MEGA
SEE THE BIGGER PICTURE

Assurer une gestion efficace des risques en intégrant le contrôle interne et la conformité aux processus opérationnels

Livre blanc

Sommaire

1. Le contrôle interne et la conformité au service de la protection de l'entreprise

Aujourd'hui, les entreprises font face à une avalanche de réglementations telles que la loi française Sapin 2, le Sarbanes-Oxley Act, la loi italienne 262, le Senior Manager and Certification Regime (SM&CR) au Royaume-Uni, le Foreign Corrupt Practices Act (FCPA), le Healthcare Insurance Portability and Accountability Act (HIPAA), ainsi que de multiples lois de Lutte Contre le Blanchiment d'argent (LCB) et tant d'autres. De plus, les autorités de régulation à travers le monde demandent d'avoir une visibilité accrue au niveau des processus de l'entreprise afin d'apprécier l'efficacité du dispositif de maitrise.

Garantir la conformité à ces réglementations, ainsi que le respect des normes sectorielles et des règles internes, restent une tâche ardue pour de nombreuses organisations. **Un défi qui nécessite d'avoir une vision holistique de l'ensemble des processus de l'organisation** et d'identifier rapidement les déficiences afin de procéder à des mesures de mitigation.

Le non-respect de ces exigences en temps voulu peut non seulement entraîner de lourdes amendes et des dommages durables liés à la réputation de l'entreprise, mais peut également mettre en danger la survie de celle-ci. **Dans ce contexte, une visibilité à la fois totale et précise (granulaire) sur les processus métier et leur état de risque et de conformité en temps réel est essentielle. Cela permet d'éviter non seulement les risques de conformité, mais également les risques non traités ou « hors radar » qui peuvent proliférer dans l'organisation conduisant à des déficiences opérationnelles, des fraudes, etc.**

Sans surprise, de nombreuses entreprises estiment qu'analyser et répondre à toutes ces exigences - en particulier celles liées à la réglementation - est un véritable défi. Elles s'appuient généralement sur les fonctions risque, contrôle et audit interne (2ème et 3ème ligne tels que définis par l'IIA) qui fonctionnent généralement avec un budget et des ressources limitées pour des résultats parfois mitigés.

Cependant, en intégrant le contrôle interne et la conformité tout au long du cycle de vie des processus métier dans une approche GRC (Gouvernance, Risque et Conformité) centrée sur les processus métier, les fonctions risque et contrôle sont en mesure de contribuer activement à la performance et à la résilience des processus pour s'acquitter de leur mandat.

L'adoption de cette approche est aujourd'hui essentielle. Elle améliore non seulement l'efficacité et la conformité aux réglementations, mais elle réduit également les risques opérationnels, renforce la qualité des processus, réduit les coûts et fluidifie la collaboration entre le contrôle interne, la gestion des risques et les propriétaires de processus. Grâce à cette méthodologie, les fonctions risque et contrôle fonctionnent plus efficacement et deviennent une source d'amélioration opérationnelle. C'est ce que ce document mettra en exergue.

2. Les nouvelles attentes des fonctions de contrôle interne et de conformité

Les défis typiques liés au contrôle Interne et à la conformité

La plupart des ressources d'une organisation ont tendance à se concentrer sur la préservation d'une croissance constante et la gestion opérationnelle de l'activité plutôt que sur des initiatives de gestion des risques et des contrôles. Les organisations comptent souvent sur la gouvernance et les fonctions risque et contrôle pour les protéger des risques opérationnels. Cependant, sans une visibilité claire sur les processus métier et leurs responsables, les gestionnaires de risques peuvent passer à côté de risques potentiels, augmentant ainsi la probabilité de survenue d'incidents.

Voici les cinq problématiques majeures rencontrées par la gestion des risques, le contrôle interne et la conformité, ainsi que les opportunités d'amélioration pour chacune :

Problématique	Difficultés	Opportunités
Faire disparaître les silos entre les responsables de processus et les contrôleurs internes	• Toutes les fonctions de gouvernance (risques et autres) ont souvent des visions différentes de l'organisation et de ses processus • Les responsables de processus peuvent voir la conformité comme un obstacle à l'efficience • L'absence d'un référentiel de processus commun amène un allongement des durées d'audits, de vérification des processus et d'évaluations des risques • Cela engendre une duplication des taches et un gaspillage de ressources	• La centralisation de tous les processus, risques et contrôles dans un référentiel unique donne aux parties prenantes un accès instantané aux bonnes informations • Une approche collaborative de la gestion des risques fédère l'expertise et suscite l'engagement des parties prenantes • Une meilleure visibilité des tâches à valeur ajoutée entraîne une rationalisation plus précise des efforts et du temps • L'organisation peut rendre compte en toute confiance d'une gestion des processus en accord avec la conformité et la séparation des tâches
Evaluer les risques opérationnels	• Difficile pour les fonctions de gouvernance d'évaluer l'impact des risques sur l'organisation par manque de visibilité sur les processus • L'impact d'un risque est souvent cantonné aux conséquences à court terme, sans compréhension des effets de bord que peut provoquer un incident • Les descriptions de processus sont souvent longues et indigestes	• Maintenir un référentiel commun de processus permet aux gestionnaires de risques et contrôles d'analyser les liens avec les processus de l'organisation et d'évaluer plus aisément l'impact du risque pour concevoir des contrôles. • Utiliser les diagrammes de processus pour remplacer les longues descriptions et ainsi identifier plus facilement les risques potentiels

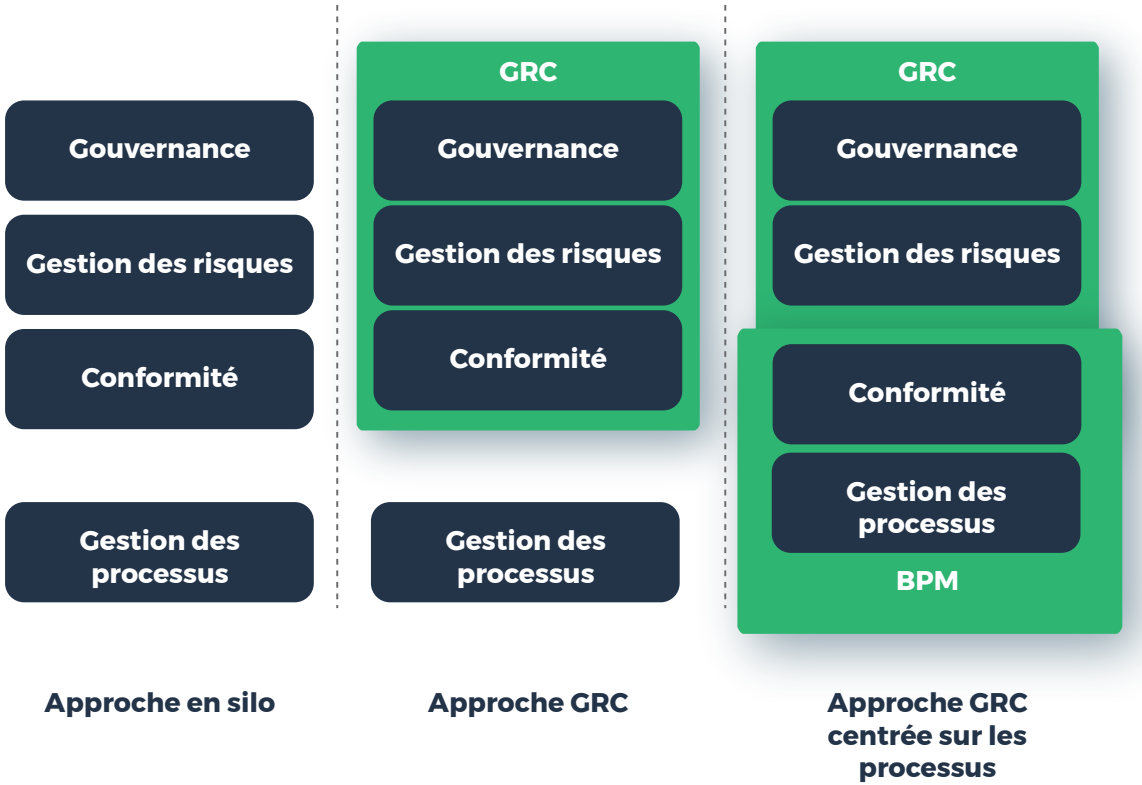
Problématique	Difficultés	Opportunités
Consolider les niveaux de risque	• Les entreprises ont du mal à agréger les risques par lignes métiers et processus • Par conséquent, il est pratiquement impossible de fournir une vue d'ensemble de l'univers des risques à la direction générale	• La gestion des risques et des contrôles dans un référentiel central partagé, permet d'avoir une approche fédérée de l'évaluation des risques et des contrôles en utilisant une méthodologie commune • Alimentée par des données pertinentes, la consolidation des risques se fait de manière transparente dans l'ensemble de l'organisation
Anticiper les risques futurs	• Le manque de vision unifiée des risques et des processus rend difficile l'anticipation des risques et des contrôles associés • Les organisations doivent anticiper et être en mesure de déployer des plans de continuité d'activité basés sur des analyses d'impact	• Avoir une visibilité sur tous les processus et leurs interdépendances permet d'identifier plus facilement les risques opérationnels potentiels, de mieux anticiper les déficiences et de planifier la continuité des activités • Être en mesure de visualiser rapidement les incidents au niveau d'une étape du processus et leurs effets potentiels sur l'organisation permet une adaptation rapide
Surveiller les plans de remédiation	• En raison de ressources limitées, les équipes de contrôle interne et de conformité ont du mal à équilibrer l'atténuation des risques et identifier les moyens d'améliorer l'efficacité des processus • La surveillance des plans d'actions sans référentiel centralisé entraîne des inexactitudes, des redondances et des risques plus élevés	• La surveillance des risques et des plans de remédiation sur un référentiel unique qui utilise des workflows automatisés augmente la protection de l'entreprise, la traçabilité et évite la duplication des efforts • L'utilisation d'un outil qui fournit des alertes et des conseils pour piloter les plans d'actions permet une approche proactive de la gestion des risques

L'évolution du contrôle interne, de la conformité et des processus métier

Afin de relever ces défis, les organisations doivent se tourner vers une solution qui leur fournit une représentation holistique contextualisée de leurs risques, contrôles et processus métier. Cela permet aux parties prenantes de prendre des décisions efficaces, simples, de manière organisée et d'avoir une compréhension globale de la conformité nécessaire dans l'ensemble de l'organisation. Cette approche s'appuie notamment sur l'utilisation de diagramme de flux d'information simplifiés.

L'objectif est d'obtenir une vue intégrée de la gestion des processus métier (Business Process Management) et des risques. Le diagramme ci-dessous représente l'évolution ces dernières années de l'intégration de la gestion des processus métier avec celle de la Gouvernance, Risques et Conformité (GRC).

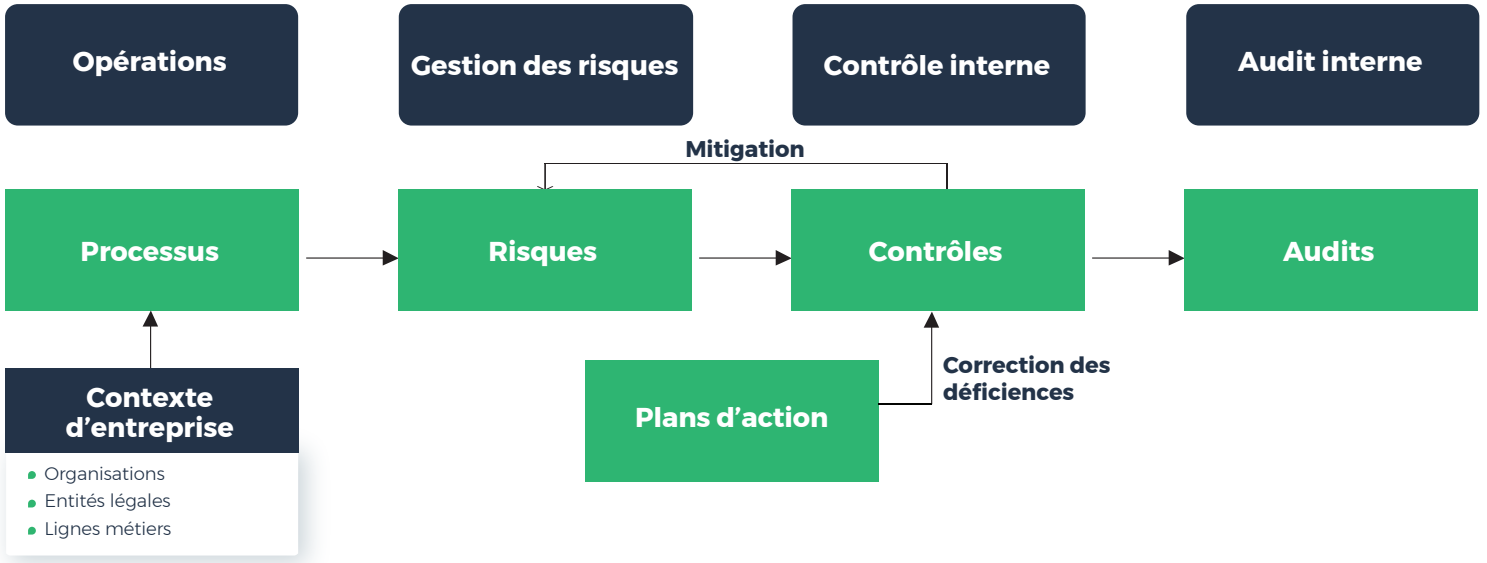
Evolution de l'integration du BPM et de la GRC



Une gestion des risques efficiente nécessite une vue à 360° des liens entre les processus métier, les réglementations, les risques, les contrôles et l'ensemble des exigences internes. Cette approche holistique de la gestion des risques permet de rationaliser les efforts entre les départements, brisant les silos et facilitant l'anticipation des risques à effet domino. Elle facilite également les contrôles et audits qualité.

Le diagramme ci-dessous montre les liens logiques entre les processus et les activités GRC.

Relation logique entre le BPM et la GRC



Voici les étapes clés à respecter lors de la mise en place d'une activité GRC centrée sur les processus métier :

- Avoir une vue claire de la contextualisation des risques par processus métier et de leurs interconnexions
- Hiérarchiser les efforts de mitigation via l'utilisation de campagnes d'autoévaluations des contrôles en fonction de la criticité métier

L'intégration du contrôle interne et de la conformité aux processus dès la phase de conception initiale, et à un niveau granulaire, permet aux propriétaires de processus, aux gestionnaires des risques et aux contrôleurs internes de collaborer de manière efficace. Cette connexion et étroite collaboration sont essentielles pour gérer efficacement les risques et la conformité.

Cette approche est en phase avec **le nouveau modèle de l'IIA des « 3 lignes »** qui encourage la communication, la coopération et la collaboration entre les différentes lignes, avec le postulat que tous les rôles doivent travailler ensemble pour contribuer à la protection de l'organisation et à la création de valeur. Cette méthodologie, qui s'articule autour de la transparence et l'efficacité, a évolué au fil du temps sur la base de cette réflexion.

3. Comment intégrer le contrôle interne et la conformité aux processus métier ?

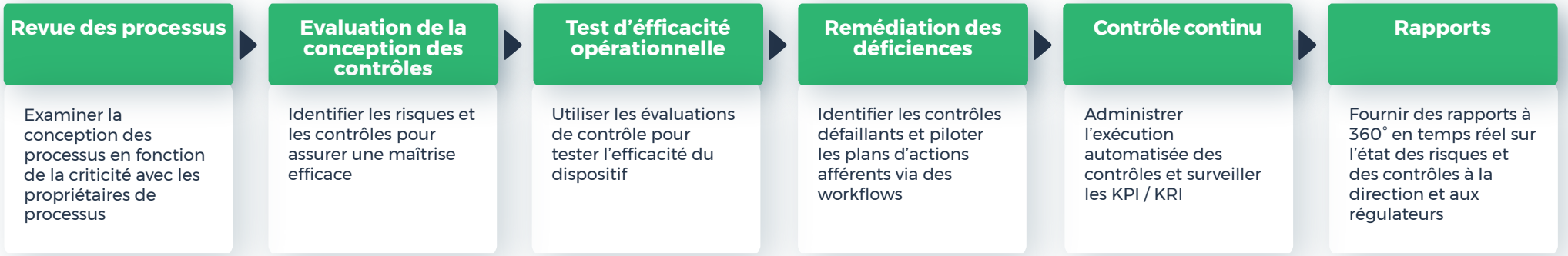
Partager une vision commune et briser les silos est une condition préalable

Fédérer le contrôle interne et la conformité au sein des processus métier implique le partage d'une vision commune à travers chaque fonction. Un vecteur important à cette évolution réside dans l'utilisation partagée des diagrammes de processus sous format interactif. Ceux-ci sont interconnectés et régulièrement mis à jour bénéficiant aux contrôleurs internes, à la conformité, ainsi qu'aux propriétaires de processus en :

- Accélérant l'analyse des processus et les contrôles qualité
- Offrant une visibilité sur les différentes phases constituant les processus et la séparation des tâches
- Améliorant l'évaluation des impacts des risques dans toute l'organisation
- Favorisant l'évaluation de la conception des contrôles pour renforcer la protection de l'organisation
- Simplifiant le suivi des plans de remédiation
- Réduisant les efforts de conformité et de mitigation

L'utilisation d'un référentiel commun via une approche GRC centrée sur les processus métier contribuera davantage à la diffusion d'une culture du risque dans toute l'organisation – ce qui est une base essentielle à une saine gestion des risques.

Le contrôle interne et la conformité fonctionnent généralement selon une séquence en six étapes :



Cette approche peut être efficace. Cependant, un écueil typique se produit lorsque les propriétaires de processus, les contrôleurs internes et les responsables de la conformité utilisent des outils, formats ou référentiels différents : cela laisse la porte ouverte aux risques et défaillances de contrôle avec des conséquences potentiellement désastreuses - sans parler de duplication des tâches et d'inefficacités.

En comparaison, l'utilisation et le partage d'un référentiel commun pour les processus, les risques et les contrôles entre les fonctions améliorent non seulement la conformité de l'entreprise aux réglementations et aux normes, mais renforcent également son efficacité et sa résilience. Cette démarche agit comme un catalyseur pour :

- Partager une culture de la gestion du risque dans toute l'organisation
- Affiner les pratiques de gestion des risques et réduire les déficiences opérationnelles
- Mettre en place une approche standardisée pour la conception des processus en vue d'accroître leur efficacité
- Améliorer la revue du processus qualité
- Soutenir la mise en place des plans de continuité d'activités

Les principaux facteurs clés de succès dans le cadre de cette démarche sont donc les suivants :

- Utiliser un référentiel unique pour les processus, les risques et les contrôles, partagé entre les propriétaires de processus et toutes les fonctions risques et contrôle afin d'obtenir une vue holistique combinée de l'environnement des risques de l'entreprise ;
- Permettre aux mêmes fonctions de travailler à un niveau plus granulaire via l'utilisation de diagrammes de processus pour s'assurer de l'efficacité du dispositif ;
- Maintenir à jour le référentiel des processus - car les processus, les réglementations et les exigences changent constamment et des problèmes mineurs non répertoriés en amont peuvent entraîner des problèmes majeurs en aval ;
- Apporter de l'agilité dès la conception des processus afin de permettre une adaptation rapide avec un minimum d'impact sur l'activité.

En intégrant le contrôle interne et la conformité aux processus, les entreprises peuvent améliorer leur résilience et adaptabilité. Cela leur permet de renforcer la conformité et de réduire le risque opérationnel, tout en améliorant la qualité des processus et en fournissant une approche fédérée de la gestion des risques dans toute l'organisation.

Les 5 étapes pour déployer une approche GRC centrée sur les processus

Une fois que l'organisation dispose d'une vision plus claire des défis et opportunités liés à une approche GRC centrée sur les processus, nous pouvons passer à sa mise en œuvre. Cette méthodologie va non seulement booster l'implication des fonctions risque et contrôle, mais également améliorer la qualité et l'efficacité des processus, la communication transverse et instituer une culture du risque dans l'entreprise.

Voici les étapes clés pour mettre en place cette méthodologie :

1. Cartographie des processus, des risques et des contrôles

Tout d'abord, il est recommandé de cartographier et de lier les processus métier aux réglementations, risques, contrôles et aux lignes métier. Cela permet d'avoir une vue agrégée et contextuelle très utile pour la direction générale, ainsi que pour les régulateurs. Les processus doivent également être connectés aux objectifs de l'entreprise, aux normes, aux comptes financiers (pour la conformité SOX), ainsi qu'aux personnes responsables (Séparation des taches) en utilisant une simple vue hiérarchique. Cela aide en outre à :

- Simplifier l'identification des risques et des contrôles en utilisant les diagrammes de processus métier pour remplacer (ou compléter) le long processus narratif
- Visualiser clairement où et comment positionner les efforts de maitrise sur les diagrammes de processus tout en évaluant les risques et la conception des contrôles
- Développer des vues et des rapports qui affichent la chaîne des impacts des risques sur les processus pour éviter l'omission de certains risques - en s'assurant que la direction a une visibilité complète sur les initiatives de remédiation et la séparation des tâches
- Effectuer une évaluation régulière des contrôles, mener des revues de conception de processus pour s'assurer que les risques et les contrôles sont toujours pertinents et à jour, et évaluer l'efficacité de la conception des contrôles pour garantir une maitrise adéquate des risques

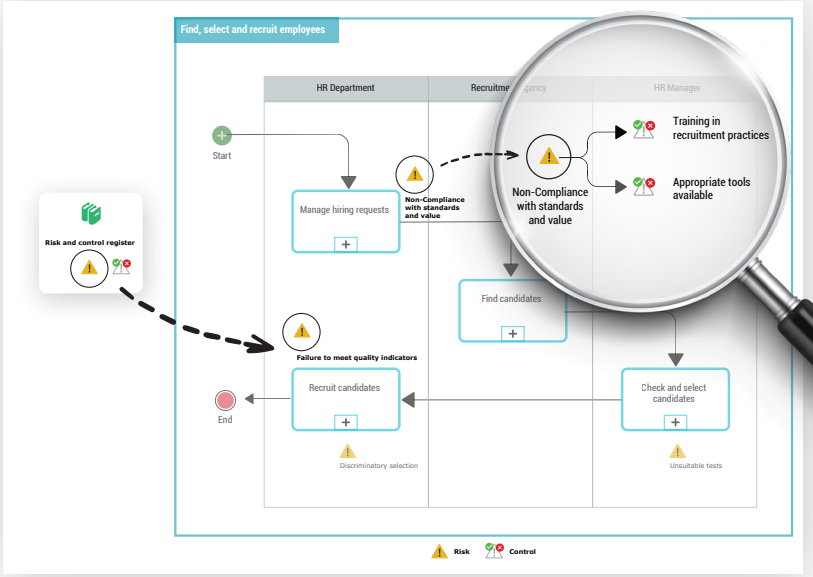
Mais ce n'est pas la mission d'une seule et unique personne. C'est le résultat d'un effort de collaboration dynamique impliquant les propriétaires de processus, le contrôleur interne, les gestionnaires des risques et les auditeurs (1ère, 2ème et 3ème ligne) pour s'assurer que les processus métier sont régulièrement revus et sécurisés. Les captures d'écran suivantes montrent comment cela peut être fait avec un référentiel interconnecté.

Vue GRC centrée sur les processus

2 .Evaluation de la conception du dispositif de maitrise

Ensuite, il est recommandé d'identifier les risques et les contrôles au cours de la revue du processus, et de s'assurer ainsi que les contrôles sont efficacement intégrés dans la conception du processus pour atténuer les risques en conséquence. Cela aide à :

- Identifier et supprimer les contrôles redondants et inefficaces – permettant ainsi d'optimiser les coûts
- Améliorer l'efficacité des processus, en examinant régulièrement le dispositif de maitrise associé afin de garantir sa pertinence dans des conditions de marché changeantes.
- Partager des rapports et des informations sur les niveaux de risque et de contrôle actuels à l'aide de cartes de chaleur (heatmaps) consolidées qui peuvent elles-mêmes être filtrées par secteur d'activité, entité juridique et processus.

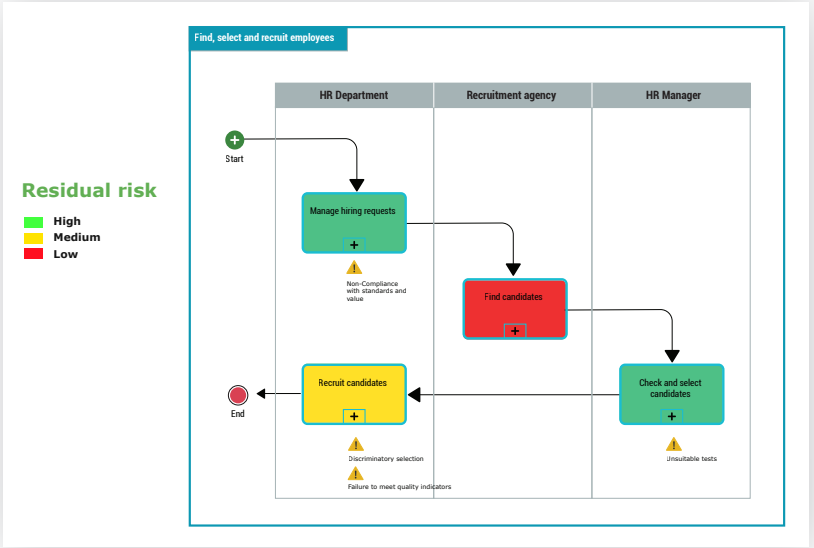


Vue GRC centrée sur un processus

3. Evaluation de l'efficacité du dispositif de maitrise

La troisième étape de l'adoption d'une approche GRC centrée sur les processus métier consiste à tester l'efficacité des contrôles au sein du dispositif de maitrise. Pour que les entreprises arrivent aisément à ce résultat, il faut alors :

- Utiliser des campagnes d'évaluation (trimestrielles, semestrielles ou annuelles) pour effectuer des contrôles via des questionnaires afin de s'assurer que les contrôles sont non seulement bien conçus mais également efficaces
- Impliquer les correspondants contrôle interne via des alertes et des workflows automatisés pour garantir une collaboration fluide et efficace avec l'organisation
- Collaborer avec les propriétaires de processus pour identifier les contrôles qui peuvent être mal conçus en utilisant des méthodes de test appropriées (enquête, réexécution, observation ou inspection)
- Mettre en place des scénarios de test pour vérifier si les contrôles fonctionnent comme prévu
- Partager tous les résultats des évaluations de contrôle provenant du contrôle interne avec l'audit interne (et vice-versa) pour faciliter les travaux d'audit et permettre la comparaison des résultats via des rapports prêts à l'emploi.



Vue GRC centrée sur un processus après évaluation

4. Identification des déficiences et pilotage des plans d'action

Après l'évaluation, l'étape suivante consiste à identifier les déficiences, à créer des plans d'action et à suivre les progrès. Les meilleures pratiques à considérer incluent de :

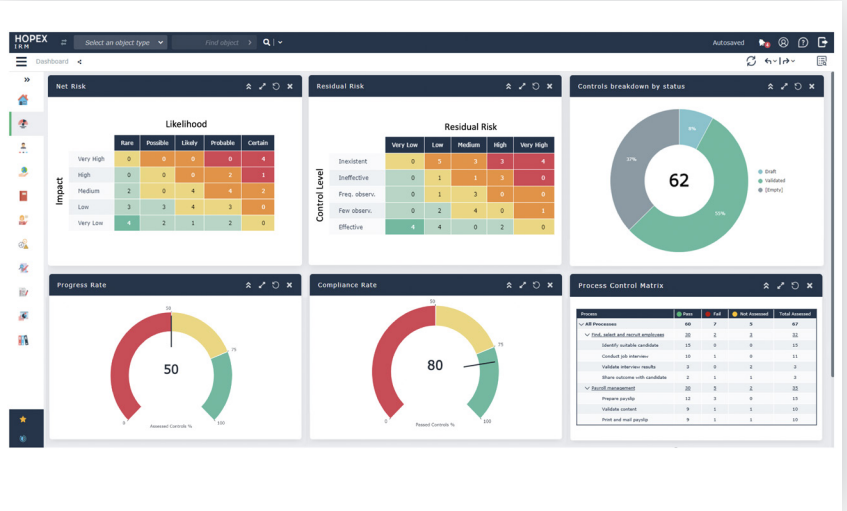
- Concevoir des plans d'action lorsque des déficiences sont identifiées et suivre leur exécution avec les propriétaires de processus
- Surveiller les efforts de mitigation directement sur les diagrammes des processus métier en reliant les plans d'action aux contrôles déficients
- Suivre les progrès du contrôle interne et de la conformité de manière centralisée et efficace

Vue GANTT de suivi des plans d'actions

5. Monitoring en continu des contrôles

Enfin, grâce à tous les efforts mentionnés précédemment, l'organisation peut désormais facilement surveiller en continu les contrôles. Un référentiel unique permet alors de :

- Mettre en place une surveillance continue des contrôles pour tester la robustesse du dispositif de maitrise des risques en utilisant l'automatisation des évaluations de manière simple et rapide.
- Alerter automatiquement les fonctions risque et contrôle et les propriétaires de processus en cas de défaillance du dispositif afin qu'ils puissent prendre les mesures appropriées et limiter les effets domino
- Se connecter à des systèmes externes via des API et des services Web pour collecter les résultats des évaluations de contrôle à une fréquence définie et en utilisant la collecte de KPI, KRI et KCI pour suivre leurs performances



Vue cockpit GRC

4. Les avantages d'une approche fédérée entre le contrôle interne, la conformité et les processus métier

Le manque d'une visibilité granulaire au niveau des processus peut compliquer l'évaluation des risques et la bonne définition des contrôles. Ce qui entrave la mise en place d'une gestion des risques efficace. L'intégration des risques et des contrôles au design des processus dans un référentiel unique et selon une méthodologie commune, permet aux organisations de démontrer à leur direction et aux autorités de réglementation la mise en place d'un dispositif de maitrise des risques robuste qui favorise l'efficacité opérationnelle.

Cette approche collaborative de la gestion des risques et des contrôles peut contribuer à rendre les opérations plus agiles, efficaces et adaptables aux changements au niveau des activités de l'entreprise, des exigences du marché et des changements règlementaires. L'approche GRC centrée sur les processus aide à se conformer aux règlementations mais aussi à :

- **Mettre en place une source unique et consolidée pour les activités GRC :** Gérer les processus, risques, contrôles, incidents et audits dans un référentiel unique permet aux équipes de travailler en synergie. Cela contribue à réduire les risques, améliorer les processus et apporter une vision consolidée des risques à la direction.
- **Réduire les risques opérationnels :** S'appuyer sur la cartographie des processus permet de disposer d'une meilleure analyse d'impacts des risques sur les opérations et d'identifier les opportunités de mitigation.
- **Standardiser les processus et gagner en productivité :** Cartographier les processus permet de standardiser les méthodes de travail dans l'entreprise. Partager les processus à travers un portail dynamique facilite l'accès à l'information.
- **Améliorer la résilience opérationnelle :** Evaluer les risques et contrôles en collaboration avec les propriétaires de processus et émettre des recommandations directement au niveau des processus donne la possibilité de lancer de réelles actions d'améliorations. Cartographier les processus permet également d'être conforme vis à vis des Standards Qualité (ex. ISO 9001)
- **Assurer la continuité d'activités :** Cartographier les processus et les évaluer constituent une étape clé pour réussir son plan de continuité d'activité.
- **Diffuser une culture de la gestion de risques à travers l'organisation :** Le partage d'un référentiel de risques, de contrôles et de processus permet aux collaborateurs de partager les mêmes définitions et taxonomies - et donc de parler le même langage
- **Encourager la collaboration :** Une approche fédérée permet de partager une vision commune et unifiée du risque de manière consolidée afin de mieux anticiper les risques futurs et d'éviter les incidents.

5. Pour une gestion efficace des risques au service de la résilience de l'organisation

Traditionnellement, dans les organisations, les processus métier et la gestion des risques étaient souvent des disciplines cloisonnées avec des interactions limitées. Mais la nature dynamique, complexe et interdépendante dans laquelle les entreprises opèrent aujourd'hui, requiert une nouvelle approche.

L'intégration de la gestion des risques, du contrôle interne et de la conformité aux processus via une approche GRC centrée sur les processus redéfinit les relations entre les processus métier et la gestion des risques. Il exploite les deux disciplines de manière moderne et innovante afin d'avoir une meilleure compréhension et un contrôle plus granulaire des risques liés aux processus métier, tout en offrant une transparence totale à la direction et aux régulateurs.

En fournissant une image fidèle des interdépendances entre les risques liés aux différents processus et de leurs impacts sur l'organisation, cette méthodologie apporte des avantages indéniables. Les plans de mitigation peuvent être directement intégrés dans la conception des processus, réduisant ainsi les risques et les coûts opérationnels, brisant les silos et apportant des améliorations opérationnelles.

La mise en place et l'utilisation d'une plateforme connectée présente ainsi de nombreux avantages. Elle est vectrice d'une meilleure résilience opérationnelle et d'une plus grande agilité, tout en soutenant la transformation de l'entreprise et sa continuité d'activités. Ce qui est une nécessité dans l'environnement actuel.

À propos de MEGA

Fondé en 1991, MEGA est un éditeur français d'envergure mondiale reconnu leader international sur le marché depuis plus de onze ans. Présente sur les 5 continents, l'entreprise travaille en partenariat avec ses clients et les accompagne dans leurs projets de gouvernance et de transformation. MEGA les aide à prendre les bonnes décisions pour optimiser leur mode de fonctionnement et accélérer la création de valeur. La plateforme HOPEX connecte et centralise l'ensemble des informations liées aux métiers, au système d'information, aux données et aux risques dans un référentiel commun tout en s'intégrant parfaitement dans l'écosystème existant de l'entreprise. Les équipes Services de MEGA accompagnent et guident les clients dans leurs projets en suivant une approche pragmatique qui garantit un retour sur investissement rapide.

MEGA
SEE THE BIGGER PICTURE

www.mega.com