Gestion des règles et de la conformité

Réduire le coût et la complexité liés au respect de réglementations multiples

Sommaire :

Introduction

Dans l'environnement commercial fortement réglementé d'aujourd'hui, les entreprises doivent se conformer à de multiples obligations légales en matière de confidentialité, de processus et d'activité. Quelle que soit l'étendue de l'environnement de conformité d'une entreprise, les similarités entre ces différentes obligations sont à l'origine de chevauchements des exigences en matière de gestion, de documentation, de contrôle et d'audit, qui peuvent anéantir les efforts réalisés en vue d'identifier et de gérer efficacement et complètement les risques et la conformité.

Les entreprises qui adopteront une approche transversale seront en mesure de limiter l'augmentation des coûts et la complexité croissance de la mise en conformité, tout en obtenant des informations utiles et à jour sur les risques qui pèsent sur leurs processus essentiels et sont susceptibles d'affecter leurs performances, sous forme d'actions juridiques, d'amendes et de pénalités, ou d'atteintes à leur réputation ou à celle de leurs marques.

Ce livre blanc aborde quelques-uns des principaux défis de la gestion des règles et de la conformité et présente la solution technologique développée par IBM pour y faire face.

Définition de la gestion des règles et de la conformité

La gestion des règles et de la conformité peut concerner des domaines très variés, allant des réglementations financières, telles que la loi Sarbanes-Oxley (SOX), jusqu'aux réglementations propres à certains secteurs verticaux, tels que l'industrie pharmaceutique ou le secteur manufacturier. Mais l'idée de base qui préside à la gestion des règles et de la conformité est de comprendre la totalité du spectre réglementaire auquel une entreprise est soumise, puis de s'assurer qu'elle a mis en place la structure de contrôle des risques appropriée afin de limiter ceux-ci pour chaque réglementation. Et comme l'environnement réglementaire change fréquemment, l'une des fonctions essentielles de la gestion des règles et de la conformité est de permettre de suivre ces changements et de s'y adapter afin que les performances de l'entreprise n'en souffrent jamais. Dans la pratique, les entreprises n'ont souvent qu'une mauvaise compréhension globale des risques liés à la conformité qui pèsent sur elles, ce qui les place dans une position précaire susceptible d'entraîner une érosion importante de l'identité de leurs marques.

L'importance de la gestion des règles et de la conformité

Aussi, mettre en place un contrôle centralisé de leurs activités dans les domaines de la gestion de la gouvernance, des risques et de la conformité constitue pour toutes les entreprises un facteur clé de réussite.

Selon IDC, les entreprises réalisant en moyenne 500 millions de dollars de chiffre d'affaires sont soumises à entre 35 et 40 obligations réglementaires (pour les entreprises plus importantes, ce nombre est encore plus élevé).[1] De nouvelles lois et réglementations sont élaborées en permanence et les obligations à respecter changent constamment. Cela soumet les entreprises à un risque sans cesse croissant de pénalités et de dommages à leurs marques si leurs processus internes sont inadéquats ou défaillants.

Aujourd'hui, une entreprise internationale type est soumise à des réglementations dans de multiples domaines :

- Confidentialité (directive sur les données de l'Union Européenne, California Privacy, Gramm-Leach-Bliley Act, etc.)
- Sectoriel (CFR Part 11, HIPAA, Bâle II, OSHA, NASD, FERC, NRC, etc.)
- Gouvernemental (FISMA, OMB Circular A-123)

En outre, au cours des cinq dernières années, l'extension de la portée des réglementations s'est accompagnée d'une augmentation des pénalités encourues en cas de non-conformité. Ces pénalités peuvent aller de simples amendes jusqu'à une baisse de la capitalisation boursière si cette non-conformité est portée à la connaissance des investisseurs. Cette dernière répercussion est nettement plus sévère, et ce principalement parce que le fait que les investisseurs ont davantage conscience de l'importance du respect des réglementations signifie que les marchés sont prompts à sanctionner les entreprises qui ne les respectent pas.

L'environnement réglementaire actuel, en constante évolution, impose à tous les collaborateurs d'une entreprise de comprendre l'exposition au risque de non-conformité qui est associée à chaque poste essentiel de l'entreprise, et de gérer activement ces expositions afin de réduire au maximum les risques. Dirigeants et Managers doivent surveiller dynamiquement que les réglementations sont bien respectées, afin que l'entreprise dispose d'une souplesse et d'une capacité de modification suffisantes pour s'adapter aux changements survenant dans son environnement.

Actuellement, la plupart des entreprises ont une approche individualisée du respect des réglementations, qu'elles abordent réglementation par réglementation ou de façon différente pour chaque entité juridique et commerciale. Cette approche fragmentée et décentralisée se révèle inefficace.

En déployant une plateforme centralisée de gestion des règles et de la conformité, les entreprises peuvent non seulement réduire le coût sous-jacent et la complexité inhérents au respect de réglementations nombreuses, mais aussi atteindre un niveau inégalé d'efficacité et bénéficier d'une visibilité accrue.

En adoptant une solution technologique de gestion des règles et de la conformité, elles peuvent abandonner leurs approches anciennes basées sur des feuilles de calcul et lier leurs différents postes à des règles et des processus spécifiques, réduire le nombre de contrôles requis, et ainsi réduire les coûts des audits internes sans augmenter le niveau global du risque de non-conformité.

Le défi de la gestion des règles et de la conformité

Les pénalités importantes dont la loi Sarbanes-Oxley a été assortie en 2002 (et les poursuites judiciaires retentissantes qui ont suivi) ont immédiatement éveillé l'attention des entreprises internationales et les ont forcées à adopter de nouveaux processus et à déployer de nouvelles solutions pour satisfaire aux exigences de cette loi.

Malheureusement, dans leur hâte de déployer ces solutions, elles ont souvent ignoré le besoin de se mettre en conformité avec d'autres réglementations nouvelles, telles que HIPAA, PCI ou le Patriot Act.

Ces dernières n'ont pas bénéficié de la même publicité que la loi SOX, mais elles prévoient aussi des sanctions financières sévères et des peines de prison en cas de non-conformité.

Le résultat a été le déploiement de systèmes cloisonnés, optimisés pour la loi SOX mais incapables de répondre facilement aux exigences des autres réglementations (non financières).

Le problème de la conformité a été compliqué par le fait que bon nombre des risques et des contrôles qui étaient documentés et testés en vue de la conformité à la loi SOX s'appliquaient également à ces autres types de réglementation. Résultat, les auditeurs internes et l'ensemble des employés ont été obligés de façon répétée de répondre aux mêmes questions et de documenter et tester les mêmes contrôles, dans des formats différents et pour des publics différents, ce qui a conduit à une baisse globale de leur productivité et à une augmentation des coûts.

Les entreprises ont commencé à réaliser que le processus de respect de la loi SOX était bien documenté et compris, mais que les autres programmes de mise en conformité souffraient toujours d'un manque de standardisation et de l'utilisation de processus majoritairement manuels et sources d'erreurs, qui créaient de la confusion et rendaient impossibles une génération de rapports et une analyse dynamiques. Pour compliquer les choses, la complexité croissante du paysage réglementaire fait que de nombreuses entreprises ne savent même pas quelles lois, réglementations et normes elles doivent respecter, et encore moins si elles les respectent ou non.

De nombreux produits dédiés permettent de répondre à des exigences réglementaires spécifiques, mais cette approche cesse d'être utilisable quand l'entreprise doit respecter des dizaines de réglementations. Ces solutions dédiées ne peuvent capturer et gérer que les informations provenant des applications liées aux réglementations concernées et n'offrent aucune visibilité sur les interdépendances des ressources pour les processus d'entreprise, les règles, les risques et les obligations réglementaires. Elles ne sont pas non plus prévues pour s'intégrer automatiquement avec les solutions conçues pour le respect de la loi SOX, ce qui signifie que plusieurs applications isolées continueront d'être déployées.

Pour surmonter le défi de la gestion de la conformité, il faut mettre en œuvre une plateforme centralisée multiréglementation qui permette de détecter les interdépendances des risques et de les analyser facilement, et qui facilite la gestion de ces interdépendances des ressources, processus, règles et réglementations. Une telle solution devrait être capable de créer un tableau de bord unique permettant aux cadres de visualiser ces liens, de rédiger des rapports à leur sujet, et de créer des processus et des flux de travail automatisés pour s'assurer que les interdépendances sont utilisées, que les redondances de ressources sont éliminées et que les objectifs sont atteints de la manière la plus rentable possible.

Quand une approche multiréglementation centralisée est déployée à l'échelle d'une entreprise, ses cadres peuvent commencer à réaliser que les ressources qui sont nécessaires pour répondre aux exigences d'une réglementation peuvent aussi être utilisées pour en respecter une autre. Les entreprises internationales, par exemple, peuvent découvrir que des rapports similaires, voire identiques, peuvent être utilisés pour respecter non seulement la réglementation HIPAA, mais aussi les réglementations équivalentes en matière de confidentialité en vigueur dans l'Union Européenne. Par conséquent, au lieu de dupliquer les ressources et les tâches précédemment utilisées pour respecter chacune de ces réglementations, il est possible de consolider et simplifier les flux de travail et l'utilisation des ressources.

Présentation d'IBM OpenPages Policy and Compliance Management (PCM)

IBM OpenPages Policy and Compliance Management (PCM) est une solution logicielle de gestion des règles et de la conformité, qui diminue la complexité et la lourdeur associées au respect des nombreuses obligations réglementaires sectorielles, gouvernementales et relatives à la confidentialité. Elle automatise le processus de test, de révision, d'attestation et de résolution, tout en permettant d'identifier les similarités entre les exigences afin de diminuer les redondances et la duplication des efforts.

OpenPages PCM s'appuie sur la plateforme IBM OpenPages GRC Platform, ce qui permet aux entreprises d'utiliser une infrastructure commune de référentiel de données, de flux de travail et de génération de rapports pour toutes leurs activités liées à la conformité. OpenPages GRC introduit également des types d'objets communs (entité, processus, risque, etc.) qui sont également utilisés par les autres modules IBM OpenPages (Financial Controls Management, Operational Risk Management, IT Governance et Internal Audit Management).

L'architecture d'OpenPages PCM inclut des obligations (et des sous-obligations). Les obligations sont des objets spécifiques qui incluent les lois, les réglementations et les meilleures pratiques. Une obligation peut inclure tout ce dont une entreprise veut effectuer le suivi, y compris des lois et des statuts, des réglementations et des règles internes (par exemple, un code d'éthique ou les valeurs de l'entreprise). L'utilisation de ces obligations confère une efficacité nouvelle à tout le processus de mise en conformité, car disposer d'un objet universel pour tous les types de problèmes de conformité signifie que les cadres chargés de leur résolution n'ont pas besoin d'effectuer séparément le suivi des statuts, des réglementations et des règles mais peuvent utiliser le modèle d'objet « obligation » pour centraliser toutes les activités liées à la conformité.

Bénéfices d'OpenPages PCM pour les utilisateurs

Les clients qui déploient OpenPages PCM peuvent en retirer les principaux avantages suivants :

- **Visibilité sur la conformité.** Le référentiel centralisé d'OpenPages PCM est relié à une infrastructure de risques et de contrôle souple et basée sur des règles. Grâce à celle-ci, il est possible de définir, contrôler et gérer dans toute l'entreprise les relations entre les risques en matière de conformité et de générer des rapports les concernant, ce qui permet d'ajuster les niveaux de tolérance aux risques et de réduire les conséquences imprévues dues à des défauts de conformité.

- **Meilleure gestion de la conformité.** OpenPages PCM comporte une bibliothèque d'obligations hautement configurable capable d'importer et de gérer n'importe quelle combinaison d'obligations, lois ou meilleures pratiques, qu'elles soient gouvernementales, sectorielles ou technologiques. Les obligations de cette bibliothèque peuvent être aisément harmonisées (détermination des exigences communes), rationalisées en fonction de l'infrastructure de contrôle de l'entreprise (ce qui réduit au minimum les risques de contrôler trop ou pas assez les environnements) et synchronisées (ce qui évite la duplication des efforts) dans le contexte d'un environnement réglementaire en constante évolution.

- **Souplesse et agilité organisationnelles.** OpenPages PCM est entièrement configurable, ce qui favorise une approche flexible de la conformité, qui prend en compte les changements et s'aligne sur les procédures et nomenclatures existantes de l'organisation, réduisant ainsi le coût total de possession.

- **Solution GRC complète.** OpenPages PCM est totalement intégré avec le produit complet OpenPages GRC, ce qui permet aux organisations de proposer des services partagés – tels que la génération de rapports, l'automatisation des flux de travail et l'administration – pour les autres modules IBM OpenPages dédiés à la gouvernance informatique, aux contrôles financiers, aux risques opérationnels et aux audits internes, avec un minimum d'efforts.

- **Harmonisation et standardisation des programmes de conformité entre les différents services et unités fonctionnelles.** OpenPages PCM gère une bibliothèque centralisée de lois, de réglementations et de meilleures pratiques qui permet de tirer parti des chevauchements entre les obligations réglementaires et de suivre et surveiller les modifications externes apportées aux réglementations afin de permettre une approche plus efficace des règles et de la conformité.

- **Offre à l'équipe chargée de la conformité la souplesse dont elle a besoin pour appréhender l'état de conformité à différents niveaux.** OpenPages PCM permet aux utilisateurs finaux et aux administrateurs d'accéder rapidement à des synthèses de la conformité réglementaire vue aux niveaux des unités fonctionnelles, des unités commerciales, des emplacements géographiques ou d'une obligation spécifique.

- **Génère des rapports pratiques qui garantissent la compréhension des risques de conformité.** Les robustes fonctionnalités de génération de rapports et d'aide à la décision offrent des tableaux de bord dynamiques, des diagrammes et des rapports interactifs concernant l'état de conformité pour plusieurs réglementations.

- **Permet aux dirigeants d'être sûrs de respecter la réglementation.** OpenPages PCM offre un flux de travail complet qui surveille et gère dynamiquement les problèmes et transmet les synthèses de conformité réglementaire aux intervenants concernés. Ce flux permet à chacun de prendre conscience de la nécessité du respect de la conformité et contribue à garantir l'application des règles et des procédures de l'entreprise.

- **Adaptation du système aux procédures de l'organisation.** OpenPages PCM est intégralement configurable, ce qui signifie que les utilisateurs peuvent tout configurer – formulaires, interfaces utilisateur, langue, rapports, flux de travail et paramètres à l'échelle globale du système –, ce qui contribue à réduire son coût total de possession.

OpenPages PCM en action

OpenPages PCM offre plusieurs fonctionnalités qui permettent à votre entreprise de se conformer aux réglementations qui la concernent.

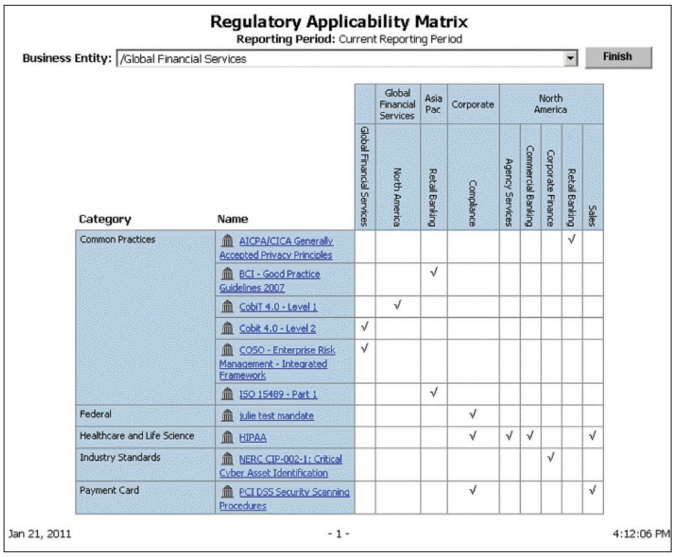
Référentiel de gestion de la conformité complet

OpenPages PCM fournit un référentiel de données unique qui sert de source centrale pour toute la documentation relative à la conformité et aux risques, ce qui couvre les entités, les processus, les risques, les contrôles, les tests et les résultats des tests. Ce référentiel permet une gestion documentaire complète grâce à ses fonctionnalités d'extraction et d'archivage, de contrôle des versions et de piste d'audit. Il permet également une hiérarchisation quasi illimitée des entités, risques et contrôles afin de s'adapter à la structure unique de chaque entreprise, et aide à éliminer les redondances grâce au partage des documents, des processus, des risques et des contrôles.

Gestion de la bibliothèque de réglementations

OpenPages PCM offre un référentiel de données centralisé unique qui permet de gérer la conformité à plusieurs réglementations. Les membres de l'équipe chargée de la conformité peuvent gérer une bibliothèque centralisée de lois, de réglementations et de meilleures pratiques, et suivre et surveiller les modifications externes apportées aux réglementations au fil du temps.

Grâce à cette approche centralisée, OpenPages PCM peut fonctionner en tant que « service partagé » pour les organisations, permettant à différents services, entités juridiques et unités commerciales d'harmoniser et de standardiser leurs programmes de conformité pour promouvoir une approche standardisée et efficace de la conformité. Il est également possible de faire correspondre des réglementations similaires aux mêmes contrôles, ce qui permet aux organisations de conserver de la souplesse et d'adopter la meilleure approche possible pour la gestion des règles et de la conformité.



Regulatory Applicability Matrix

Reporting Period: Current Reporting Period

Business Entity: /Global Financial Services — Finish

Category	Name	Global Financial Services	Global Financial Services / North America	Asia Pac / Retail Banking	Corporate / Compliance	North America / Agency Services	North America / Commercial Banking	North America / Corporate Finance	North America / Retail Banking	North America / Sales
Common Practices	AICPA/CICA Generally Accepted Privacy Principles								√	
	BCI - Good Practice Guidelines 2007			√						
	CobiT 4.0 - Level 1		√							
	Cobit 4.0 - Level 2	√								
	COSO - Enterprise Risk Management - Integrated Framework	√								
	ISO 15489 - Part 1			√						
Federal	Julie test mandate				√					
Healthcare and Life Science	HIPAA				√	√	√			√
Industry Standards	NERC CIP-002-1: Critical Cyber Asset Identification							√		
Payment Card	PCI DSS Security Scanning Procedures				√					√

Jan 21, 2011 - 1 - 4:12:06 PM

Figure 1 : Le tableau de bord réglementaire d'OpenPages PCM offre un aperçu rapide de la situation de l'organisation vis-à-vis de l'ensemble des réglementations qui la concernent.

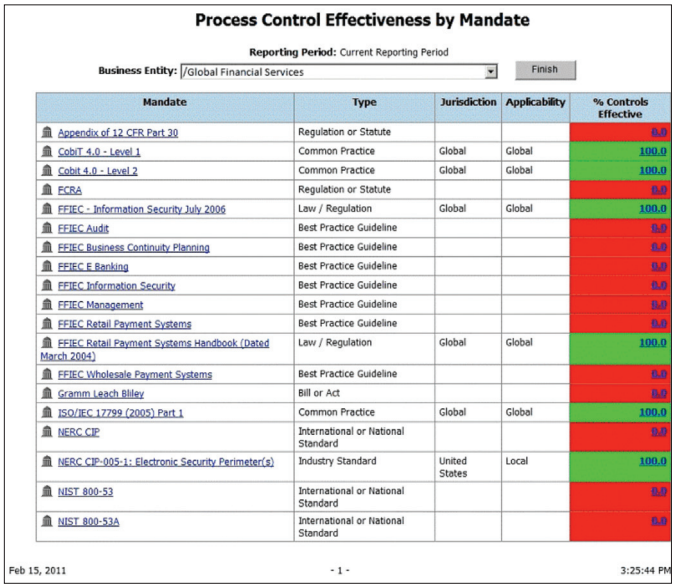
Aide à la décision et tableaux de bord

L'un des concepts essentiels de la gestion des règles et de la conformité est la transparence : pouvoir voir se qui se passe dans l'organisation du point de vue de la conformité. OpenPages PCM offre cette visibilité sous la forme d'une génération de rapports entièrement configurable pour toutes les unités fonctionnelles, qui apporte des tableaux de bord et des fonctionnalités d'analyse riches, interactifs et en temps réel.

Les tableaux de bord dynamiques, les graphiques et les rapports indiquent l'état de la conformité aux différentes réglementations. Les utilisateurs peuvent également explorer des sous-rapports pour procéder à une analyse des causes premières et créer des rapports à l'aide d'un outil de conception ad hoc fonctionnant par glisser-déposer dans un navigateur Web.

OpenPages GRC propose également l'outil CrossTrack et permet ainsi d'explorer les sous-rapports d'un rapport et les données détaillées sous-jacentes. Cette possibilité facilite la production de rapports contextuels adaptés aux tâches spécifiques des utilisateurs.

En outre, OpenPages PCM est dynamique, ce qui fait que les problèmes sont signalés – et les notifications émises – immédiatement par l'intermédiaire du flux de travail d'OpenPages PCM. La génération dynamique de rapports améliore le niveau global de précision et d'efficacité.



Process Control Effectiveness by Mandate

Reporting Period: Current Reporting Period

Business Entity: /Global Financial Services — Finish

Mandate	Type	Jurisdiction	Applicability	% Controls Effective
Appendix of 12 CFR Part 30	Regulation or Statute			0.0
CobiT 4.0 - Level 1	Common Practice	Global	Global	100.0
Cobit 4.0 - Level 2	Common Practice	Global	Global	100.0
FCRA	Regulation or Statute			0.0
FFIEC - Information Security July 2006	Law / Regulation	Global	Global	100.0
FFIEC Audit	Best Practice Guideline			0.0
FFIEC Business Continuity Planning	Best Practice Guideline			0.0
FFIEC E Banking	Best Practice Guideline			0.0
FFIEC Information Security	Best Practice Guideline			0.0
FFIEC Management	Best Practice Guideline			0.0
FFIEC Retail Payment Systems	Best Practice Guideline			0.0
FFIEC Retail Payment Systems Handbook (Dated March 2004)	Law / Regulation	Global	Global	100.0
FFIEC Wholesale Payment Systems	Best Practice Guideline			0.0
Gramm Leach Bliley	Bill or Act			0.0
ISO/IEC 17799 (2005) Part 1	Common Practice	Global	Global	100.0
NERC CIP	International or National Standard			0.0
NERC CIP-005-1: Electronic Security Perimeter(s)	Industry Standard	United States	Local	100.0
NIST 800-53	International or National Standard			0.0
NIST 800-53A	International or National Standard			0.0

Feb 15, 2011 - 1 - 3:25:44 PM

Figure 2: Le rapport d'OpenPages PCM indique le détail des réglementations clés par secteur d'activité.

Flux de travail automatisé

OpenPages PCM utilise le flux de travail robuste et souple d'OpenPages GRC pour automatiser la notification et l'achèvement des activités de gestion, telles que la conception et l'examen du fonctionnement.

Le flux de travail signale aux utilisateurs les différentes tâches et actions par l'intermédiaire de la Page d'accueil et d'alertes transmises par courrier électronique, et peut transmettre les avis d'incident et de défaillance de contrôle aux instances de contrôle des risques opérationnels et financiers. Il permet également aux cadres de voir les plans correctifs pour les éventuelles déviations en matière d'attitude vis-à-vis des risques, et d'attribuer et suivre les responsabilités employé par employé.

Entièrement configurable

OpenPages PCM est entièrement basé sur une interface Web et totalement configurable. Cela signifie que les responsables informatiques peuvent personnaliser et gérer le système sans faire appel à des ressources supplémentaires, réduisant ainsi le travail administratif.

Voici quelques-uns des éléments configurables de l'interface utilisateur d'OpenPages PCM :

- **Formulaires de données.** Configurez les zones, ajoutez ou supprimez des zones, affichez ou masquez des menus déroulants.
- **Interface utilisateur.** Configurez les libellés de l'interface, les noms des menus et les intitulés des boutons.
- **Internationalisation.** Configurez les traductions pour l es ajouts et les modifications apportés à l'interface.
- **Rapports.**Mettez automatiquement à jour le modèle de rapport pour refléter les modifications apportées à la configuration. .

La configurabilité d'OpenPages PCM offre de la souplesse aux organisations en leur permettant d'adapter leur système aux modifications qui interviennent dans leur environnement interne ou externe. Par exemple, il est possible d'ajuster la structure de données (hiérarchies et relations entre les données) tout en préservant l'état historique des données. Le flux de travail d'OpenPages PCM peut aussi être facilement modifié pour refléter les modifications apportées dans les activités de l'entreprise liées à la conformité.

Conclusion

Aujourd'hui, gérer les règles et la conformité est une nécessité absolue pour les entreprises. Cependant, étant donné que la complexité de l'environnement réglementaire suit une pente ascendante, les organisations doivent commencer à abandonner les méthodes manuelles et les approches en silos. Dans ce contexte d'accroissement continu des pressions réglementaires, les entreprises qui adopteront une approche transversale seront en mesure de limiter l'augmentation des coûts et de la complexité. Elles pourront également obtenir des informations précieuses sur les risques qui pèsent sur leurs processus essentiels et sont susceptibles d'affecter leurs performances, sous forme d'actions juridiques, d'amendes et de pénalités, ou d'atteintes à leur réputation ou à celle de leurs marques.

Abandonner progressivement les processus manuels dans le domaine du respect des réglementations implique de déployer une solution technologique capable de centraliser et gérer les activités liées à la conformité et d'offrir à la direction la visibilité requise sur la situation globale de l'organisation en la matière. La solution OpenPages PCM fournit tous les éléments indispensables pour permettre aux organisations de centraliser leurs activités liées à la conformité et de devenir des entreprises mieux gouvernées.

En mettant en œuvre une solution de gestion des règles et de la conformité telle qu'OpenPages PCM, les organisations deviennent capables de réduire la complexité inhérente au respect des réglementations, et d'offrir à leurs clients, employés et partenaires un service et des résultats de qualité supérieure, tout en limitant les risques globaux et en maîtrisant les coûts d'exploitation liés à la conformité.

À propos d'IBM Business Analytics

Les logiciels IBM Business Analytics aident les entreprises à mesurer, comprendre et anticiper leur performance financière et opérationnelle en transformant les données en décisions et les décisions en action. IBM propose à cet effet une gamme complète et unifiée d'applications d'aide à la décision, d'analyse prédictive avancée, de pilotage de la stratégie et des performances financières, de gouvernance, de gestion du risque et de la conformité. Avec les logiciels IBM, les entreprises peuvent détecter les tendances, les schémas récurrents et les anomalies, comparer des scénarios de simulation, prédire les menaces et opportunités potentielles, identifier et gérer les risques principaux, et planifier, budgéter et prévoir les ressources.

Compagnie IBM France
17, Avenue de l'Europe
92275 Bois-Colombes Cedex
France

L'adresse de la page d'accueil IBM est :
ibm.com/fr

[1] Information Week. How to Implement an Integrated GRC Architecture, Janvier 2008. Copié sur le site http://www.informationweek.com/whitepaper/Software/Business-Systems-Management/how-to-implement-an-integrated-grc-architectur-wp1262847996397 le 15 avril 2011.

Merci de recycler ce document

Business Analytics software

YTW03136-FRFR-01