

memento

Logiciel IBM **Information Management** Lotus Rational Tivoli WebSphereibm.com/software/fr

Governance & Risk Management

Aligner les ressources IT aux objectifs business pour permettre une meilleure sécurité, visibilité et contrôle de l'information délivrée aux utilisateurs, clients et partenaires.

> DE QUOI S'AGIT-IL ?

- L'approche Governance & Risk Management répond à plusieurs objectifs :
 - Procurer **Visibilité, Contrôle et Automatisation du cycle de vie** des services pour atteindre les objectifs business.
 - Etendre ce concept aux spécificités des secteurs Industriels et Telecommunications.
 - Fournir une **posture de Sécurité avancée**.
 - Garantir la **disponibilité et continuité des données**.
- Les problématiques adressées par le programme peuvent être regroupées selon quatre thématiques :
 - Service management.
 - Enterprise Asset Management & Service Assurance.
 - IT Security.
 - Business Continuity.

> POUR QUELS CLIENTS ?

- Entreprise :**
 - A partir de 500 collaborateurs.
 - Tous secteurs d'activité.
- Contacts :**
 - Directeur informatique.
 - Directeur de production ou d'exploitation.
 - Responsable de site.
 - Responsable Sécurité du Système d'Information (RSSI).
 - Responsable de la conformité.
 - Responsable du Plan de Reprise d'Activité (PRA) ou Plan de Continuité d'Activité (PCA).

> BÉNÉFICES CLIENTS

- Réduction des coûts d'exploitation et d'administration.
- Respect des contrats de service.
- Réduction du nombre d'incidents et d'arrêts d'exploitation.
- Ajustement des budgets informatiques aux objectifs métiers.
- Conformité à la politique de sécurité.
- Amélioration de la satisfaction des utilisateurs.
- Contrôle des actifs de l'entreprise pour améliorer le ROI.
- Gain de confiance des clients : respect des délais, sécurité...
- Accélération de la mise sur le marché de nouveaux produits.

> MESSAGES IMPORTANTS

- La multiplication des modes d'accès au système d'information **accroît les besoins de sécurisation** : protection des données des clients, des fournisseurs et des informations propres à l'entreprise, dans le respect de la législation.
- Les offres de sécurité d'IBM répondent aux **nouveaux besoins client** en proposant une approche de bout en bout.
- L'offre IBM répond aux besoins de visibilité, contrôle et automatisation du système d'information.
- Au niveau organisationnel, les solutions IBM se réfèrent à une **norme ISO reconnue** (elle-même mise en place en interne par IBM).
- Cette approche assure la cohérence, l'interopérabilité et l'intégration de plates-formes et d'environnements hétérogènes.

Références clients

> NIWS

NIWS, intégrateur de systèmes et prestataire informatique, a mis en place une infrastructure autonome virtualisée et autogérée, qui l'aide à rationaliser et à standardiser les processus. La société a pu améliorer la satisfaction de ses clients et renforcer sa capacité d'adaptation au changement.

> Herbalife

Depuis son introduction en bourse, la société Herbalife, un fournisseur international de produits diététiques et de compléments nutritionnels, est soumise à des obligations déclaratives plus contraignantes. L'entreprise s'est donc tournée vers IBM pour développer un portail clé en main. Grâce à la souplesse de ce portail, à ses automatismes et à ses puissants outils de statistiques, Herbalife peut optimiser ses processus de contrôle et de transparence, conformément à ses impératifs de bonne gouvernance.

> QUESTIONS CLÉS

- Les risques de l'entreprise sont-ils **identifiés** ? Une cartographie précise en est-elle établie ?
- Les impacts des risques sont-ils identifiés et regroupés en différentes familles ? Par exemple, impact sur le produit, sur le flux matière (dans l'industrie), sur la logistique, sur le flux financier, sur les lois et les règlements, sur le risque d'image...
- Ces impacts sont-ils **mesurés et hiérarchisés** ?
- Les risques sont-ils **maîtrisés** par les systèmes de management de l'entreprise (management de la qualité, système prévention et sécurité) ?
- Ces systèmes prévoient-ils la **mise sous contrôle** du risque ? Au-delà des dispositions prises pour éviter qu'il ne se produise, prévoient-ils, en cas d'occurrence, la reprise d'activité ou sa continuité, éventuellement dans un mode dégradé ?
- Existe-t-il dans l'entreprise un processus qui vise à tirer les renseignements en cas de survenance d'une crise ?
- Etes-vous capable de **fixer une priorité** sur les processus métier à restaurer en premier lieu ?
- Est-il facile de calculer le coût pour l'entreprise de l'arrêt d'un de ses serveurs ?
- Connaissez-vous précisément le **temps nécessaire** à la restauration qui permettrait d'offrir des conditions d'utilisation acceptables ?
- Pensez-vous que votre système est capable de se mettre en conformité et de **s'adapter rapidement** au changement en cas d'évolutions réglementaires ?
- Vos données critiques restent-elles **accessibles** en cas de coupure de courant ?
- Après une interruption serveur, combien de temps faut-il pour que vos données soient à nouveau accessibles ?
- Combien de temps vous faut-il pour retrouver un mail archivé depuis plus de cinq ans ?

memento Governance & Risk Management

> COMMENT ABORDER UN PROJET ?

Au départ : définir la stratégie appropriée aux besoins métiers et aux contraintes informatiques et économiques.

SERVICE MANAGEMENT

• L'approche IBM Service Management passe par les étapes suivantes :

- Evaluation globale des processus / organisation.
- Conception de la solution cible.
- Elaboration du plan de transformation.
- Réalisation d'un bilan après plusieurs mois.

• Ces étapes s'appuient sur ITIL (IT Information Library), qui définit, pour chaque métier de l'entreprise, les **meilleures pratiques** pour :

- l'organisation de la production informatique ;
- l'amélioration de l'efficacité du système d'information ;
- la réduction des risques ;
- l'augmentation de la qualité des services informatiques.

IT SECURITY

• IBM traite le sujet de la sécurité informatique à travers 4 aspects :

- **Evaluer** : comprendre son exposition aux risques et les besoins de protection.
- **Défendre** : protéger son organisation des attaques externes et internes.
- **Accéder** : fournir et gérer les différents niveaux d'accès aux applications et données.
- **Superviser** : détecter, analyser et réagir aux menaces.

• Le point de départ est très souvent la réalisation d'un audit de vulnérabilité.

BUSINESS CONTINUITY

• L'approche IBM couvre quatre points d'entrée de la problématique de continuité opérationnelle :

- **Comprendre** sa vulnérabilité.
- **Assurer disponibilité et cohérence** des données en cas d'audit ou d'interruption opérationnelle.
- **Etendre** cette disponibilité à l'ensemble de l'infrastructure métier.
- Avoir un **Plan de reprise d'activité**.

> LES POINTS FORTS D'IBM

- IBM maîtrise l'ensemble des composantes - savoir-faire, technologies et expertise - pour mettre en œuvre une démarche de type « Governance and Risk Management » dans les trois domaines suivants :
 - Service Management.
 - IT Security.
 - Business continuity.
- Les solutions de « Service Management » aident les centres d'exploitation à délivrer aux utilisateurs des **services de qualité**, à des **coûts maîtrisés**, en alignant les processus informatiques avec les objectifs de service demandés par les directions métier.
- L'offre IBM pour le « Service Management permet d'**optimiser les processus de l'informatique** et de les intégrer avec les données. La clef de voûte en est le recueil de bonnes pratiques ITIL.
- Les solutions de Sécurité d'IBM assurent l'**intégrité, la confidentialité et la disponibilité des informations**.
- Les solutions de « IT Security » assurent l'**intégrité, la confidentialité et la disponibilité des informations**.

> L'OFFRE

Pour chaque thème, une offre complète matérielle (STG), logicielle (SWG) et services (GTS). Ne pas oublier le financement !

- **L'offre Service Management**, en bref :
 - Composante logicielle : Rational et Tivoli, pour le développement et la gestion du projet.
 - Composante matérielle : System p, x, z, i, Consolidation et Virtualisation de systèmes, backup, mirroring, blade center...
 - Composante services : Solutions d'évaluation et de mise en place.
- **L'offre Enterprise Asset Management**, en bref :
 - Logicielle : Tivoli Maximo Asset Management.
 - Matérielle : Hardware Asset Management for IT.
 - Services : EAM Deployment Services.
- **L'offre Security**, en bref :
 - Composante logicielle : Rational, Tivoli, et dans une moindre mesure, DB2.
 - Composante matérielle : Data Encryption, System z, System p, Blades.
 - Composante services : Internet Security Systems, Physical Security.
- **L'offre Business Continuity**, en bref :
 - Composante logicielle : Rational et Tivoli.
 - Composante matérielle : System p, x, z, i, Blades, TotalStorage® SAN Volume Controller, Enterprise Storage Server®, Grid, Virtualization.
 - Composante services : Services de Haute disponibilité, PCA et PRA.
- **Financement** :
 - Financement de tout ou partie d'un projet, y compris via un partenaire IBM et incluant matériel, logiciel ou service IBM et non IBM.
 - Location, ouverture de crédit, crédit-bail, plan de paiement échelonné, différé de paiement.

> EN SAVOIR PLUS

<http://www-935.ibm.com/services/fr/cio/risk/>

<http://www-306.ibm.com/software/tivoli/governance/>

• Pour connaître l'offre s'appliquant à chaque étape d'un projet de Service Management :

<http://www-06.ibm.com/software/tivoli/governance/servicemanagement/solutions.html>

• Pour connaître l'offre s'appliquant à chaque étape d'un projet de Sécurité :

<http://www-306.ibm.com/software/tivoli/governance/security/index.html>

• Pour connaître l'offre s'appliquant à chaque étape d'un projet de Business Resilience :

<http://www-306.ibm.com/software/tivoli/governance/gbusinesscontinuity/index.html>