résistance au stress / Le Leadership partagé est accepté, voire favorisé / Sensibilité politique & stratégique / Tolérance à l'ambiguïté.*

- La figure suivante publiée en 2013 par le PMI regroupe des activités de projet, qui sollicitent soit des attributs de compétences techniques / ... de Leadership / ... Stratégiques & Management :



Source: PMI (Project Management Institute) -- New Brunswick Chapter, Canada

- Dès la version 4 française de son corpus des connaissances (Body of Knowledge) en 2008, le PMI identifiait déjà les onze compétences interpersonnelles fondamentales du Chef de projet, face à son équipe de projet les différentes parties prenantes (soit les entités qui participent au projet –ou– qui sont impactées par le projet), soit :

*Accompagnement (Coaching) / Communication / Climat de confiance instauré / Développement de l'esprit d'équipe / Gestion des conflits / Influence / Leadership / Motivation / Négociation / Prise de décision / Sensibilité politique & culturelle.*

- Pour compléter cette liste, voici des attributs de compétences requis en période de Changement :

- **AMBIGUITÉ** tolérée : on avance, même si bien des incertitudes demeurent; espérant que la trajectoire suivie est bonne ...
- **AMBIDEXTRIE** managériale (Exploration & Exploitation, réalisée simultanément).
- **AGILITÉ** (ex: Pour s'adapter / Pour se donner la possibilité de changer d'idée en cours de route / Pour ...).
- **COURAGE** managérial (se dire qu'agir est souvent mieux que le statu quo).
- **COMMUNICATION** : Écoute active / Communication interne / Communication publique.
- **INTELLIGENCE CULTURELLE** : Capacité de comprendre les contextes qui nous sont moins familiers, puis s'y adapter (Early & Mosakowski, 2004), (Hofstede Insights: <https://www.hofstede-insights.com/country-comparison...> ).
- **POLITIQUE** : Habiletés politiques requises pour évoluer dans une organisation dont les règles du jeu ne sont PAS ÉCRITES (par ex: Obtenir rapidement de l'avancement, ne pas se faire virer).
- **STRATÉGIQUE** : Sens inné de l'Alignement stratégique (ex: se sentir guider par une main invisible).

\* \* \*

## 2.4 Confiance : Un prérequis essentiel aux affaires

• Hervé Sérieyx est un auteur, conférencier et un consultant français réputé, qui a travaillé à la fois dans le secteur public et dans les entreprises privées. Dans son ouvrage portant explicitement sur la Confiance, il a dressé une courte liste d'activités du manager qui influent sur la confiance et peut-être même le moral des troupes :

- Cible partagée : Pour donner du sens.
- Cohérence : Faire ce que l'on dit. Ne rien annoncer qui ne sera pas vécu.
- Coopération : Pour que ça marche, il faut que l'on coopère. Ça prend des compétences pointues, mais des liens transversaux pour comprendre les autres.
- Reconnaissance de la compétence : Attirer les talents, puis marier les talents. Il faut créer une organisation apprenante, afin que ceux qui y sont se développent.
- Communication : La vraie communication n'est pas du courriel et du BlackBerry. En fait, on peut tuer une organisation si l'on utilise que ça...
- Créativité : Obligatoire dans un contexte de mondialisation.
- Convivialité : Il faut favoriser une ambiance festive. Il faut de la Rigueur dans l'exécution des processus et de la Chaleur dans le Management.
- Contrat social : Dans la Société on a des droits, mais aussi des devoirs.
- Changement : Toute idée neuve dans la société reçoit une poussée inverse et proportionnelle à sa force (Principe d'Archimède).
- Courage : Afin que les autres n'aient pas peur.

\* \* \*

## SECTION 3 : Données + Informations + Connaissances + Compétences

### 3.1 Définition

• Signalons d'entrée de jeu que les 5 niveaux --ou couches-- sont requises et déjà présentes dans la plupart des organisations publiques ou privées.

• Voici certaines précisions terminologiques et autres particularités pouvant alimenter un certain continuum de complexité ou peut-être même un certain idéal recherché : D-I-C-C-S.

• Données (Data)

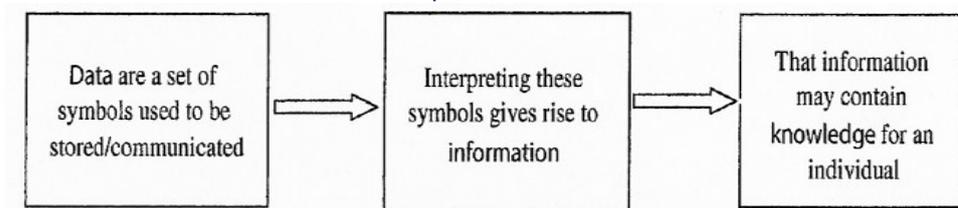
- Faits bruts (souvent quantitatifs) résultant d'une observation ou d'une mesure.
- Concerne surtout « le Quoi » ...

• Informations (Information)

- "Usefull Data"
- Agrégation de données en vue de transmettre un message.
- Ensemble de Données, construites en fonction de règles, nécessitant : Intermédiation humaine / Signification consensuelle / etc.
- Concerne surtout « le Comment » ...

• Connaissances (Knowledge)

- Informations à forte valeur ajoutée, nécessitant une expertise humaine pour assurer : Compréhension des relations entre les composantes / Compréhension des modèles / ...
- Concerne surtout « le Pourquoi » ...



• Compétences (Competencies / Skills)

- Savoir + Savoir-faire + Savoir-être + ...
- Capacité reconnue dans ... une matière & qui donne le droit d'en juger (Petit Larousse).
- Compréhension des connaissances contextualisées pour : Décisions pertinentes & Actions efficaces, donc allant souvent bien au-delà d'une simple capacité théorique ...

• Sagesse (Wisdom of Knowledge)

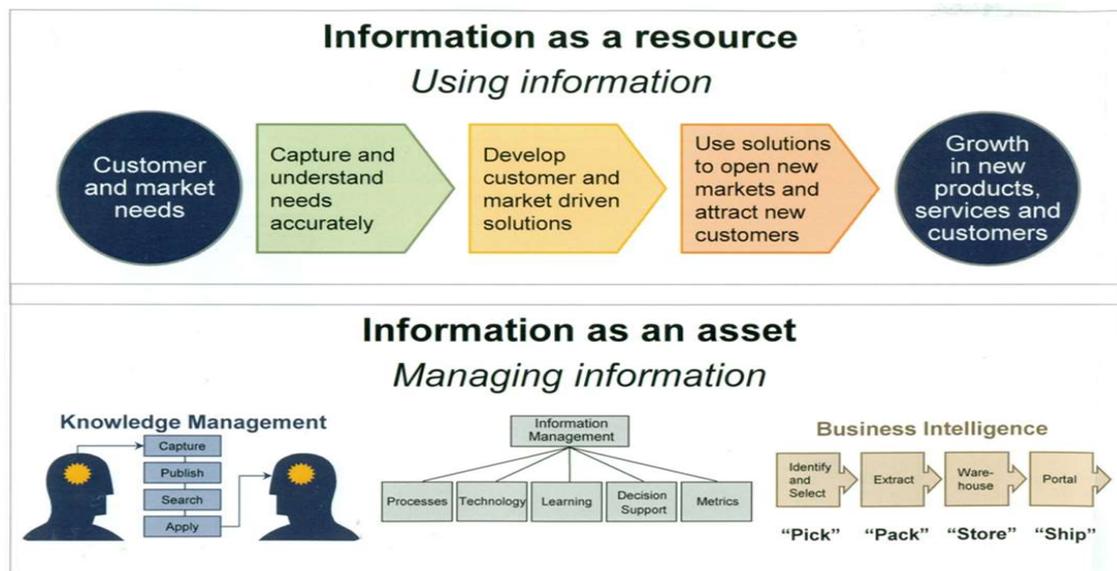
- Capacité à bien agir, acquise par Anticipation & Répétition des actes.
- Compréhension claire des Principes sus-jacents applicables à la situation réelle ...

\* \* \*

### 3.2 Actifs informationnels & Ressources informationnelles

• Le Tableau ci-dessous de GARTNER (2006) permet de distinguer visuellement et rapidement « l'information comme Actifs informationnels » –et d'autre part– « l'information comme Ressources informationnelles ».

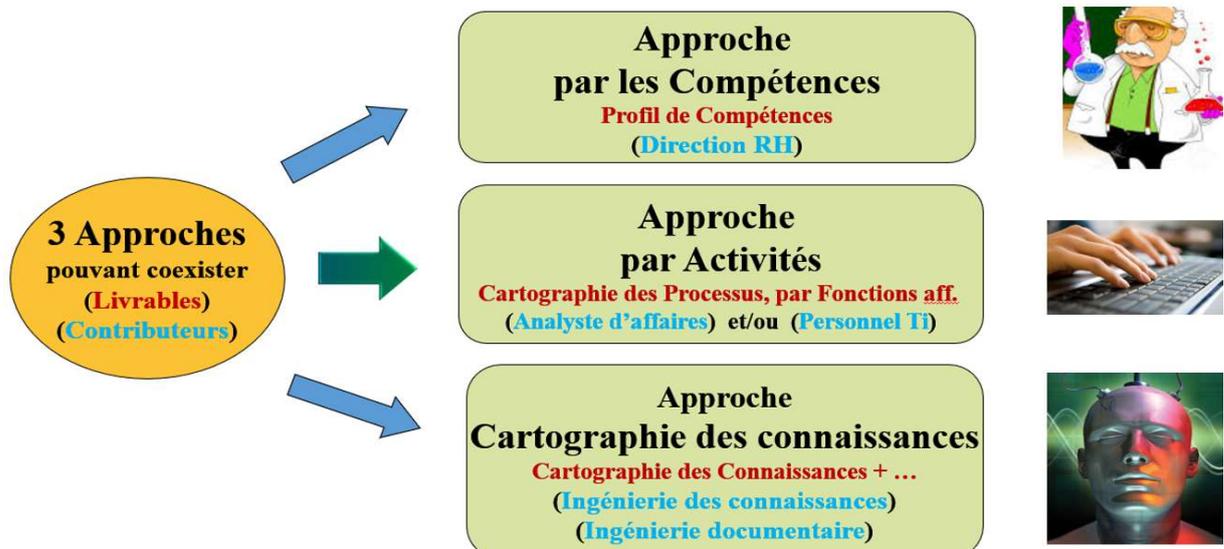
- Un Actif informationnel, tel un actif (asset) en bourse, est sujet à créer de la valeur ajoutée.
- L'information est l'une des quatre principales ressources de l'organisation post-moderne, soit : Financières (RF) + Humaines (RH) + Matérielles (RM) + Informationnelles (Ri) ...



Source : Gartner (2006) « EXP » Réutilisation, avec permission, 2008.

### Approches organisationnelles complémentaires

- Les Données-Informations-Connaissances (D-i-C) de l'organisation publique ou privée sont traités par trois grandes approches qui coexistent et qui interpellent des professionnels distincts.



Source : Lauzon Y., 2014; RFQM 2019

\* \* \*

### 3.3 Propriétés & Typologies d'information

#### Propriétés de l'information

- Voici une liste non exhaustive :
  - Accessible / Disponible
  - Authenticité
  - À jour
  - À temps (au bon moment)
  - Confidentialité
  - Compréhensibilité
  - Concision requise pour les Hauts dirigeants, mais aussi pour certains Gestionnaires (Managers) ...
  - Complète
  - Intégrité
  - Normalisée (Standardisée) ou non
  - Pérenne
  - Pertinence
  - de Qualité
  - Traçabilité
- Avec le bon niveau de précision (selon attentes du récepteur, réglementation, etc.)
- Avec le bon niveau de détail, incluant :
  - Granularité
  - Si agrégée, le niveau de détail est tout de même conservé
  - Source (Primaire / Secondaire), autre métadonnées ...

#### Typologies d'information

- Tout d'abord, deux grands types de connaissances, pouvant être schématisés sous la forme d'un iceberg, coexistent dans toutes les organisations post-modernes :
- Connaissances Tacites (ex : savoir-faire) : Trucs que l'on sait faire, mais que l'on est souvent incapable d'expliquer facilement comment le faire. Par ex : un musicien de Jazz qui joue bien, mais sans feuille de musique, ni démarche formalisée. Ces connaissances correspondent à la partie non visible de l'iceberg, donc la plus imposante.
- Connaissances Explicites : Savoirs documentés prenant la forme, par exemple, de déclarations, règles et procédures, etc., qui sont ensuite mises à disposition dans un recueil de connaissances ou dans un système informatique de KM, afin d'être exploitées et valorisées par d'autres collaborateurs. Ce type de connaissances représente la partie visible de l'iceberg.
- Bien entendu, outre ces distinctions entre connaissance « Tacite / Explicite » il existe également d'autres catégorisations possibles pour les connaissances retrouvées dans nos organisations post-modernes :
  - Individuelle / Collective (Groupe ou Équipe) / Organisationnelle.
  - Blanche / Grise / Noire (\*)
  - Interne / Externe à l'organisation.
  - Individuelle / Collective / Organisationnelle // (Micro / Méso / Macro).

- Cruciale & Non cruciale (\*\*)
- Confidentielle / Partagée / Publique.
- De base (Core) / Avancée / (Advance) / Innovatrice (Innovative) (\*\*\*)
- Essentielle & Non essentielle.
- Stratégique / Tactique / Opérationnelle.
- Tacite « Implicite » / Explicite.
- Utile / Peu utile / Inutile.
- Valeur VRiN (\*\*\*\*) / Peu de valeur / Sans valeur.

NOTA : La Norme française XP50-053 donne plusieurs définitions sur ces différents types d'information.

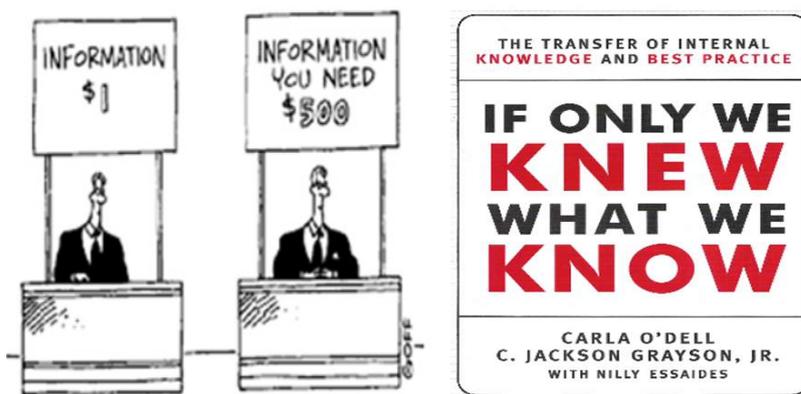
(\*): « Blanche = Facile à trouver », « Grise = plus difficile à trouver », « Noire = espionnage ou usage illégal »

(\*\*): Crucialité = Criticité de la tâche X Dépendance à la compétence d'une personne (ou quelques personnes) déjà dans l'organisation ou facilement accessibles à l'organisation.

(\*\*\*): (i) Connaissance de base (Core Knowledge) est celle qui est requise par toutes les entreprises d'une industrie, mais elle est souvent une barrière à l'entrée pour un nouvel entrant (firme) dans un marché. Ce type de connaissance n'apporte pas vraiment un avantage concurrentiel à long terme, mais il est indispensable pour survivre à court terme. Par ex. Savoir requis pour faire un produit alimentaire, que toutes les entreprises du secteur détiennent. (ii) Connaissance avancée (Advanced Knowledge) permet à la firme de maintenir sa position concurrentielle, face aux autres firmes du secteur. Cette connaissance découle d'une stratégie avouée où l'on tente d'en savoir toujours plus que ses compétiteurs. (iii) Connaissance innovatrice (Innovative Knowledge) permet d'assurer un certain Leadership de l'industrie en dictant maintenant les règles du jeu.

(\*\*\*\*) VRiN = avoir en soi de la Valeur– Rare – Inimitable – Non substituable).

• Cette caricature, de même que cette couverture de livres KM, valent bien mille mots ... chacune, me servant aussi de « Mot de la fin », pour la présente section (-)



\* \* \*

## **SECTION 4 : Approche intégrée couvrant 7 domaines de Management (GSA5) & 4 domaines de Normativité (MED2)**

- Chacun des onze domaines ci-dessous impliquent des professionnels distincts, avec un esprit critique (\*) plus ou moins développés, pouvant être sollicités au gré des événements et circonstances.
- Ces professionnels se sont dotés progressivement entre eux d'un vocabulaire distinct (créant ainsi des chapelles de communication), de corpus de connaissance ou *Body of Knowledge* ou *BoK* (à ne pas confondre avec Book) et/ou des méthodologies et référentiels de meilleures pratiques (Best practices) distincts.
- Mais les Applications numériques actuelles (ex: COFFRE-FORT numérique) obligent de plus en plus l'interdisciplinarité professionnelles et le décloisonnement des « SILOS externes ».
- L'organisation post-moderne doit ouvrir ses portes, mais aussi ses yeux et ses oreilles, façon de parler ... (;-), pour détecter les signaux faibles de l'environnement, décider d'agir et passer rapidement à l'action. Oubliez la réunionite et la bureaucratie excessive ... PARTICIPACTION... (;-)
- Sept domaines de Management (GSA5), qui sont gérables en impliquant des spécialistes utilisant notamment de bonnes pratiques, vous sont présentés dans les prochaines pages :

**GS**, pour: • Gouvernance  
• Sécurité

Puis **A5**: • Accès à l'information  
• Architecture  
• Assurance  
• Audit  
• Archivistique

Puis, quatre domaines de Normativité (**MED2**), qui sont sujets à interprétation par des spécialistes internes ou externes (ex : consultants), suivront :

- Morale
- Éthique
- Déontologie
- Droit

(\*): «*Esprit critique* » désigne ici un «*Esprit qui n'accepte aucune assertion sans contrôler la valeur de son contenu et son origine*». (in *Le scepticisme, l'esprit critique est l'aristocratie de l'intelligence*, Edmon & Jules de Goncourt, Journal, 1861, p. 963).

\* \* \*

### **4.1 Gouvernance**

- La Gouvernance corporative est d'abord l'*Art de bien gérer*, en mettant en place une Structure décisionnelle (ex : Conseil d'administration, Comité de direction CODIR, autres Comités thématiques, Règles de décision, Modes de représentation, etc.) permettant d'identifier les Opportunités et de contenir et maîtriser

les Menaces & Risques. Ceci est vrai au niveau sociétal, partenarial, organisationnel et même fonctionnel (par ex: la fonction d'affaire Gestion des ressources humaines ou GRH), etc.

- Outre cette Structure décisionnelle, la Gouvernance s'intéresse aussi à l'Arbitrage de valeurs (ex : entre les intérêts & les attentes variés des parties prenantes), la Prise formelle de décision (ex : savoir trancher judicieusement et rendre la décision acceptable ...), mais aussi le Pilotage de la création de valeur ; ce qui implique de s'adapter aux circonstances, en tout temps.

- On assiste actuellement à un certain engouement médiatique pour la Gouvernance d'entreprise, notamment au Québec depuis cinq ans. Bien entendu, plusieurs intervenants s'accordent pour dire que celle-ci doit être reconjuguée au présent, d'où l'expression « Gouvernance d'entreprise renouvelée », ceci afin de prendre en compte les valeurs sociétales dominantes & évolutives, maintenant véhiculées plus largement, rapidement et facilement par les technologies (TIC), notamment via les réseaux sociaux.

- Outre la Gouvernance corporative, ou Gouvernance d'entreprise, il existe aussi la Gouvernance des technologies de l'information (une des grandes fonctions de l'organisation publique ou privée) et la Gouvernance sociétale.

- De facto, la Gouvernance d'entreprise renouvelée est pluri-niveaux: La Société / Entreprise / Unité d'affaires stratégique (DAS). En effet, si la Gouvernance du niveau supérieur est compromise, les difficultés des niveaux inférieurs apparaissent assez rapidement, un peu comme un « effet domino ».

- En ce qui concerne la Gouvernance sociétale, prenons par exemple les paradis fiscaux, qui sont maintenant décriés dans les médias traditionnels. Ne soyons pas dupes, ceux-ci n'ont jamais été perçus positivement et acceptés par la population. En fait, il ne faut jamais confondre consentement tacite avec tolérance par ignorance ou encore l'incapacité d'agir. Qui plus est, l'information véhiculée par les médias traditionnels, puis depuis 2006 par les médias sociaux, est à tout le moins partielle et parfois même partielle.

- Ainsi, on retrouve le même phénomène avec les incivilités en entreprise (harcèlement moral, harcèlement sexuel) où la dénonciation est encore trop souvent rarissime, voire même tabou.

### **Analogie de la peinture**

- Pour moi, la Gouvernance corporative serait la couche de fond, qui servirait à faire coller tout le reste dans l'organisation publique ou privée. Si ça ne va pas bien de ce côté-là, le bateau risque de prendre l'eau à plusieurs endroits, comme on dit ... (-)

- Car la Gouvernance corporative devrait d'abord servir à créer de la valeur plus pérenne aux différentes parties prenantes (PP), en impliquant toujours mieux les différents acteurs de l'organisation.

\* \* \*

## 4.2 Sécurité

### La sécurité ne date pas d'hier

- Eh oui, la sécurité est une préoccupation bien réelle depuis les premières formes de civilisation humaine. Il y a 6000 ans on sécurisait déjà les villages pour protéger nos populations, mais aussi pour réduire les risques de crises alimentaires.
- En mandarin, le mot Crise (Weiji) serait d'ailleurs la fusion de deux concepts : Danger (Wei) & Opportunité (Ji).



- Bien entendu, la mise en place des moyens de protection évolue, de manière ponctuelle ou itérative, au fil des incidents & brèches. On n'a qu'à penser aux serrures pour s'en convaincre ...



### Questions importantes de sécurité

- Voici des questions importantes, qu'il faut se poser dans nos organisations publiques ou privées :
  - Q1) Protéger quoi ? & Pourquoi ?
  - Q2) Quels sont les risques ? & Quels sont les Mesures à prendre & Moyens d'atténuation (mitigation) des risques, pour assurer la continuité des opérations ?
  - Q3) Quel est le maillon faible de la chaîne, même après la mise en place de ces Mesures & Moyens (car souvent des risques demeurent, appelés « risques résiduels ») ?  
Et puis, si l'on parlait de votre degré de sensibilité au risque (ou tolérance au Risque) ...
- Et dans toutes vos réponses, prière de ne pas oublier de bien considérer les éléments suivants :
  - Continuité des activités principales / Bonne compréhension & Engagement réel des personnes / Innovations technologiques / Interaction personne-machine / Périodes plus risquées / Sécurité & Droit / Sécurité des personnes / Sécurité logicielle & réseau / Sécurité matérielle ...

## Normes

- J'ai été longtemps membre de la *Commission canadienne auprès de l'ISO*, de même qu'Expert-conseil de niveau *Rapporteur thématique* dans le *Groupe de facilitation des procédures du Commerce international des Nations-Unies* (ONU-CEFACT-WP4), de 1993-03 à 1996-09. Ces expériences furent très enrichissantes, axées sur une contribution internationale bénévole, pour ce qui est des heures travaillées le soir et les week-ends.

- Une norme est :

*« Un accord documenté, contenant des spécifications techniques ou autres critères précis, destinés à être utilisés systématiquement en tant que règles, lignes directrices ou définitions de caractéristiques, pour assurer que les matériaux, produits, processus et services sont aptes à leur emploi ».*

- Plusieurs voient dans la normalisation, qu'un aspect technique et/ou une démarche procédurale. ERREUR !

Une norme est aussi une « barrière à l'entrée » dans un marché économique donné, pour l'entité qui n'est pas encore reconnue, comme étant conforme à la norme.

En fait, une norme peut donc s'avérer être une Arme économique, à effets structurants.

- En clair, si vos fournisseurs locaux, régionaux ou nationaux ne sont pas conformes à la nouvelle norme actuellement en vigueur *de facto* requise, alors que les fournisseurs hors-frontières le sont; alors ces derniers débarqueront rapidement pour vous aider à répondre aux besoins exprimés dans votre *Cahier des charges*.

- L'exemple qui me vient en tête est le passage ultra rapide d'une norme britannique en sécurité des ressources informationnelles (BS 7799), qui est devenue en un temps record une norme internationale (ISO 17799) grâce au mode Fast Track de l'ISO et au fait que la délégation britannique a été très aidante pour inviter les pays africains surtout anglophones à aller voter dans les instances de normalisations (ex : sous-groupes techniques).

Mais pourquoi au juste, me direz-vous ?

Est-ce pour aider à l'évolution de la jeune science informatique ? ...

Mais, bon dieu, réveillez-vous ! (-)

C'est plutôt pour s'assurer que les entreprises britanniques, mais aussi celles de leurs principaux pays partenaires, puissent passer rapidement en « Pôle position » dans le marché mondial de la sécurité informatique.

C'est naturel, puisque c'est l'argent qui mène le monde, direz-vous ... (-)

- Mais la normalisation a tout de même des fonctions régulatrices fondamentales en guidant les fonctionnalités, les usages, les niveaux de qualité, ... de presque tout ce qui nous entoure aujourd'hui.

- En effet, la normalisation a plusieurs utilités fondamentales comme:
  - Définir un vocabulaire & Langage commun, facilitant ainsi la collaboration (faire ensemble), la compréhension mutuelle et le dialogue constructif (évitant notamment l'incompréhension, bien exprimée dans le phénomène mythique de la Tour de Babel).
  - Mieux connaître & Partager les principes & règles, afin de les mettre en application correctement.
  - Donner confiance aux clients, aux prescripteurs et à toutes autres parties prenantes.
  - Développer des marchés plus ouverts aux produits et services.
  - Interopérabilité, est plus facile à assurer.
  - Mettre en Conformité juridique (Lois, Règlements, Normes).

En clair, certaines dispositions qui pourraient être incluses directement dans un contrat, se retrouve plutôt dans une norme explicitement nommée, à laquelle on se réfère.  
 (NOTA : ne pas confondre ici avec l'importante notion < incorporation par référence >, qui est illégale dans certaines juridictions de la francophonie).

  - Qualité, est plus facile à valider.
  - Sécurité, est plus facile à assurer.
  - Réduit les Risques & Impacts environnementaux.
  - Conforte les choix stratégiques des Organisations publiques, parapublics ou privées.
  - Favorise l'élaboration d'outils de mesure (métrologie, ...), de bonnes pratiques (Best practice) et de méthodologie
  - Facilite le transfert de technologies.

### **Normes internationales**

- Le système de normalisation internationale repose sur quelques niveaux :
  - International (ex : l'Organisation internationale de normalisation ISO).
  - des associations nationales, (Ex : ACNOR (CSA) au Canada, ANSI aux États-Unis, DIN en Allemagne...).
  - des organisations gouvernementales.
  - des organisations non gouvernementales (ONG).
  - des professionnels (Accréditation, Certification).
  - des intervenants sectoriels reconnus dans leur milieu, ...
- Les Principes d'élaboration d'une norme internationale (ISO) sont faciles à comprendre : Approche par consensus, travail via des Groupes de travail (par ex : SC7, ...), qui échangent, collaborent et parfois débattent vigoureusement, parfois pour des éléments de natures techniques ou procédurales, mais souvent pour des questions économiques, notamment à cause du phénomène de barrière à l'entrée évoqué ci-haut ... Bref, on parle encore ici de fric !
- Parmi les avantages d'une norme internationale (par ex. : ISO), mentionnons :
  - Organisme international, mais non gouvernemental.
  - Pratiques aguerries dans l'établissement de normes internationales, gage de qualité.
  - Participation des consommateurs, des entreprises et des gouvernements, gage de crédibilité.
  - Organisation avantageusement connue du secteur privé, gage d'intérêt et d'adhésion
  - Solution peu coûteuse à l'échelle internationale, surtout pour les petits pays.
- Voici brièvement la Démarche d'élaboration (cycle) d'une norme internationale (ISO) :
  - Étude de faisabilité.

- Document préliminaire.
- Formation du Comité de normalisation.
- Étude en comité et recherche de consensus.
- Révision & Correction linguistiques.
- Enquête publique.
- Vote final.
- Étude de 2e niveau (norme nationale).
- Approbation, publication et diffusion.

• Parmi les critères d'évaluation ou caractéristiques fondamentales d'une norme, citons :

- Objectives & Vérifiables.
- Publiques.
- Justes.
- Crédibles.

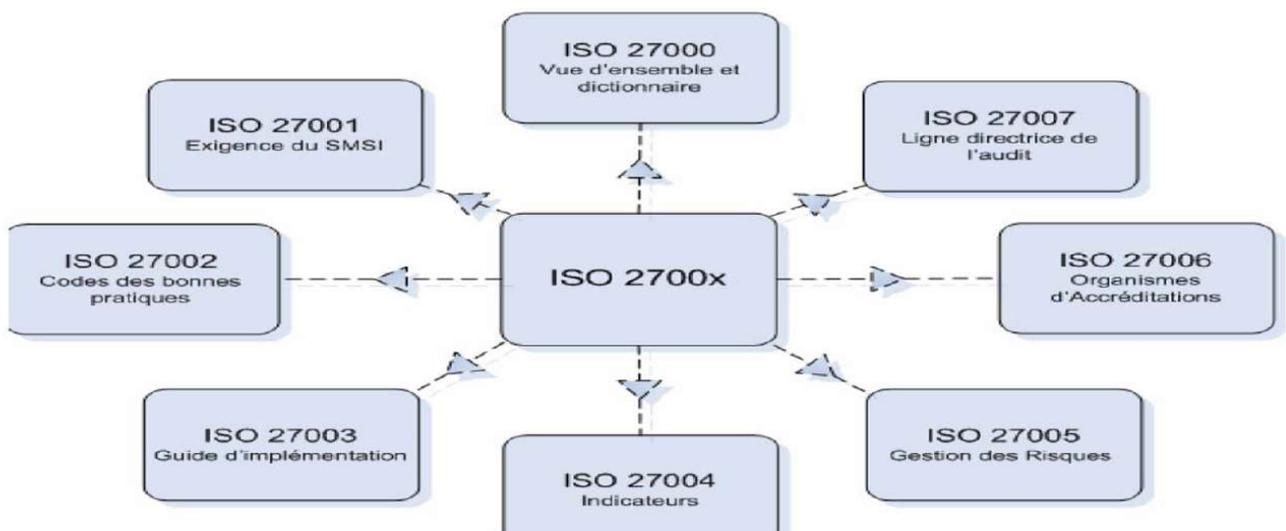
### Normes ISO de Protection de l'information

• Lorsqu'on parle de Protection de l'information, on retrouve plusieurs familles de normes ISO :

- ISO 9001 : 2008 – Système de management de la qualité.
- ISO 14001 : 2004 – Système de management environnemental.
- ISO 27001 : 2005 – Système de management de la sécurité de l'information (SMSI).
- ISO 28000 : 2007 – Spécifications pour les systèmes de management de la sûreté pour la chaîne d'approvisionnement.
- ISO 34001 : 2013 – Système de management de la sûreté.

• Une famille de normes se décline ensuite en une norme fondamentale avec ses annexes ou encore quelques normes portant sur un même thème. Par ex. pour la famille ISO-27000 relative au management de la sécurité de l'information :

#### FAMILLE des NORMES ISO-27000



Source : Université de Sherbrooke, 2011

## Normes nationales

- Une organisation de normalisation d'un pays (ex : AFNOR pour la France), génère et/ou adopte des normes pour ses besoins nationaux ou régionaux, qui peuvent éventuellement devenir des normes internationales, genre ISO. Mais, l'inverse est aussi vrai. Une norme ISO peut être reprise dans le cadre d'une norme française.
- Au Canada, on retrouve quatre principales entités rédactrices et/ou émettrices de normes, soit : ACNOR (CSA) / BNQ (Bureau de normalisation du Québec) / ONGC (Gouvernement du Canada) / ULC.

## Standards des Secteurs industriels

- Outre les normes internationales et nationales, il y a aussi des standards de secteurs industriels (ou quasi-normes), qui ne sont pas écrits ou proposés formellement par des entités rédactrices et/ou émettrices de normes (dont c'est le travail à temps complet).

*NOTE : Le mot standard ici a un signifiant différent, plus restreint, que la simple traduction du mot norme.*

- Par exemple, dans le secteur de la finance on retrouve notamment :
  - Financial Compliance & Disclosure : NI 52-109 (Conformité financière)
  - PCI-DSS (Paielement par carte à puce)
  - Sarbanes-Oxley 404 (Conformité financière & TiC)
- En terminant ce thème de la normalisation, mentionnons qu'outre les normes et quasi-normes (soit les standards des secteurs industriels particuliers, par ex.: IETF, pour l'industrie de l'Internet), il y a aussi le cas des <normes propriétaires> proposées par les entreprises (Apple, Microsoft, Oracle...).

## Principes fondamentaux de Sécurité

- La norme ISO sur les Codes de pratique en matière de management de la sécurité de l'information (ISO 27002) présente onze principes fondamentaux :

### 11 PRINCIPES de la NORME 27002

- 1 : **La politique de sécurité** : pour exprimer l'engagement de la direction à la sécurité.
- 2 : **L'organisation de la sécurité** : pour définir les responsabilités de l'équipe de gestion de la sécurité de l'information au sein de l'entité.
- 3 : **La classification et le contrôle** du « portefeuille informationnel » : pour maintenir un niveau de protection approprié au patrimoine informationnel de l'entité.
- 4 : **La sécurité et les ressources humaines** : pour réduire les risques d'origine humaine, de vol, de fraude ou d'utilisation abusive, notamment par la formation des utilisateurs.
- 5 : **La gestion des incidents liés à la sécurité** : pour garantir que le mode de notification des événements liés à la sécurité de l'information est efficace et efficace.
- 6 : **La sécurité physique et environnementale** : pour prévenir les accès non autorisés aux locaux, aux actifs informationnels, aux informations de l'entité ainsi que les dommages, les perturbations, et la compromission de ces locaux.
- 7 : **La gestion de l'exploitation et des télécommunications** : pour assurer le fonctionnement adéquat des télécoms, et minimiser les risques qui y sont associés.
- 8 : **Les contrôles d'accès** : pour maîtriser les accès au patrimoine informationnel.
- 9 : **L'acquisition, le développement et la maintenance des systèmes** : pour que la sécurité soit une part intégrante dès l'acquisition, le développement et la maintenance des systèmes d'information, ceci dès les phases de spécification et de conception.
- 10 : **La gestion de la continuité d'activité** : pour parer aux interruptions des activités en cas de sinistres impactant le système d'information.
- 11 : **La conformité à la réglementation** interne et externe : pour éviter les infractions de nature légale, réglementaire ou contractuelle.

Source : Université de Sherbrooke, 2011

- Voici les *Lignes directrices de l'OCDE régissant la sécurité des Systèmes & Réseaux d'information* :

**1. Sensibilisation**

Les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité.

**2. Responsabilité**

Les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information.

**3. Réaction**

Les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité.

**4. Éthique**

Les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes.

**5. Démocratie**

La sécurité des systèmes et réseaux d'information doit être compatible

avec les valeurs fondamentales d'une société démocratique.

**6. Évaluation des risques**

Les parties prenantes doivent procéder à des évaluations des risques.

**7. Conception et mise en œuvre de la sécurité**

Les parties prenantes doivent intégrer la sécurité en tant qu'un élément essentiel des systèmes et réseaux d'information.

**8. Gestion de la sécurité**

Les parties prenantes doivent adopter une approche globale de la gestion de la sécurité.

**9. Réévaluation**

Les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité.

**Important de ne pas confondre**

- Il est très important de ne pas confondre les éléments suivants :

MENACE (Élément négatif)  
 RISQUE (Probabilité de réalisation d'un écart négatif –ou positif – à la prévision)  
 VULNÉRABILITÉ (Exposition au risque ...)  
 IMPACT (Conséquence ...)

- Voici quelques exemples de vulnérabilités organisationnelles.

Type de vulnérabilité	Exemple
1. Matériel informatique	Manque d'entretien
	Portabilité
2. Logiciel	Absence d'enregistrement des logs
	Interfaces de saisie compliquées
3. Réseau	Absence de chiffrement des transferts
	Point unique d'accès
4. Personnel	Formation insuffisante
	Manque d'encadrement
5. Localisation (lieu)	Système électrique instable
	Site en zone inondable
6. Structure organisationnelle	Absence de séparation de tâches
	Absence de description de tâches

## Méthode harmonisée d'Analyse de risque (MEHARI)

- En ce qui a trait au risque, la Méthode Harmonisée d'Analyses de Risque (MEHARI) est une méthode bien utilisée au Québec, notamment dans les organisations publiques. Elle a été développée dès 1996 par le CLUSIF (Club de la Sécurité informatique de France). D'ailleurs, le CLUSIF indique sur son site (<https://clusif.fr/mehari/...>), qu'il a établi en 2015 un partenariat avec le CLUSIQ.

- D'ailleurs, on y retrouve sur ce site :

### « Positionnement et principe de base de Méhari »

Le domaine visé par MEHARI est celui de la sécurité de l'information, englobant les systèmes informatisés mais aussi l'information sous toutes ses formes, numériques, analogiques, écrites, etc.

Dans ce domaine, l'objectif de Méhari n'est pas seulement d'identifier les situations de risque et d'en apprécier le niveau, mais de mettre en évidence les mesures permettant de ramener les risques à un niveau acceptable.

Au-delà de la nature des mesures à mettre en œuvre, Méhari s'attache en outre à en définir le niveau de qualité et d'efficacité requis.

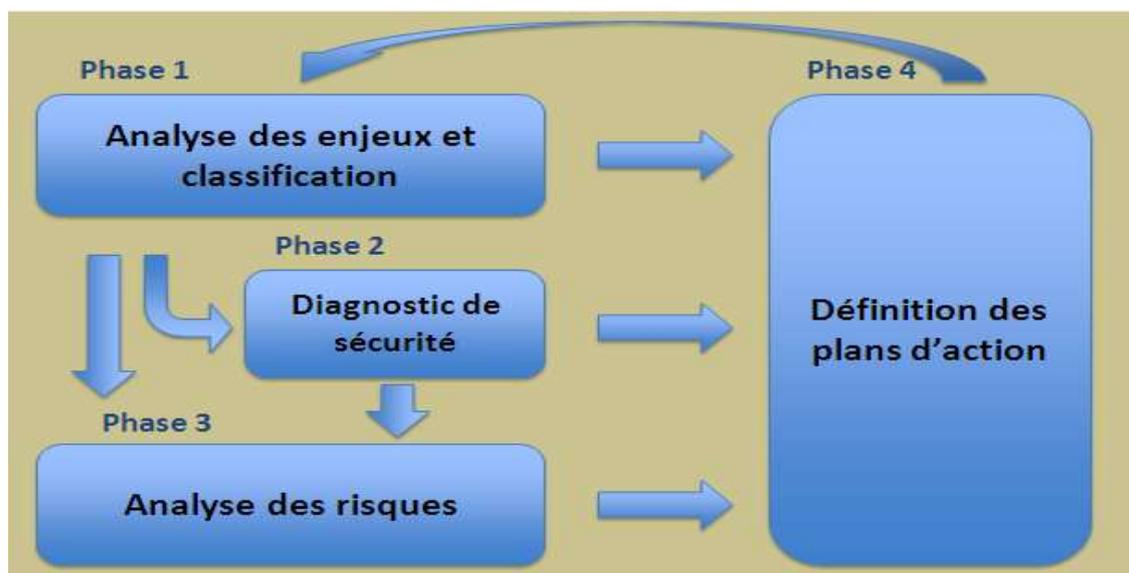
Enfin, Tous les modules de Méhari sont fondés sur un principe de base qui est de ne jamais sous-évaluer un risque et qui se décline de deux manières :

Toujours envisager le pire en termes de conséquences

Ne tenir compte que des effets « contrôlés » des mesures de sécurité ».

Source:<http://www.clusiq.ca/les-fondamentaux-de-la-demarche/#1500889591497-06ae37b1-7350...>

- La figure ci-dessous identifie les quatre phases de la Méthode :



\* \* \*

### 4.3 Accès à l'information & Protection de la vie privée

#### Contexte

• Nous allons maintenant traiter de l'ACCÈS à l'INFORMATION & PROTECTION de la VIE PRIVÉE (**AIPVP**), en couvrant notamment :

- Données personnelles & Renseignements personnels.
  - Distinctions : Protection des renseignements personnels –VS– Protection de la Vie privée.
  - Principes AIPVP.
  - Niveaux de préjudice : Individuel / Organisationnel / Pluri-Organisationnel (ex: Partenarial).
- D'entrée de jeu, je vous invite dans vos réflexions sur ce thème structurant à porter une attention très spéciale :
- À la juridiction applicable (par ex: Union Européenne / Votre pays / Votre région ou province / ...).
  - Au Consentement cumulatif.
  - À la Protection tout au long du Cycle de vie de l'information (voir diapo suivante).

• En France, la CNIL ou Commission nationale de l'informatique et des libertés, créée dès 1978, fait un travail remarquable en matière d'AIPVP. Comme le souligne Wikipedia, la CNIL ... :

« ... est une autorité administrative indépendante française. La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Elle exerce ses missions conformément à la loi no 78-17 du 6 janvier 1978 modifiée le 6 août 2004 ».

• En Belgique, la CPVP (ou Commission pour la protection de la vie privée) a pour principale mission de veiller au respect de la vie privée des citoyens et notamment à la protection de leurs données à caractère personnel. Créée en 1992, la CPVP a vu évoluer son rôle en 2017-2018, face au nouveau cadre législatif en matière de protection des données ou RGDP (NOTE : décrit à la page suivante) se voyant dotée d'importants pouvoirs en terme non seulement d'enquête et de contrôle mais aussi de sanction.

• Au Canada, le gouvernement fédéral s'y active via le *Commissariat à la protection de la vie privée du Canada* (<https://www.priv.gc.ca/fr/...>) et quelques provinces sont plus impliquées ou proactives dans leurs démarches, notamment : l'Alberta ( [www.oipc.ab.ca...](http://www.oipc.ab.ca...) ), la Colombie-Britannique ( [www.oipc.bc.ca/...](http://www.oipc.bc.ca/...) ), l'Ontario ( [www.ipc.on.ca/...](http://www.ipc.on.ca/...) ) et le Québec ( [www.cai.gouv.qc.ca/...](http://www.cai.gouv.qc.ca/...) ).

• Au niveau associatif, on retrouve au Canada et plus spécialement au Québec, l'AAPI ou Association des professionnels en accès à l'information (AI) et en protection de la vie privée (PVP), qui est appuyée dans sa démarche par les pouvoirs publics. En effet, l'association créée en 1991 offre différents services à ses membres et offre différents outils dont des Guides pratiques en AIPVP : (<https://aapi.qc.ca/outils-et-services/outils-specialises/guides-pratiques-aapi/...> ).

#### 7 dimensions de la Protection de la vie privée

• De façon générale, la protection de la vie privée (PVP) (ou respect de la vie privée) concerne le droit d'une personne de choisir dans quelle circonstance et dans quelle mesure elle accepte de s'exposer elle-même aux autres, ce qui touche notamment :

- Droit à sa dignité (ex: mourir dignement, ...).

- Respect de son mode de vie (ex: langue parlée à la maison, orientation sexuelle, religion, ...).
  - Protection de l'intégrité de sa personne et de son autonomie.
  - Protection de l'accès à son domicile (ex: contre les fouilles et les perquisitions abusives, ...).
  - Protection de son intimité (ex: pouvoir rester seul, ...).
  - Protection de son anonymat.
  - Protection des renseignements personnels (PRP) (Autodétermination informationnelle).
- De façon générale, la protection des renseignements personnels (PRP), concerne le droit d'une personne de déterminer --quand, comment et dans quelle mesure-- des renseignements la concernant peuvent être:
- 1.. Colligés (Ramassés)
  - 2.. Stockés
  - 3.. Rendus accessibles
  - 4.. Utilisés
  - 5.. Communiqués
  - 6.. Conservés
  - 7.. Détruits

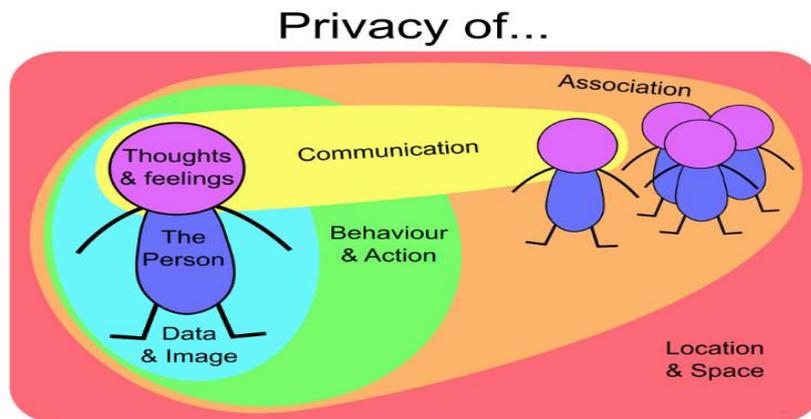
*NOTE : Ces éléments ou étapes forment ce qu'on appelle le Cycle de vie du renseignement personnel.*

- Règle générale, les renseignements personnels sont confidentiels sauf deux exceptions explicites :
    - Exception 1 : Si le consentement de la personne concernée est obtenu
    - Exception 2 : Si la loi permet de le faire, sans le consentement de la personne concernée (par ex. : personne sur une civière en danger de mort)
  - Règle générale, dans un document, les renseignements nominatifs sont ceux qui :
    - 1.. Concernent une personne physique et non une personne morale (donc PAS une organisation publique ou privée).
    - 2.. Permettent de l'identifier ou de la distinguer d'une autre personne physique.
- NOTE : Ces renseignements nominatifs sont alors confidentiels.*

### Quelques principes AIPVP

- Voici quelques principes touchant l'AIPVP :
  - Avoir une personne responsable de l'AIPVP, qui est IMPUTABLE des résultats
  - Être pro-actif, plutôt que réactif ...
  - Intégrer la Protection de la Vie privée directement dans le développement des systèmes d'info. & Assurer de facto une protection par défaut ...  
(sans obliger l'utilisateur à devoir modifier des paramètres après l'installation ...).  
*Privacy by Design (PBD) & Privacy Enhanced Technology (PET).*
  - Protection de bout en bout, donc tout au long du Cycle de vie de l'information.
  - Limitation de la collecte des données pers.
  - Déterminer dès le départ les fins de la collecte.
  - Obtenir le consentement éclairé de la personne.
  - Information exacte (bonne & à jour).
  - Adopter des mesures connues de sécurité.
  - Transparence des pratiques.
  - Informer la personne visée.
  - Assurer un droit d'accès, un droit de correction.

- Voici maintenant une image de drôle allure, qui soulève pourtant des enjeux bien réels, pas drôle du tout!



Source : <http://www.otom.info/seven-types-of-privacy/...>

Privacy of ...

Thoughts & Feelings =	Pensées & Sentiments
The Person	La Personne
Data & Image	Données & Image
Behaviour & Action	Comportement & Action
Communication	Communication
Association	Association
Location & Space	Lieu (localization) & Espace

### Quelques enjeux AIPVP

- Voici une liste NON exhaustive d'enjeux liés à l'AIPVP :
    - Accès à vos données personnelles via des contrats de recherche + ...
    - Big data (données massives) & Re-nominalisation (Re-personnalisation; Des-anonymisation).
    - Identité numérique & Tiers de confiance.
    - Informations dans l'infonuagique (Cloud).
    - Intelligence artificielle.
    - Attention à la Prise de décision automatique.
    - Signataire de la Déclaration de Montréal pour un développement responsable de l'intelligence artificielle ([https://www.declarationmontreal-iaresponsable.com/...](https://www.declarationmontreal-iaresponsable.com/)).
    - Mobilité des personnes (Localisation & Accès distant à ses informations personnelles).
    - Objets connectés.
    - Développement Agile apportant de nouveaux défis en AIPVP & Sécurité (DEV-OP) & (DEV-SEC-OP)
    - Passage graduel d'une approche "Qui dois-je craindre?" --> "À qui puis-je avoir confiance? "
    - Dernier enjeu et non le moindre, concerne les suites du Règlement no 2016/679, dit Règlement Général sur la Protection des Données (RGPD) ou (GDPR, de l'anglais : *General Data Protection Regulation*).
- [https://fr.wikipedia.org/wiki/R%C3%A8glement\\_g%C3%A9n%C3%A9ral\\_sur\\_la\\_protection\\_des\\_donn%C3%A9es...](https://fr.wikipedia.org/wiki/R%C3%A8glement_g%C3%A9n%C3%A9ral_sur_la_protection_des_donn%C3%A9es...)

\* \* \*

#### 4.4 Architecture

- En avril 2015, l'institut international d'analyse d'affaires (IIBA ou International Institute of Business Analysis) lançait la version 3 du Guide BABOK (ou Business Analysis Body of Knowledge), publié pour la première fois (V1) en 2005. (<http://www.iiba.org/babok-guide...>). La version 4 est annoncée pour 2019.
- Ce Guide BABOK V.3 couvre les cing perspectives les plus populaires du travail des Analystes d'affaires, qui ont souvent pour rôle de représenter le volet affaires et le point de vue des unités d'affaires clientes, notamment lors du développement des systèmes d'information, soit :
  - Agilité / Architecture d'affaires / Intelligence d'affaires (BI) / Management des processus d'affaires / Technologies de l'information (TI).
- Les six domaines de connaissances couverts par BABOK V.3 sont :
  - Planification & suivi de l'analyse métier: décrit les tâches utilisées pour organiser et coordonner les efforts d'analyse métier.
  - Élicitation & Collaboration: Décrit les tâches utilisées pour préparer et mener les activités d'élicitation et confirmer les résultats.
  - Gestion du cycle de vie des exigences: décrit les tâches utilisées pour gérer et gérer les exigences et les informations de conception, du début à la fin.
  - Analyse de la stratégie: décrit les tâches utilisées pour identifier le besoin de l'entreprise, y répondre et aligner la stratégie de changement au sein de l'entreprise.
  - Définition et analyse des exigences: décrit les tâches utilisées pour organiser les exigences, spécifier et modéliser les exigences et les conceptions, valider et vérifier les informations, identifier les options de solution et estimer la valeur potentielle pouvant être réalisée
  - Évaluation de la solution: décrit les tâches utilisées pour évaluer les performances et la valeur fournie par une solution et pour recommander des améliorations pour augmenter le nombre de valeurs.

\* \* \*

#### 4.5 Assurance

- Il y a des liens évidents entre l'évaluation des Risques d'affaires et technologiques, couverts précédemment dans la section 4,2 et l'Assurance.
- L'Assurance est une fonction d'affaires fondamentale, qui sert notamment à donner confiance aux investisseurs, aux institutions publiques dont les Agences de conformité (par ex. : SEC ou *U.S. Securities and Exchange Commission*), ainsi qu'aux autres parties prenantes.
- Plusieurs professionnels sont impliqués dans des activités d'Assurance, de même que les associations professionnelles qui les regroupent (auditeur: ISACA-ITAF) / (Actuaire: ICA-CIA) / (Assureur: BAC-IBC) / Etc.
- Dans certaines de mes allocutions publiques, j'aime bien rappeler l'importance historique du *Droit maritime* dans l'évaluation des risques, l'établissement des conditions d'Assurance et de couvertures des dommages, de même que le partage des rôles & responsabilités entre les différents intervenants.
- J'aime également démontrer à ces occasions, à l'aide de photos chocs, voir parfois carrément choquantes, comment certaines personnes, dont des gestionnaires et hauts dirigeants, sont fort peu conscients du DANGER.

## 4.6 Audit

- Selon Wikipedia, « l'Audit est une expertise professionnelle effectuée par un agent compétent et impartial aboutissant à un jugement par rapport à une norme sur les états financiers, le contrôle interne, l'organisation, la procédure, ou une opération quelconque d'une entité ».
- En matière d'Audit, il y a toujours plusieurs facettes & référentiels à considérer. Par ex. pour les Systèmes d'information (Si) : un incontournable est le référentiel complet COBIT 2019, véritable « coffre à outils du management postmoderne de l'information d'affaires ».
- La traçabilité dans le domaine de l'Audit est également très importante, comme c'est maintenant le cas pour la chaîne d'approvisionnement alimentaire. En cas de problème (ex. : empoisonnement alimentaire) on veut rapidement retrouver la provenance, limiter la vulnérabilité (donc l'exposition au risque) et corriger les lacunes dans l'instant et dans la durée ... Dans le cas des organisations on souhaite parfois retracer le fil des événements et aussi de la prise de décision.
- Dans le travail d'Audit, il faut habituellement partir des Objectifs de vérification, puis des Indicateurs et finalement arriver aux moyens (et non l'inverse ...). De même, il faut se garder de la tentation bien humaine de changer la méthode (ex : méthode comptable gouvernementale), lorsque les résultats ne sont pas à la hauteur de nos espérances ... (-;

\* \* \*

## 4.7 Archivistique

- Selon Wikipedia : « l'Archivistique est la discipline relative aux principes et aux techniques relatifs à la gestion des archives. Elle relève à la fois des sciences auxiliaires de l'histoire et des sciences de l'information et des bibliothèques ».
- La « Théorie des trois âges » présente le cycle de vie du document en trois phases successives ;
  - 3 États : actif (bureau) / semi-actif (entrepôt) / archives historiques ou destruction
- Selon wikipedia : « les deux principes de base de l'Archivistique sont d'une part le principe du respect des fonds (principe de provenance), qui impose de traiter les documents en fonction de leur provenance et non de leur sujet, ce qui implique de les classer et de les inventorier sans perdre de vue leur lien organique avec l'entité qui les a produits, et d'autre part le contrôle du cycle de vie de l'information ».
- L'archivistique s'intéresse à la plupart des propriétés de l'information identifiées à la section 3,3, notamment l'accès aux documents et la confidentialité des informations, l'intégrité, l'authenticité...

\* \* \* \* \* \*

## 4 Domaines de **NORMATIVITÉ (MED2)**

- La Normativité est ce qui crée un certain encadrement normatif.
- Apportons tout d'abord une première distinction fondamentale concernant le niveau d'application :
  - MORALE : Le bien et le mal selon les valeurs sociétales, les us & coutumes et la tradition ...
  - ÉTHIQUE : Le bien et le mal selon les valeurs adoptées par l'entreprise ...

- DÉONTOLOGIE : Le bien et le mal selon les Codes, les Règles, les Protocoles & autres Bonnes pratiques du métier (selon un Ordre professionnel) ...
- DROIT : Régit la vie en société ... les droits des uns et des autres ... système juridique ...

#### 4.8 Morale

- Voici deux définitions de la Morale:

- C'est un ensemble de règles de conduite et de valeurs, fondées sur une distinction entre le bien et le mal, qui sont proposés ou imposés à un individu ou à un groupe (OQLF)

- C'est un ensemble de normes et de règles, qui doivent s'imposer à tous, elle dit le bien et le mal, c'est donc à la fois un référentiel et un impératif (Isaac, 2000)

- La Morale propose ou impose donc une norme de conduite en société.
- Ce qui est moralement discutable, frôlant l'interdit dans un pays, peut très bien s'avérer être une industrie florissante dans un autre ...
- Mon professeur Norbert Alter de l'Université Paris Dauphine m'a bien appris que la technologie n'est pas neutre sociologiquement, ni moralement, car elle a des impacts singuliers ...

\* \* \*

#### 4.9 Éthique

- Alors que la morale propose ou impose une norme de conduite sociétale, l'éthique se vit au niveau organisationnel, de l'ordre du questionnement (et non des vérités absolues), sur les grands principes de vie et de ce qui est souhaitable, voire acceptable en organisation; Elle oblige donc à faire des choix conscients (plus ou moins documentés) et à savoir les expliciter ...
- L'éthique fait appel à nos valeurs, notre flair, notre capacité de distinguer ... bref, ce qu'il faudrait faire dans une situation précise dans notre organisation, mais souvent, sans référence à des règles écrites, bien explicites ...
- En fait, souvent on ne publie que les VALEURS organisationnelles, plutôt que de s'en remettre à de longs écrits, ce qui donne lieu à des interprétations diverses (parfois même en cour de justice !). Bien entendu, certaines organisations se dotent d'un Code d'éthique (genre Code des valeurs favorisées)
- L'Éthique est donc à la fois l'ART DE LA PRUDENCE, tout en DÉJOUANT L'INTERDIT DE PENSER ...

\* \* \*

## 4.10 Déontologie

### Association professionnelle

- Contrairement à la corporation professionnelle, l'Association professionnelle n'a pas des rôles statutaires dans le cadre de l'application d'une *Loi professionnelle* d'une juridiction en particulier (ex : Province de Québec). Son rôle est essentiellement de regrouper des personnes intéressées par une cause et/ou des activités thématiques d'affaires. Par exemple, en Gestion de projet, on retrouve quelques associations internationales dont les principales sont PMI & IPMA.

### Corporation professionnelle

- La Corporation professionnelle (ou Ordre professionnel) regroupe des membres praticiens dans le cadre de l'application d'une Loi professionnelle d'une juridiction (ex : Québec). Certains Ordres professionnels sont à l'usage exclusif de la pratique du métier dans leur juridiction, pour leurs membres inscrits au Tableau (Registre) de l'Ordre (ex : Pharmaciens québécois). D'autres Ordres professionnels regroupent plutôt des membres dont seulement le titre professionnel est réservé aux membres inscrits au Tableau de l'Ordre, mais pas la pratique professionnelle en elle-même. (ex : Géologues professionnels). Bien entendu, ce critère (Usage exclusif -VS- Titre réservé) influence les règles du marché professionnel.

NOTA : Les membres d'une Corporation professionnelle sont assujettis à un Code de déontologie. La déontologie est l'ensemble des règles & devoirs qui régissent une profession ou une fonction, (1) la conduite de ceux qui l'exercent, (2) les rapports entre ceux-ci et leurs clients et/ou le public (en général), habituellement définis par un Ordre professionnel.

- D'ailleurs, les professions, à titre réservé ou à usage exclusif, se dotent d'un Code de Déontologie.

\* \* \*

## 4.11 Droit

- Tout d'abord, un peu d'histoire, illustrant ainsi la forte évolution volumétrique du Droit :

- Code de Babylone (1726 avant J.C.)
  - 300 articles, gravé sur stèle d'argile
  - Publié sous le règne du Roi Hammourabi
- Code de Solon (Athènes, 594 avant J.C.)
  - Aucune modification possible sans l'accord de l'éditeur (Solon)
  - Exil de Solon, promis de 10 ans ...
  - Code conservé dans des bibliothèques : Alexandrie / Antioche / Pergame
- Code Romain (Rome, 534 après J.C.)
  - 4 700 éléments
  - Publié sous le règne de l'empereur Justinien

- On retrouve maintenant des " tonnes et des tonnes " de textes et règles législatives ou réglementaires, plus ou moins bien appliquées d'ailleurs, dans la réalité sociale actuelle, plutôt ouverte, avouons-le !

## Applications réelles des règles législatives ou réglementaires

- Deux exemples canadiens me viennent en tête : Avant que la législation canadienne autorise la consommation de la *marijuana dite légale*, en 2018, 10% des adultes québécois et 20% des adultes de la Colombie-Britannique en consommaient déjà sur une base régulière, selon plusieurs sondages.

Autre exemple, la Loi québécoise sur l'immatriculation des armes à feu est entrée en vigueur le 29 janvier 2018 et toute arme à feu --sans restriction présente sur le territoire du Québec-- doit de ce fait être immatriculée. Au moment d'écrire ces lignes (mi-février 2019) seulement 20% des détenteurs québécois d'armes à feu avaient fait leur devoir de déposer une demande.

Bref, un autre coup d'épée dans l'eau, comme on dit!

- En France, plusieurs lois sont adoptées sans décret d'application, ce qui relève ici aussi, plus de l'intention, que de l'action... (-)

- Personnellement, ce que je retiens de tout ça, c'est que le gros bon sens ne se décrète pas. D'ailleurs, ma grand-mère me disait souvent : *L'amour est plus fort que la police...* (-)

- Bien entendu, tout n'est pas écrit. Il y a aussi le *Contrat oral* et il ne faut pas oublier non plus les traditions (la plupart étant non écrites dans des textes formels, même si connues du plus grand nombre...). De même, les mentions connues de tous « Agir en bon père de famille » & « Agir en bonne mère de famille » ne sont pas appuyées par de longs textes juridiques.

## Niveaux de pouvoir

Dans une démocratie, on retrouve habituellement les trois niveaux de pouvoir suivants :

- 1.. Le Politique, regroupant les membres de l'Assemblée nationale, du Parlement, ... qui discutent et votent les lois écrites par des légistes (par ex : des légistes rattachés au ministère de la Justice). (NOTE : Ne pas confondre "LE Politique" avec LA Politique partisane)

- 2.. L'Exécutif, regroupant l'ensemble des employés de l'état (fonctionnaires, professionnels, gestionnaires, hauts-dirigeants) ("Civil servants"), qui œuvrent au gouvernement au quotidien.

- 3.. Le Juridique, regroupant les différents niveaux et types de tribunaux, qui veillent au respect des lois en vigueur.

NOTE : En droit, il y a différents niveaux de textes, pas nécessairement au même rang dans chaque pays. C'est du cas par cas, selon le système et la tradition juridique, mais globalement ça ressemble souvent à :

- Constitution du pays.
- Chartes.
- Lois ayant préséance sur les autres lois.
- Lois thématiques ou omnibus (multi-thèmes).
- Règlements.
- Décrets d'application (le cas échéant. Par ex. : En France).
- Décisions de Jurisprudence.
- Doctrine & autres textes juridiques savants ...

## Influences mutuelles

- Les juridictions sont plus ou moins autonomes, selon leur niveau et leur position comme pays. Mais une chose est certaine, elles s'influencent passablement les unes les autres. Par exemple le Droit québécois ressemble au Droit français, qui prend aussi sa source dans le vieux Droit romain.
- Par ailleurs, les membres de l'Union européenne (U.E.) peuvent devoir changer leurs législations et/ou réglementations, à la suite d'une décision prise, souvent à Bruxelles, par la Commission Européenne.
- De même, lorsqu'une province canadienne se voit dans l'obligation de changer ses règles après avoir été déboutée par la Cour suprême du Canada; d'autres provinces canadiennes ayant des règles similaires, peuvent devoir aussi les modifier à plus ou moins court terme.

## Ère du numérique

- Les pays de tradition civiliste (dont la codification du Droit est notamment *ex-ante* dans un Code civil) et les pays dits de Common Law (dont les règles sont principalement édictées par les tribunaux, au fur et à mesure des décisions individuelles) ont adopté chacun à leur manière les règles entourant la conduite des affaires numériques, dont le Commerce électronique (eCommerce).
- Ces règles touchent notamment les thèmes suivants des documents numériques (ci-après appelés DOCS):
  - Archivage numérique / Fiscalité des achats en ligne / Preuve (valeur probante) des DOCS / Manifestation du consentement & Signature des DOCS / Protection des consommateurs / Tiers-certificateurs / Etc.
- Outre le *Droit public*, il y a aussi l'évolution du *Droit privé* dont les contrats doivent aussi tenir compte des particularités du Numérique. En cas de différends, on peut recourir à différents moyens comme la médiation, l'arbitrage ou encore les différents tribunaux (par ex. Cour des petites créances, etc.). Signalons que la longueur des contrats serait liée au niveau de confiance, donc très variable selon les époques.

\* \* \*

## SECTION 5 : Meilleures pratiques en Management : L'exemple des TiC

- En 2001, je me suis procuré une Anthologie du Management conçue et réalisée par Marcel Côté et Taïeb Hafsi, professeurs à HEC Montréal, qui ont regroupé dans un ouvrage de 1656 pages, 116 contributions rédigées par 160 auteurs provenant d'une quarantaine de Départements & Centres de recherche universitaires du Canada français. Évidemment, un tel ouvrage couvrant très large (the BIG PICTURE) ne peut rester très longtemps à la fine pointe de l'actualité ... (-)

- En 2003, j'ai eu l'idée d'organiser au Québec des Séminaires thématiques gratuits portant les Meilleures pratiques en Management, essentiellement en Management TI avec Prof. Gilles Saints-Amant (puis le Prof. Laurent Renard de l'UQAM qui a pris la relève) et en Gestion des Ressources Humaines (GRH). Ces événements aux 18 mois ont tous été de grands succès de participation et de contenu. MERCI aux conférenciers qui se sont dévoués à la tâche toutes ces années.

*NOTE : Personnellement, je ne suis pas certain que ces événements fonctionneraient aussi bien de nos jours, notamment parce beaucoup de gens croient à tort que toutes les informations requises pour un travail sont déjà disponibles sur Internet et/ou que la réponse à une question technologique ou managériale doit nécessairement venir de la région de la Silicon Valley ou d'Harvard Business School. Deux erreurs de perception, car peu d'activités humaines sont aussi riches en apprentissage qu'entendre en 1 journée 8 spécialistes de domaine de votre pays --reconnus nationalement ou même internationalement-- qui vous racontent en 50 minutes chacun, une synthèse de ce qui s'est passé ces 18 mois derniers mois avec une projection pour les 18 prochains.*

- C'est Michel Carpentier, œuvrant en gestion des ressources humaines (GRH) du Secrétariat du Conseil du trésor du Québec, qui m'a sensibilisé dès 2004-2005 à l'importance du facteur humain et de la gestion du changement dans la conduite des projets publics, alors que c'est le Prof. Yves Negro de France qui m'a sensibilisé dès 2006 à l'importance de l'approche client dans les services, notamment le management de proximité des relations avec les clients et les parties prenantes. Ces deux regards, conjugués à la recherche constante d'une performance pérenne par l'optimisation des ressources et l'innovation ont modifié à jamais mon regard sur le management des organisations post-modernes.

- Vous trouverez à l'Annexe 1 une liste de *Meilleures pratiques en management TI*, produite par mon collègue Gérard Blanc.

### Gestion par processus

- Une définition générale de Processus, que j'utilise dans mes formations se résumerait comme suit :  
*Un ensemble d'activités réalisées par des personnes, avec des moyens et selon des règles, en vue d'atteindre des objectifs stratégiques.*

- Dans la plupart des référentiels que je connais, on y liste un ensemble de processus d'une organisation ou d'un domaine de gestion, selon différents niveaux de gestion. Ainsi, les processus définis par COBIT 2019 sont différents de ceux définis par ITIL, CMMI ou PMBoK V.6, et ce, même si on modélise quelquefois le même domaine de gestion... Toutefois une certaine convergence prend forme progressivement, surtout depuis cinq ans.

## Référentiels

- Voici d'abord deux définitions, également utilisées dans mes formations à l'international:
  - *Un référentiel est un ensemble organisé de connaissances organisationnelles normalisées qui permet d'orienter et de prescrire l'action rationalisée en permettant la communication, la coopération et l'apprentissage collectif dans un domaine de gestion.*
  - *Un référentiel est un ensemble de pratiques généralement reconnues par consensus national ou international, applicables la plupart du temps et il existe un large consensus aussi sur sa valeur et son efficacité. Les participants à ce consensus international peuvent être des professionnels de l'industrie, des membres des organismes de normalisation, des universitaires et des auteurs. Avant la publication de tous documents, un processus assez transparent permet à toutes personnes intéressées de commenter une version préliminaire.*
- Certains référentiels sont du *domaine public*, car ils ont été développés et sont gérés par différentes associations internationales, par ex. : CMMI, COBIT & COSO, ISO 17799, PMBoK & OPM3, SWEBoK.
- Un référentiel peut contenir l'un --ou plusieurs-- des éléments suivants :
  - Normes ISO (p.ex.: ISO 27002 pour la gestion de la sécurité des technologies de l'information).
  - Cadres de référence (COSO & COBIT, ITIL, OPM3) qui sont des pratiques éprouvées approuvées par des experts reconnus.
  - Corpus de connaissances organisationnelles propres à une discipline de gestion (PMBoK version 6 pour la gestion de projet) qui décrivent les principes et les techniques spécifiques à une discipline de gestion.
  - Corpus de compétences des personnes. Par exemples, en génie logiciel (SWEBoK) ou le *Project Manager Competency Development Framework (PMCDF)* du PMI, en gestion de projet.

## Modèle de Maturité

- Un modèle descriptif et normatif des niveaux de maturité à travers lesquels les processus (ou les capacités organisationnelles) d'une organisation vont évoluer à mesure que l'organisation rehausse ses capacités après avoir posé une réflexion structurée et ordonnée sur ses pratiques pour atteindre des pratiques généralement reconnues.
- Le modèle de maturité est fondé sur l'apprentissage organisationnel. Une organisation ne peut pas devenir experte ou s'approprier des pratiques « reconnues » dans ses actions quotidiennes sans mettre en place une démarche d'apprentissage organisationnel propre à son contexte. Cet apprentissage correspond aux niveaux du modèle de maturité de processus.
- Pour terminer, je vous dirais qu'**un bon signe de maturité en management** (par ex. : en gestion de projet), c'est **lorsqu'on est capable de dire NON PATRON**, avec un raisonnement pratique bâti sur des situations concrètes et surtout lorsqu'on a l'intime conviction que l'on a bien raison !

Comme on dit en anglais :

***“You should never consult anyone who has lesser quality information than you have, otherwise you will be led astray despite your best judgment”.***

***“Given you have the best available information over a specific situation, you should hold your ground defending your case and not yield to anyone”.***

***“Never forget: A thousand idiots will never equal a genius” .... (;-)***

## CONCLUSION & PROSPECTIVE

En guise de conclusion et de prospective, j'aimerais identifier des binômes et autres thèmes porteurs qui devraient ces prochaines années canaliser les énergies de beaucoup de professionnels œuvrant dans l'un ou l'autre des onze domaines du **GSA5-MED2** :

- Biométrie & Hyper-contrôle ...
- Vidéosurveillance & Liberté individuelle ...
- Cyberguerre & Cyberdémocratie ...
- Sûreté des données de santé (par ex : Hébergement des renseignements personnelles et des données de santé).
- Usurpation d'identité numérique.
- “ Fraude du Président ” et autres piratages psychologiques (alias de l'Ingénierie sociale).
- Vol massif des données d'entreprises (Espionnage industriel à grande échelle).
- “ Fake news ” pouvant faire élire un autre “Président”.

Bien entendu, tout ça c'est de la pure science-fiction ... (-;-)

\* \* \*

MERCI de m'avoir lu jusqu'au bout & Au plaisir de vous rencontrer dans le cadre d'un événement.

D'ici là, bonne continuation,

**Pr. Yvan Lauzon, MBA**

Expert-conseil à l'international

& Professeur contractuel (Chargé d'enseignement) à l'ENAP-UQ

yvan.lauzon@enap.ca --OU-- gestionnaire2.0@gmail.com

## REMERCIEMENTS

J'aimerais remercier mes collègues québécois, sur des Conseils d'administration, ayant proposé des ajouts:

- Gilles Gravel            ISACA-Québec
- David Henhard        ISACA-Québec
- Martin Samson        AAPI

\* \* \*

J'aimerais également remercier mes collègues européens (Belgique & France), auteurs & Conférenciers, ayant proposé des compléments d'informations:

- M. Frank Leyman
- Prof. Yves Negro
- Me Thierry Piette-Coudol.

\* \* \*

**Référentiels des Meilleures pratiques en Management TiC**

Voici une liste détaillée, mais non exhaustive, d'adresses URL --ou signets-- identifiant des sites de Référentiels (ex : corpus de connaissances) et Méthodologies touchant à la Gestion des ressources informationnelles, choisies par Gérard Blanc.

---

**Méthodologies / Référentiels / Guides**  
de  
**Meilleures Pratiques**  
en  
**Management des Technologies de l'information**

---

Par Gérard BLANC, MSC, CMC, ADM.A



## MESSAGE IMPORTANT

Cette présente Annexe A1 se veut une liste non-exhaustive des Méthodologies, Référentiels & Guides de Meilleures Pratiques en Management des Technologies de l'information (Ti).

Si tous les Outils managériaux ne sont pas listés ici, c'est simplement que certains ne sont jamais devenus un Standard reconnu (par ex : une Normes nationale ou internationale), alors que d'autres ont subi les affres du temps sans être révisés systématiquement (aux 3, 4 ou 5 ans) ou mis à jour suffisamment; enfin certains ne sont plus considérés comme des Référentiels et/ou se sont fondus dans la Pratique courante de la Gestion quotidienne des Ressources informationnelles, pour devenir des évidences ou des passages obligés.

Enfin, ce qui concerne les autres cas, c'est avec sérieux et minutie que la présente liste a été établie, en ne cherchant pas l'exhaustivité, mais en prenant tout de même soin d'être ni trop sommaire (courte), ni inexploitable; caractéristique typique d'une liste beaucoup trop longue.

Les liens (URL) indiqués dans ce document ont été vérifiés et étaient fonctionnels le 22 janvier 2019.

« Puissez-vous y trouver une lecture aussi plaisante, qu'instructive »

**Gérard Blanc**, MSC, CMC, Adm.A  
Gérard Blanc-conseil  
Collaborateur régulier au périodique *Direction informatique*  
gerard.blanc@gbaconseil.ca

\* \* \*

## RÉFÉRENTIELS / MÉTHODOLOGIES / GUIDES

**Agile - Méthode agile**  
<http://agilemethodology.org/>

**BABoK - 3**  
<http://www.iiba.org/babok-guide.aspx>  
<http://regiondequebec.iiba.org/fr/news/glossaire-du-guide-babok-v3-traduit-en-francais>

**BMIS**  
<http://goo.gl/a4USi1>

**CMMI - Capability Maturity Model Integration**  
<http://cmminstitute.com/>

**CMMI - SCAMPI - Capability Maturity Model Integration - SCAMPI**  
<http://goo.gl/djKaLS>

**COBIT 5**  
<http://goo.gl/HoXGgf>  
<http://www.isaca.org>  
<http://www.isaca-quebec.ca>

**CODE D'ÉTHIQUE**

<http://goo.gl/JOzZ4D>

**COSO**

<http://www.coso.org>

**GOVERNANCE d'ENTREPRISE** - *Document de l'OCDE*

<http://goo.gl/RLNELx>

**GOVERNANCE TI**

<http://www.governanceinstitute.com>

**IEEE-1062** - *Institute of Electrical and Electronics Engineers*

<http://goo.gl/ai0ngl>

**IPMA** – *International Project Management Association*

<Http://IPMA.world>

**ISO 38500:2015** - *International Standard Organization*

<http://goo.gl/Msda9n>

**ISO 17799** - *International Standard Organization*

<http://goo.gl/V6narp>

**ISO15504-1:2004** - *SPICE - Software Process Improvement and Capability dEtermination*

<http://goo.gl/2tHHwL>

**ISO-19011, 2011** - *International Standard Organization*

<http://goo.gl/5dhNWU>

**ISO 17799** - *International Standard Organization*

<http://goo.gl/V6narp>

**ISO-12207** - *International Standard Organization*

<http://goo.gl/gwmYO5>

**ISO-20000** - *International Standard Organization*

<http://goo.gl/BRnPKt>

**ITAF**

<http://goo.gl/ZyD2ij>

**ITIL - v3**

<http://itil-officialsite.com>

<http://itsmf.ca/fr>

<http://goo.gl/9YZZKh>

**Lean management**

<http://goo.gl/Zyw3GM>

**MACROSCOPE**

<http://goo.gl/4kPGqn>

**MEHARI**

<http://clusif.fr/>

<http://meharipedia.x10host.com/wp/home/>

**Méthode 6 sigma**

<http://piloter.org/six-sigma>

**PDCA - La roue de Deming**

<http://goo.gl/HUhrKF>

**PMBok - Project Management Body of knowledge**

<http://www.pmi.org/>

**PRINCE 2 - Project in Controlled Environments**

<http://goo.gl/UoXDg9>

**QUALITÉ QUÉBEC**

<http://goo.gl/kV8EGr>

**Risk IT**

<http://goo.gl/V5qQsq>

**RUP - Rational Unified Process**

<http://goo.gl/NScpc2>

**Scrum**

<http://www.scrum.org/>

**SWEBoK - Software Engineering Body of knowledge**

<http://www.swebok.org>

**TOGAF - The Open Group Architecture Framework**

<http://www.opengroup.org/togaf>

**Val IT - Enterprise VALue : Governance of IT investments**

<http://goo.gl/zlirh0>

**ZACHMAN**

<http://goo.gl/2NtdbR>

\* \* \*

## **PUBLICATIONS -- YLA**

La firme YLA Formation inc. (YLA) publie depuis 2003 des livres numériques (eBooks) gratuits, mais aussi des livres sur support papier disponibles en librairie. Les voici, selon le MOIS de parution :

### **OUVRAGES GRATUITS (\*)**

- Facteurs clés de succès des projets municipaux dans un contexte de villes intelligentes (Smart City) (ÉD2) – (2019-03)
- Collaboration dans les Projets & Organisations publiques : Défis & Innovations à l'ère du numérique (ÉD2) – (2019-03)
- Innovation publique à l'ère du numérique (ÉD2) – (2019-03)

\* \* \*

### **OUVRAGES en LIBRAIRIE (\*\*)**

- Modélisation des rôles et compétences-clés du Chef de projet:  
Modèle CBS (Competence Breakdown Structure) – ISBN: 978-1999410636 – (2018-09)  
- Project Manager Roles & Main Skills Attribute:  
Competence Breakdown Structure (CBS) Model – 978-1999410629 – (2018-09)
- FAIRE MIEUX en faisant autrement TOUS ENSEMBLE (ÉD2) – 978-1999461485 – (2018-10)  
- DOING BETTER by doing differently TOGETHER (ED.2) – 978-1999461478 – (2018-10)
- Développez l'intelligence collective de l'équipe de projet (ÉD2) – 978-1989364017 – (2019-01)  
- Developing the collective intelligence in project teams (ED.2) – 978-1989364000 – (2019-01)
- Libérez l'intelligence collective de votre équipe de travail – 978-1989364086 – (2019-01)  
- Let the Collective Intelligence of Your Work Team Break Out – 978-1989364079 – (2019-01)
- Mieux gérer vos Projets, même Complexes -- 9781999461454 – (2019-03)  
- Managing Projects better, even Complex ones -- 978-1999461461 – (2019-03)
- Évaluation multicritère des projets publics – 978-1999461430 – (2019-05)  
- Multi-criteria Evaluation of Public Projects – 978-1999461447 – (2019-05)
- Approche intégrée de protection de l'information GSA5-MED2 : Les domaines engageants pour la performance pérenne – Deuxième édition – 978-1989364116 – (2019-05)
- Approche intégrée de la gestion de l'information : Meilleures pratiques pour une performance pérenne – 978-1989364123 – (2019-06)

\* \* \*

(\*): Ouvrages gratuits sont accessibles notamment via : **[www.share.institute](http://www.share.institute)**

(\*\*): Ouvrages payants sur papier peuvent être commandés EN LIGNE via: **[WWW.COOPSCOOUTAOUAIS.COM](http://WWW.COOPSCOOUTAOUAIS.COM)**

Pour information, contactez l'**ÉDITEUR-DISTRIBUTEUR** :

**YLA FORMATION inc.**

C.P. 24006, CSP POINTES, MONTREAL, CANADA, H1A 4Z2

**[newmanagement2.0@gmail.com](mailto:newmanagement2.0@gmail.com)**

*NOTA : En dépit des titres quasi-similaires dans une autre langue, il ne s'agit pas ici de traductions intégrales, puisque chacun de ces ouvrages a bel et bien un contenu différencié.*