Analyse des applications en commerce électronique INF22307

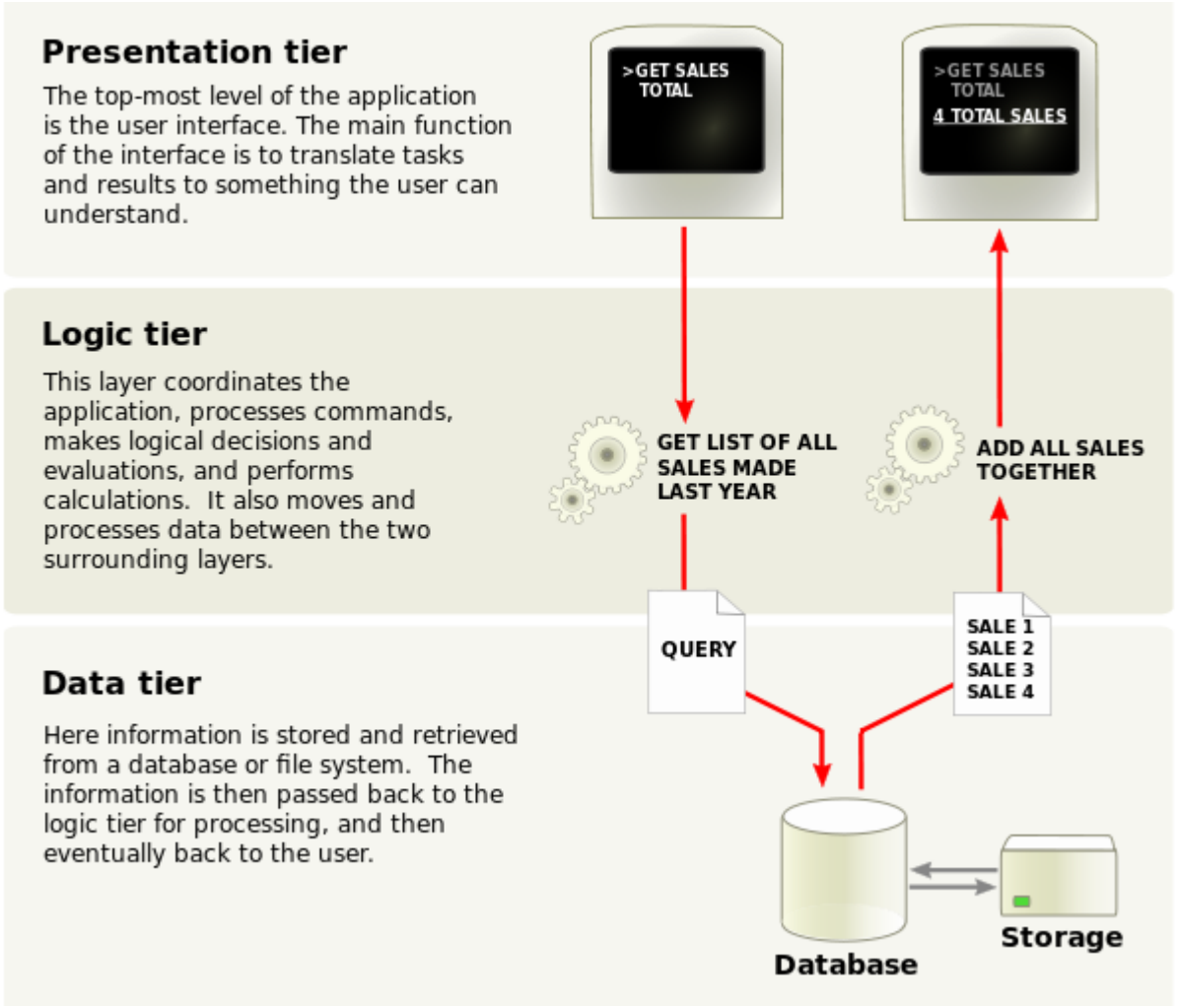
Cours #11 – Architecture, infrastructure technologique et exploitation des PGI

Martin Arsenault, ing., MBA, MGP

Novembre 2023

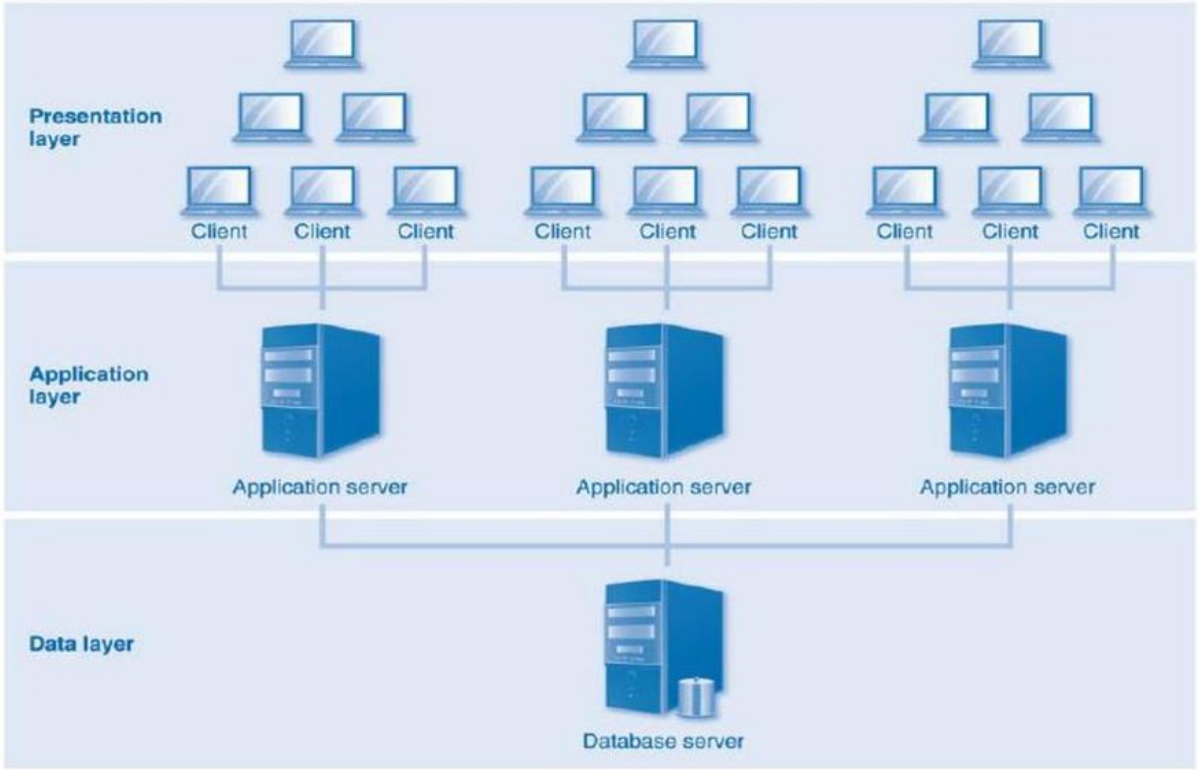
Architecture Logique

- L'architecture logique d'un système PGI est séparé en 3 niveaux (souvent appelés tiers) :
  - Couche Présentation :
    - Contient le code nécessaire à l'affichage et au traitement de l'interface du client. Ce niveau doit contenir les contrôles nécessaires pour déceler les erreurs de l'usager et/ou les opérations frauduleuses avec de mauvaises intentions.
  - Couche Application :
    - À ce niveau il n'y a plus de contrôle sur les données. Le contrôle se fait plutôt sur les opérations qui doivent être restreintes aux personnes et processus autorisés. Certaines opérations se font sur une base automatisée en fonction des paramètres saisis lors de l'implantation du PGI ce qui confirme la nécessité d'avoir des processus adéquats.
  - Couche Database :
    - Cette couche contient des données brutes qui doivent être protégées. L'accès doit être limité et contrôlé car elles contiennent toutes les données de l'organisation.



Architecture physique / technologique

- Dans les petits systèmes PGI, la couche application et Data peuvent cohabiter sur le même serveur. Ce n'est toutefois pas souhaitable pour différentes raisons :
  - Sécurité des données
  - Intégrité des données
- Il convient au minimum de mettre la couche base de données et application sur deux serveurs différents

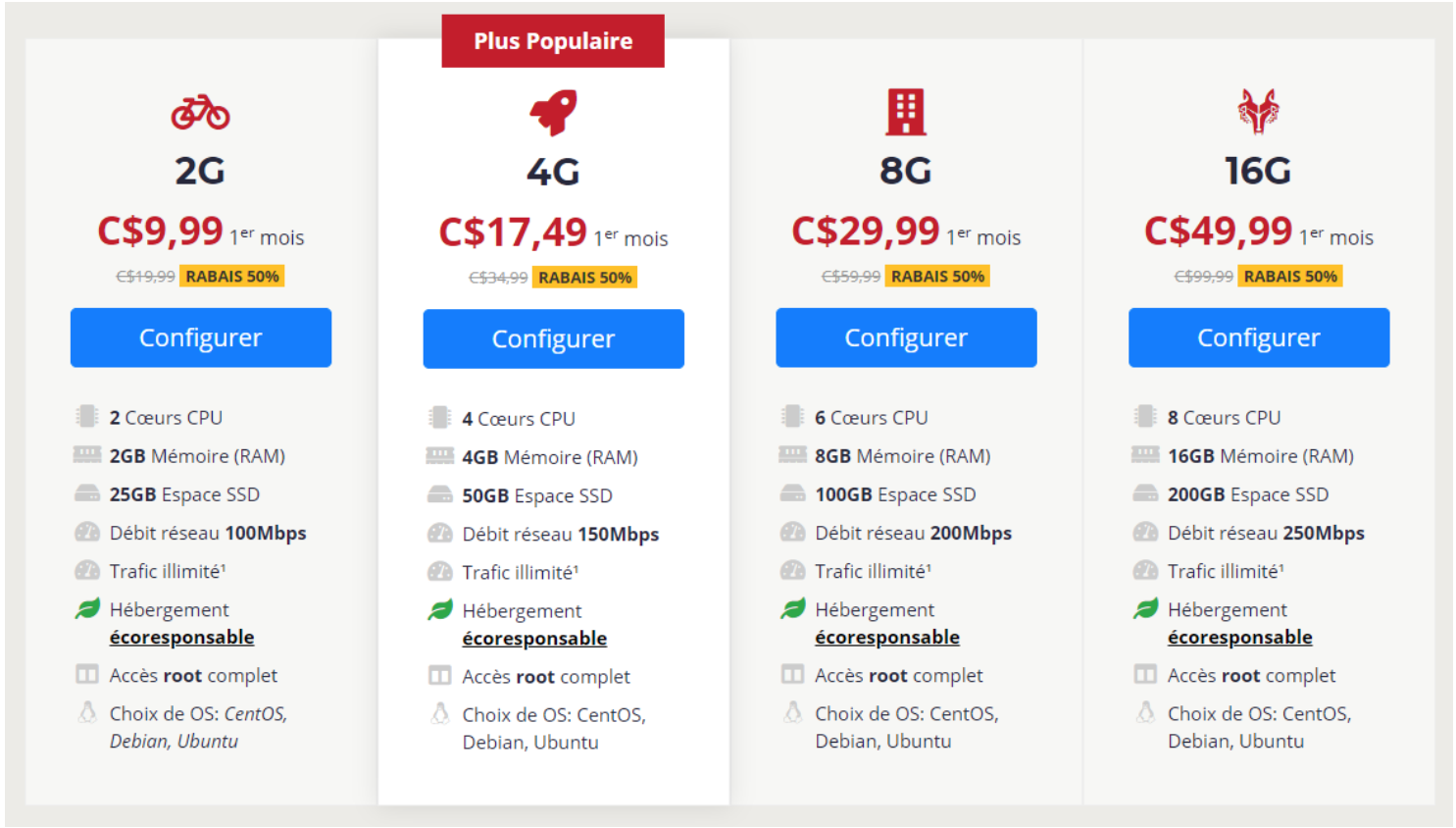


Performance de l'architecture technique

- Il faut avoir trois éléments en vue lorsque l'on pense à la performance d'un système qui supportera un PGI :
  - Performance de l'application
    - Une machine virtuelle ou un serveur moindrement bien équipé et conformément aux caractéristiques du fournisseur fera le travail amplement en fonction de la charge que vous lui demanderez.
    - Considérer le volet quantité de mémoire RAM et quantité de CPU en fonction de la quantité de données/transactions et d'utilisateurs pour assurer un traitement optimal
  - Stockage des données
    - La performance du système de stockage des données doit être considéré également. Si vous avez plusieurs usagers qui sont appelés à travailler avec le système, assurez-vous que les données puissent être accessibles rapidement (lecture/écriture).
    - Des technologies telles que NVMe, SSD et SAS peuvent aider à accélérer les temps de traitement sur les disques.
  - Bande passante du réseau
    - Cet élément est moins critique que les données sur disques ou encore l'accès à la mémoire RAM. Cependant, il faut considérer la connectivité réseau sur tout le parcours séparant le PGI jusqu'à l'usager.
    - Considérez chacun des liens réseaux et portez une attention particulière si ceux-ci doivent transiter par Internet, des fournisseurs tiers ou via des connexions site-to-site VPN

Performance de l’architecture technique

- Attention aux paramètres de vos serveurs si vous allez vers des solutions d’hébergement cloud de type IaaS



Serveur virtuel privé (VPS)

Notions de contrôle / Sécurité

- Au Canada et aux États-Unis, les entreprises doivent se soumettre à certains **contrôles rigoureux démontrant leur respect aux normes, politiques et lois** en vigueur.
- Dans le domaine financier et des affaires, de même qu'en TI, ce contrôle se fait par des **Audits**.
- Dans certains domaines, le contrôle se fait par des certifications internationales reconnues :
  - **ISO9001** qui définit les critères pour un système de management
  - **ISO14000** donne des outils pratiques aux entreprises et aux organisations de tous types qui souhaitent maîtriser leurs responsabilités environnementales
  - **ISO13216-1** qui décrit un système universel pour l'ancrage dans les véhicules des systèmes de retenue pour enfants
- Dans le domaine des TI, ce contrôle se fait par des certifications mais aussi par une volonté interne d'assurer un maintien des actifs opérationnels et fiables dans le respect des normes et pratiques en termes de sécurité de l'information.
  - **ISO27001/27002** qui aide les organisations à assurer la sécurité de leurs informations
    - Pas à l'abris malgré les normes ➔ Ex. : Desjardins et le vol d'identité

Contrôle interne

- Les contrôles internes sont des politiques et des procédures qui sont mises en place par une organisation pour assurer l'atteinte raisonnable des objectifs suivants :
  - Efficacité et efficience des opérations
    - Assurer **l'atteinte des objectifs de performance et de profitabilité** établies et le maintien des ressources.
  - Fiabilité des rapports financiers
    - Assurer **l'intégrité des données** contenues dans les rapports **assurant ainsi la fiabilité sur la situation de l'entreprise**
  - Respect des lois et obligations applicables
    - Assurer le respect les lois et les règles mises en place et envers lesquels **l'entreprise se doit de se conformer**

Audits

- Audit des entreprises
  - Un audit est une **analyse menée par un ou plusieurs experts**, avec un **œil impartial** et **indépendant**, sur un **aspect précis** de l'entreprise.

  - L'auditeur va **évaluer**, **investiguer**, mais aussi **vérifier** et **contrôler** des éléments précis. Un audit peut être ordonné dans le but de **vérifier que l'entreprise respecte des règles ou des normes en vigueur**. Un audit peut également être déclenché afin de réaliser un **état des lieux d'un service ou d'un département** complet d'une entreprise. L'audit est un **outil d'amélioration bien plus qu'un outil de sanction**, qui permet de **détecter les points forts et les points faibles**, et de **mesurer les efforts** à réaliser pour **parvenir à des résultats meilleurs**.

Types d’audit

- **L’audit financier**, centré sur la comptabilité de l’entreprise, permet de contrôler les transactions, les enregistrements, les flux monétaires, les balances/soldes et les états financiers ;
- **L’audit interne** consiste à évaluer l’entreprise en elle-même, en passant notamment en revue la comptabilité et les états financiers, mais plus généralement tout le fonctionnement de l’entreprise. Un audit interne est assimilable à un audit financier, complété par d’autres investigations sur des processus précis;
- **L’audit fiscal** est un audit centré sur la vérification des déclarations et des paiements des taxes et autres versements fiscaux réalisés par l’entreprise. L’audit consiste donc à vérifier que les déclarations et les paiements interviennent en temps et en heure et avec des montants cohérents
- **L’audit d’opérations** est quant à lui un audit avec une vocation normative. Il consiste à vérifier que toutes les normes que l’entreprise s’est imposée en interne sont bien respectées, notamment sur le plan financier et sur les processus.

Pourquoi faire un audit ?

- Plusieurs raisons peuvent mener une entreprise à exiger un rapport d’audit. D'une part, cette procédure est une **excellente façon de se préparer à une vente** puisque l'acheteur aura ainsi une plus grande confiance envers les chiffres avancés. D'autre part, l'audit peut souvent être **exigé par un créancier ou une institution financière**. Il peut aussi être **demandé par le CA de la société** en question afin que les administrateurs puissent **remplir adéquatement leurs obligations en matière de gouvernance**.
- Peuvent aussi être exigé par la loi par exemple dans le cas d’une entreprise coté en bourse et qui doit se soumettre à un audit annuel de ses états financiers.

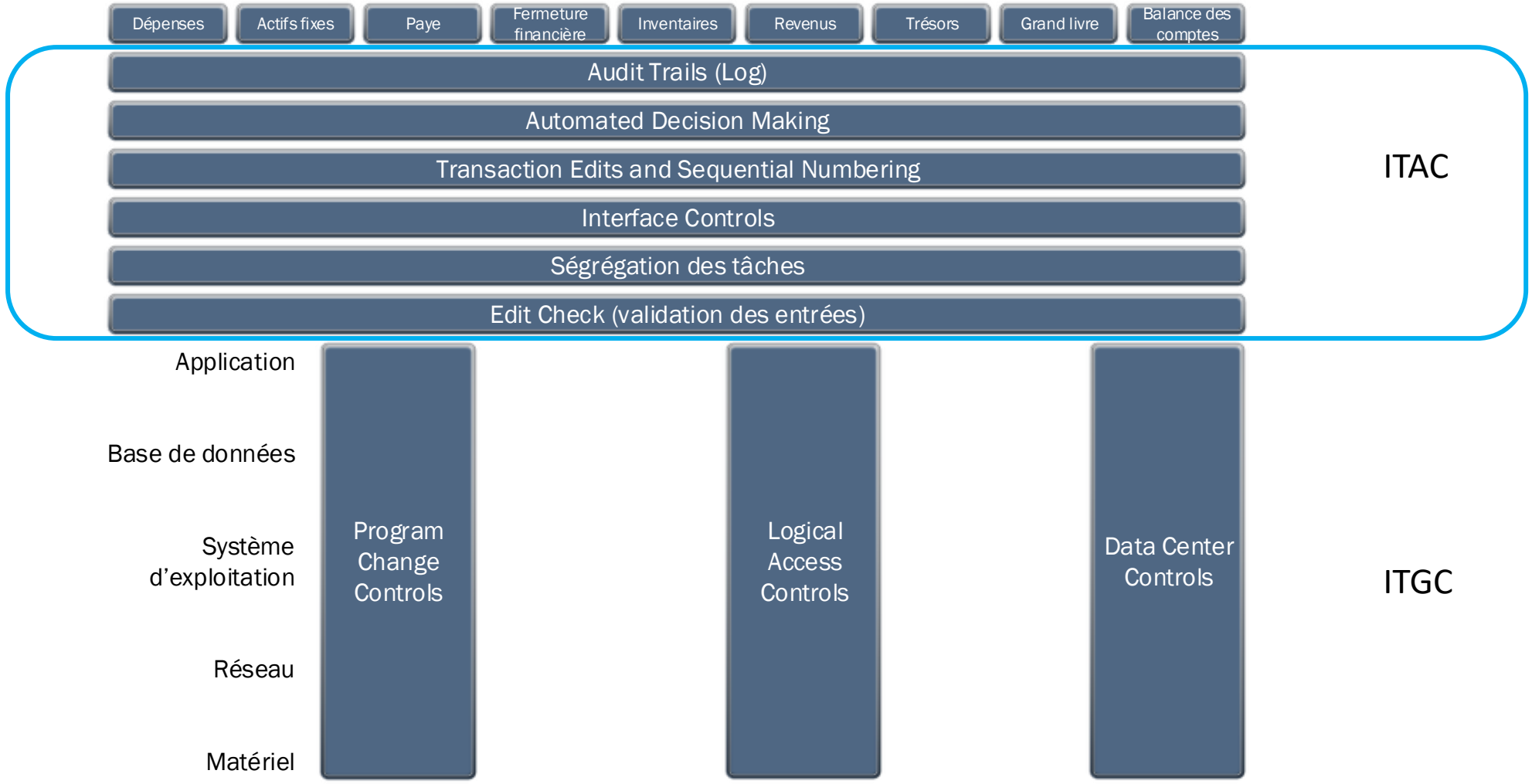
Exemple d'audit du contrôle des applications TI

- L'audit d'un système PGI :
  - Inspection de la configuration du système dans le module d'achat pour s'assurer que les quantités et les prix sont validés selon le principe du « Three-way match »
    - Un mixte d'audit financier et de processus
  - Three-Way Match = Validation de trois documents :
    - La commande d'achat préparée par l'entreprise confirmant le coût et la quantité;
    - La facture du vendeur confirmant le coût, les items vendus et le paiement;
    - La fiche de confirmation de réception de la marchandise confirmant la quantité et la conformité des items reçus.
  - Inspection de la configuration du système pour s'assurer qu'il n'y a pas de doublons :
    - Double facturation
    - Doublons sur les vendeurs

Exemple d'audit du contrôle des applications TI

- Inspection des privilèges d'accès des usagers pour les employés ayant accès aux données et vérification que la liste des usagers corresponde bien à ceux qui sont réellement autorisé à y avoir accès
- Vérification que les journaux (logs) existent bien :
  - Qu'ils sont fiables
  - Qu'ils tracent toutes les informations nécessaires dans le système
  - Qu'ils sont disponibles pour la durée de vie nécessaire
- Vérification que la pérennité du PGI est assurée :
  - Prise de copie de sauvegarde
  - Protection de son environnement
  - Les processus en place assurent une gestion saine et une évolution saine
  - Système par paliers multiples : développement, test, acceptation, production

IT General Control / IT Application Control



Contrôle d'application / IT Application Controls (ITACs)

- Ce processus contrôle les fonctions d'entrée, de processus et de sortie d'un système PGI.
- Ceci est rendu possible en permettant/bloquant ou limitant les actions des usagers et du système lui-même.
- Contrôle des entrées (Interface controls)
  - S'assure que toutes les entrées dans le PGI sont fiable, complètes et autorisées.
- Contrôle des processus (automated decision making)
  - S'assure que les données valides entrées sont traitées adéquatement et avec précision
- Contrôle des sorties
  - S'assure que les données à la sortie sont complètes, précises, fiables et accessibles aux personnes autorisées seulement.

Contrôle d'application / IT Application Controls (ITACs)

- Généralement, lorsqu'une données est saisie en entrée dans le système PGI, il n'y a plus de besoin pour en vérifier son exactitude, sa véracité et sa fiabilité. La validité doit être réalisée à la saisie.
- Les processus intégrés dans le PGI suivent leur cours et traitent les données en fonction de ce qui est programmé sans recourir à une intervention humaine. Certains processus automatisés peuvent soulever des irrégularités
  - Ex : Validation d'un écart important sur le salaire d'un employé entre deux périodes différentes
- Une validation des données se produit au moment d'insérer les données afin de s'assurer que les données répondent à certains standards pré-établis.
  - Champ laissé en blanc
  - Chiffre négatif, plage de valeur possibles
  - Format de date invalide
  - Mauvais type de caractère
  - Client et adresse de livraison
  - Etc.

Contrôle d'application / IT Application Controls (ITACs)

- Les systèmes PGI s'assurent de l'intégrité des données en documentant un « log des transactions », aussi appelé « Audit Trail » qui documente quand la transaction est saisie et par qui.
- Lorsqu'une transaction est éditée après sa saisie, celle-ci est également documenté dans le log.
- Chacune des transactions réalisées se voient documentées par un #ID unique permettant d'y associer certains détails :
  - Utilisateurs (Login ID)
  - Action réalisés (copie, transfert, modification, etc.)
  - Résultat de l'action (succès/échec/warning/erreur)
  - Date / Heure / Durée
- Certaines éditions sur des transactions peuvent ne pas être considérées comme légales et des alertes sont habituellement levées.
  - Ex : Modifier les montants d'une facture d'un client après son émission. La bonne procédure se veut d'être l'émission d'une notes de crédit ou l'émission d'une seconde facture venant modifier la première.

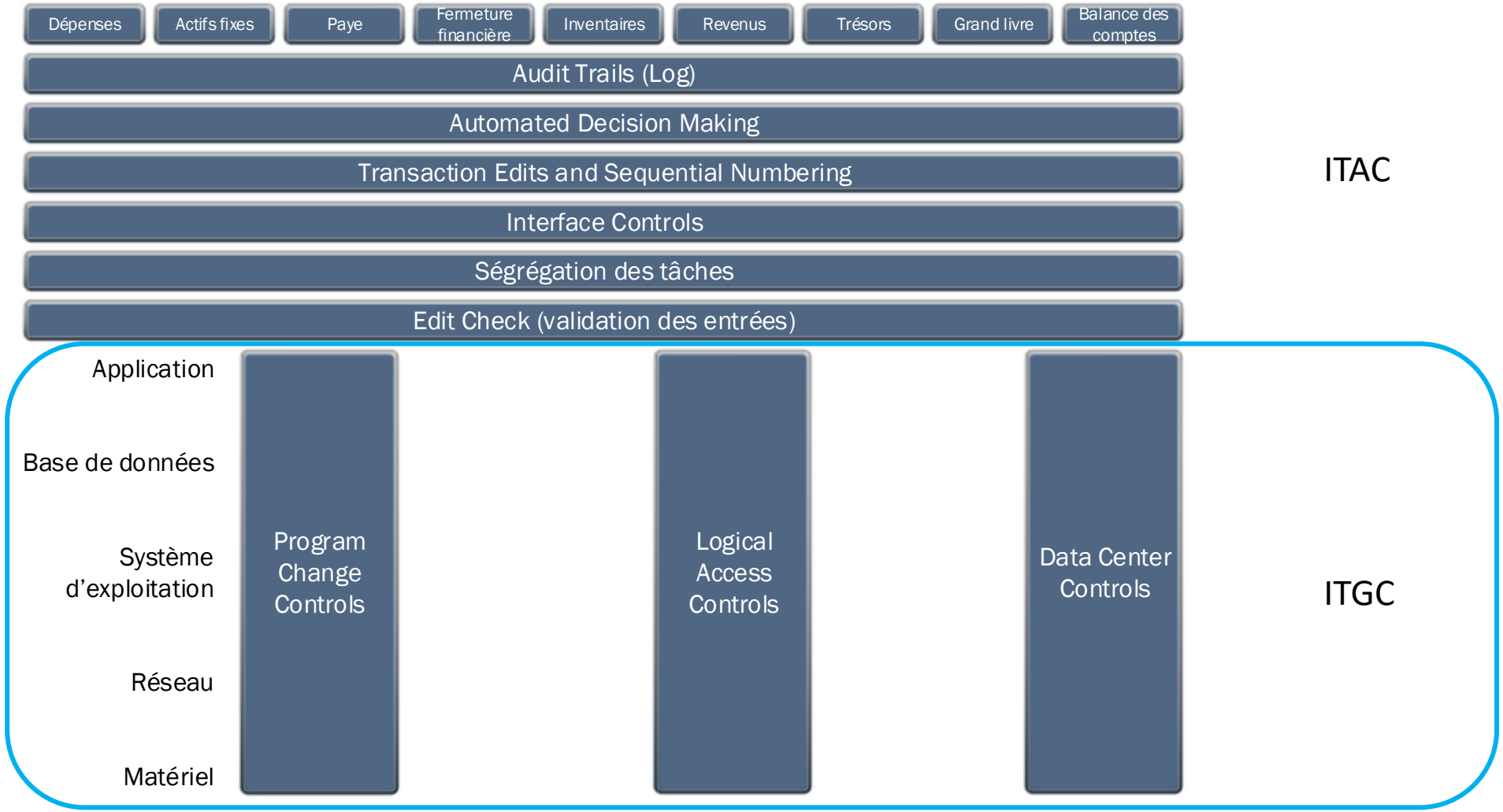
Contrôle d'application / IT Application Controls (ITACs)

- Ségrégation des tâches :
  - Une principe bien reconnu dans le monde du travail consiste à segmenter les tâches entre deux personnes lorsque vient le temps de réaliser des tâches où la fiabilité des gens requiert un niveau plus élevé.
    - Exemple : Émission d'un chèque pour paiement
  - Le système PGI et les droits des usagers peut ainsi permettre de faciliter cette gestion de façon à prévenir la fraude.
  - Un employé peut être appelé à saisir une facture et à confirmer la réception d'un item alors qu'un autre employé doit générer le paiement de cette facture.
  - Ainsi, il incombe à deux personnes la responsabilité de traiter une transaction financière impliquant une sortie/entrée d'argent.
  - Imaginez les possibilités si la même personne pouvait à la fois :
    - Passer une commande à un fournisseur de service externe
    - Confirmer la réception du service par le fournisseur externe
    - Émettre le paiement à ce fournisseur

Contrôle d’application / IT Application Controls (ITACs)

- Contrôle d’accès basé sur les rôles
  - Dans un PGI, les accès sont donnés en fonction du rôle et non pas selon son statut, l’ancienneté ou son niveau hiérarchique.
  - Les fonctions « Create, Read, Update, Delete » ne devraient pas tous être accessibles à la même personne

Contrôle général / Contrôle d'application
IT General Control / IT Application Control



Gestion des changements / Program Change Controls

- Ce contrôle gère tout ce qui est changement dans le système PGI provenant d'une demande d'un usagers ou encore provenant d'une maintenance générale ou d'application d'une patch par l'éditeur.
- Ce contrôle s'assure que l'application des changements suit un certain cadre et une série de règles pour assurer qu'ils soient conçus, testés, validés et approuvés avant d'être appliqué sur le système.
- Ce type de changement peut être appliqué en trois étapes/paliers :
  - Test (Dev)
  - Acceptation (Quality Assurance)
  - Production (Prod)

Exemple : Gestion des changements / Program Change Controls

- Les changements sont initiés seulement avec une justification d'affaires ou TI valide (sécurité, fonctions spécifiques, etc.)
- Un gestionnaire doit approuver le changement et une analyse doit être rédigée et être autorisée par un comité avant de permettre la mise en place des changements dans le module Dev
- Selon le type de changement, des usagers doivent être impliqués dans les périodes de tests (Dev) et de contrôle de qualité
- Une analyse d'impact doit être rédigée et discutée en comité avant que l'aval soit donné pour aller en production
- Après acceptation pour aller en production, un employé doit faire la mise en prod. Cet employé doit être différent de ceux qui ont procéder au processus de Dev et de QA afin d'assurer l'intégrité.

Exemple : Gestion des changements / Program Change Controls

- Inspection des privilèges d'accès des développeurs pour ceux qui sont appelé à apporter des modifications/amélioration au PGI :
  - Développement
  - Mise en production
- Vérification qu'un processus de gestion du changement est en place
  - Rédaction de la demande de changement
  - Analyse et préparation du changement
  - Confirmation du changement par le demandeur
  - Réalisation du changement en palier de développement
  - Acceptation par les développeurs du résultats obtenus
  - Réalisation du changement en palier d'acceptation
  - Acceptation par le demandeur
  - Réplication en production

Contrôle des accès / Logical Access Control

- Il s'agit du contrôle d'accès logique aux applications et systèmes. L'accès doit être limité aux personnes autorisés à avoir accès au système.
- L'accès est idéalement contrôlé via une authentification à deux facteurs :
  - 1er facteur : Validation de l'identité de la personne
    - ID/mot de passe
  - 2e facteur : Validation de l'authenticité de la personne
    - Code numérique tier, courriels tiers, contrôle biomédical, etc.
- Ce type de contrôle de l'identité est maintenant largement répandu :
  - Carte d'identité à puce
  - Tag RSA
  - Empreinte digitale, scan rétinien, etc.

Exemple : Contrôle des accès / Logical Access Controls

- Politique de mot de passe (nb/type de caractère, changement au 3 mois, historique, etc.)
- Documentation décrivant les accès et les niveaux d'accès requis
- Rôles et responsabilités relatifs à la sécurité des TI ne sont autorisés qu'aux personnes identifiées
- Mise en place de pare-feu, d'encryption et de segmentation de réseaux
- Accès directe à la base de données fermé
- Utilisation de protocole sécuritaire tel que HTTPS, TLS 1.3, SSH, etc.

Doit-on changer régulièrement nos mots de passe ?

- Doit être changé si nous le croyons compromis
- Si nous devons le changer régulièrement :
  - les gens auront tendance à réduire sa complexité
  - Les gens auront tendance à le reproduire sur un cycle
    - Ex : Différent des 3 derniers mots de passe, alors la liste en comporte 3!
  - Les gens auront tendance à l'écrire un peu partout
  - Les gens auront tendance à l'oublier ce qui en résulte une quantité élevé d'appel au soutien technique
- À faire :
  - Exiger une robustesse du mot de passe :
    - 12 à 16 caractères, lettres minuscules/majuscules, chiffres, caractères spéciaux
  - Mettre en place des processus plus complexe : Authentification multi-facteurs

Data Center Controls

- Permet de contrôler et protéger les infrastructures TI de l'organisation
- Sécurité physique
- Protection des données
- Fiabilité et disponibilité des données

https://www.youtube.com/watch?v=cLory3qLoY8

https://www.youtube.com/watch?v=kd33UVZhnAA

Sécurité de l'information / services TI

- Trois paramètres garantissant la sécurité et permettant à l'entreprise de sécuriser ses actifs :
- **Disponibilité :**
  - Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.
- **Intégrité :**
  - Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation.
- **Confidentialité :**
  - Propriété d'une information de n'être accessible ou divulguée qu'aux personnes ou entités désignées et autorisées

Source :
https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/securite_information/categorisation_information.pdf

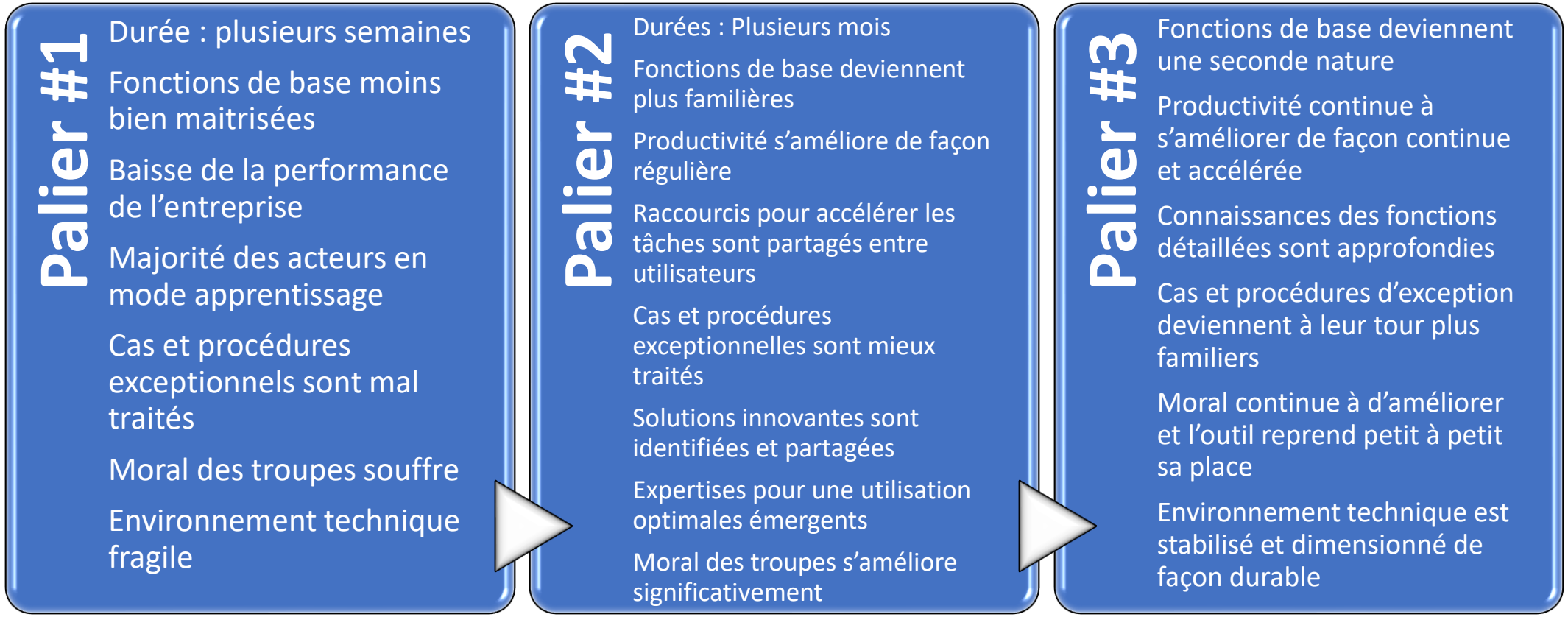
Exploitation du PGI

Comment le tout se comporte ?

Que fait-on maintenant ?

La période après le Go-live

- Trois paliers à franchir suivant la mise en exploitation « Go-Live »



Avantage d’assurer le support du PGI à l’interne

- Indépendance vis-à-vis de partenaires extérieurs
- Conservation des compétences à disposition de l’entreprise
- Coûts réduits de support et d’évolution
- Continuité des services rendus
- Compréhension des besoins spécifiques de l’entreprise
- Prise en compte du contexte spécifiques de l’entreprise
- Intégration facile entre les systèmes « maison » et PGI
- Communications efficaces et directes
- Lissage des coûts informatiques dans le temps

Avantage d’assurer le support du PGI à l’externe

- Élimination des coûts de formation des informaticiens internes
- Accès rapide à une expertise technique
- Évolution rapide vers une fonctionnalité nouvelle
- Discipline renforcée dans les processus et procédures opérationnelles
- Clarification des rôles entre offre et demande de service
- Méthodologie de support et d’évolution rigoureuse

Quoi faire avec les systèmes légataires ?

- Éliminer les systèmes dont les fonctions sont pleinement couvertes par le nouveau PGI.
  - ➔ Assurez-vous de migrer les données historiques ou de les prendre en archive
- Éliminer les systèmes dont les processus associés ont été modifiés ou intégrés par le PGI.
- Conserver en fonction et en état de fonctionnement les systèmes dont les processus ne sont pas couverts par le PGI. Ils pourront être éliminés lorsque le PGI pourra prendre en charge ces processus dans une prochaine version/mise à niveau.
- Conserver en fonction les systèmes qui n'ont aucune autre solution de substitution satisfaisante dans un futur proche et pour lesquels des processus y sont associés dans l'organisation.

Les trous fonctionnels

- Le « Zéro trou fonctionnel » n'existe pas suivant la mise en place d'un système PGI;
- L'entreprise n'est pas condamnée à vivre avec ses trous, elle peut trouver des moyens de contournement, ou encore prendre des actions pour les corriger et les diminuer progressivement;
- Il peut être utile de revenir au PGI et d'y poursuivre les travaux qui n'étaient pas critiques au moment de passer le « Go-Live »;
- L'équipe de mise en œuvre ayant travaillée au déploiement du PGI pourra être recomposée pour le mode exploitation et la correction de trous fonctionnels

Correction des trous fonctionnels – 2e vague

- Documentation des Trous fonctionnels
- Sélection des trous fonctionnels à corriger par le comité de pilotage
- Identification des expertises et des ressources techniques internes s'étant développées
- Mise en place de la méthodologie de développement pour corriger les trous
- Exécution du développement et des tests pour les trous
- Acceptation par le comité de pilotage
- Installation dans l'environnement de production
- Information/Formation aux utilisateurs

Remise en question

- Il est toujours bon de remettre en question de *statu quo*
- Si nous partons à sens inverse, il peut aussi être utile de revoir les modifications qui ont été réalisées avant le « Go-Live » et de revoir la justification de ceux-ci ?
- Le but étant de revenir dans ce cas à un PGI dépersonnalisé et conforme au modèle offert par le manufacturier

Remise en question

- Deux questions se posent :
  - Les modifications qui furent justifiées en leur temps par le fait que l'entreprise n'a pas pu ou su configurer de façon satisfaisante un processus opérationnel donné dans le PGI. Peut-elle configurer dans le PGI son processus maintenant qu'elle maitrise mieux le PGI ? Si oui, la modification correspondante doit disparaitre.
  - Les modifications qui furent justifiées en leur temps par le fait que l'entreprise n'a pas pu ou su changer un processus opérationnel donné pour le rendre configurable dans le PGI. Peut-elle changer son processus maintenant qu'elle maitrise mieux le PGI ? Si oui, la modification du processus dans le PGI doit disparaitre.
- Les modifications qui sont toujours justifiées et qui répondent négativement aux deux précédentes questions doivent demeurer.

Le PGI doit suivre l'évolution de l'entreprise

- Cession d'une partie/totalité des activités de l'entreprise
- Fusion avec une autre entreprise
- Expansion par acquisition d'une autre entreprise
- Etc.
- Le PGI doit :
  - S'assurer qu'il ne représente pas un frein
  - Être un moteur de convergence entre les différentes entités
  - Jouer à plein son rôle de catalyseur en permettant les bonnes questions
  - Accélérer le déploiement de la stratégie d'entreprise
  - Aider à définir et à mettre en place les processus opérationnels communs
  - Partager les meilleures pratiques opérationnelles entre les entités

Intégration de deux entreprises avec le même PGI ?

- Les deux entités n'ont pas nécessairement la même version
- Périmètres fonctionnels des PGI sont très probablement disjoints
- Les deux entités ont des configurations distinctes
- Les systèmes périphériques sont certainement spécifiques à chaque entreprise
- Processus opérationnels et les procédures sont souvent divergentes
- Rôles et responsabilités de chacun sur le PGI ne sont pas identiques
- Documents, rapports, produits, etc. sont généralement spécifiques

Leçons apprises - **Entreprise**

- C’est un projet d’entreprise et non pas au niveau d’un département, groupe ou individu
- Identifier les meilleurs experts dans chacun des domaines et les attitrer au projet de PGI
- Permettre une grande disponibilités des membres des équipes de mise en œuvre quitte à compenser leur absence sur leur poste régulier par des ressources temporaires
- Favoriser, encourager, promouvoir le travail en groupe, l’esprit d’équipe, etc.
- Profiter de l’arrivée du PGI pour stimuler et procéder à une refonte totale des processus
- Assurer la mise en place d’une démarche authentique, éclairée et structurée de conduite des changements réelle
- Une perte de productivité va suivre la mise en place du PGI. Celle-ci est normale mais les efforts devront être maintenus pour passer à travers cette vague.

Leçons apprises - **Management**

- Support constant, total et visible de la haute direction doit se faire sentir
- L'implication personnelle, directe, démontrée et visible des gestionnaires est incontournable
- Le plein retour sur investissement ne se fait qu'à moyen/long termes.
- Les ressources et les coûts informatiques qui sont nécessaires au suivi et au support vont réduire à la longue
- La couverture opérationnelle et le degré d'intégration des solutions apportées par le PGI augmenteront avec le temps
- Une attention et un support sans faille du management amèneront aux utilisateurs la discipline nécessaire à la pleine utilisation opérationnelle

Leçons apprises - **Utilisateurs**

- Un chef de projet à temps plein s'avère nécessaire
- L'implémentation d'un PGI ne peut être conduite que par les utilisateurs
- Rien ne peut se faire sans la volonté et sans la disponibilité des meilleurs experts des unités opérationnelles
- Initialement, seul 80% de l'ensemble des besoins opérationnels peuvent être couverts rapidement et efficacement par le PGI (Loi de Pareto)
- Au départ pour certaines fonctionnalités/départements/individus, un retour en arrière temporaire peut-être inévitable

Leçons apprises - **Informaticiens**

- L'implémentation d'un PGI en entreprise représente un nouveau métier pour l'informaticien
- Il lui est demandé de plus en plus des connaissances métiers, opérationnelles et organisationnelles plutôt que techniques
- Son travail consiste de plus en plus à intégrer des composantes et programmer des interfaces entre des système nécessitant des connaissances différentes :
  - Organisation, Communications, Gestion de projet, Analyse opérationnelle, Architecture organique, Planification, etc.
- Nouveau défi : **demeurer pleinement ouvert dans un environnement en pleine évolution technologique et de plus en plus demeurer à l'affut des notions de sécurité**

Merci et bonne semaine!!