THE POWER OF BEING UNDERSTOOD
AUDIT | EXPERTISE | CONSEIL

RSM

Risque et Conformité

Les buzzwords qui font l'actualité en 2024

L'édito

J. Grignon

Jocelyn Grignon
Associé
RSM France

GRC, Sapin 2, DORA, NIS2, CSRD ... et bien d'autres « buzzword » viennent régulièrement enrichir (pour ne pas dire envahir !) le jargon des professionnels en charge de la gestion des risques, de l'audit interne, de la conformité ou de l'ESG en entreprise. Au-delà d'abréviations à la mode, il s'agit surtout d'injonctions législatives multiples, qui s'imposent en ordre dispersé. Toujours plus ciblées, ces innovations règlementaires ont un point commun : elles nécessitent l'engagement de toutes les lignes de défense de l'organisation, jusqu'à son plus haut niveau.

Lors de notre événement « Data, IA, Sapin 2, CSRD : engagez vos lignes de défense » organisé par RSM et Diligent le 5 mars dernier à Paris, nous avons eu le plaisir d'échanger entre experts et professionnels du contrôle au sein de grandes sociétés françaises. Des réponses clés ont été apportées pour relever ces défis : mise en cohérence, création de liens entre les différents niveaux de décision et parties prenantes, réconciliation des visions micro et macro, renfort de la digitalisation, etc.

De là, l'idée d'en faire une restitution sous forme de livre blanc – à destination des dirigeants, responsables du risque, de l'audit interne, des finances ou encore de l'ESG – afin que les « buzz words » du contrôle et de la conformité au cœur de l'actualité règlementaire 2024 n'aient plus de secret pour vous...

Sommaire

01

Gouvernance, Risque
& Conformité

Comment transformer sa stratégie GRC ?

Jocelyn Grignon
Associé RSM France
M. jocelyn.grignon@rsmfrance.fr
Se connecter sur Linkedin!

Découvrir l'accompagnement RSM :
Digitalisation des fonctions contrôle et conformité

> “La digitalisation n'est pas un simple outil de modernisation, c'est une nécessité pour accroître l'efficacité de la GRC.”
>
> **Jocelyn Grignon** | Associé RSM France

Décryptage

Dans un monde professionnel en constante évolution, où la complexité des réglementations et la rapidité du changement posent des défis sans précédent, la nécessité de déchiffrer le véritable impact de la Gouvernance, du Risque et de la Conformité (GRC) n'a jamais été aussi cruciale. Comment la GRC, correctement appliquée et digitalisée, devient un pilier central pour les entreprises aspirant à l'excellence stratégique et opérationnelle ?

La pandémie de COVID-19 a testé la résilience des entreprises, révélant l'importance d'une gouvernance solide et d'une préparation aux crises. La réussite dans le domaine de la GRC repose sur la convergence et la collaboration, utilisant la digitalisation pour unifier les efforts et créer une synergie à travers l'organisation.

Le rôle primordial de la GRC

Au cœur de chaque entreprise, les professionnels de la GRC (Gouvernance du Risque et de la Conformité) jouent un rôle indispensable. Ils ne sont pas seulement des gardiens des processus internes mais des facilitateurs essentiels pour la réalisation des objectifs stratégiques. Leur travail soutient directement la gouvernance, en s'assurant que les actions décidées sont menées à bien dans le respect des lois et des réglementations. C'est une mission de la plus haute importance, car elle touche directement à la capacité d'une entreprise à naviguer dans un environnement complexe et réglementé.

L'impact transformateur de la digitalisation

La digitalisation n'est pas un simple outil de modernisation; c'est une nécessité pour accroître l'efficacité de la GRC. Elle permet de dépasser le sentiment d'être submergé par les obligations de conformité pour se focaliser sur le cœur de métier. En utilisant les technologies numériques, nous pouvons non seulement optimiser les processus de conformité mais aussi devenir de véritables partenaires stratégiques pour l'entreprise.

Satisfaire les parties prenantes

Les entreprises, sous la surveillance de divers acteurs dont le public exigeant sur l'éthique, font face à des risques réputationnels accrus. Les incidents mineurs peuvent engendrer de graves crises médiatiques. La digitalisation devient essentielle, offrant une veille et gestion proactive des signaux faibles pour anticiper les crises. L'adoption de la digitalisation est cruciale pour maintenir la réputation et la pérennité des entreprises dans cet environnement vigilant.

Convergence et collaboration

La digitalisation n'est pas un simple outil de modernisation; c'est une nécessité pour accroître l'efficacité de la GRC. Elle permet de dépasser le sentiment d'être submergé par les obligations de conformité pour se focaliser sur le cœur de métier. En utilisant les technologies numériques, nous pouvons non seulement optimiser les processus de conformité mais aussi devenir de véritables partenaires stratégiques pour l'entreprise.

L'un des aspects les plus cruciaux pour réussir dans le domaine de la GRC est la capacité à unifier les efforts à travers l'organisation. Pour les multinationales, cela signifie engager de multiples parties prenantes autour d'outils communs et de pratiques cohérentes. L'objectif est de créer une synergie entre les différentes lignes de défense, en tirant parti de la digitalisation pour une gestion plus légère et automatisée de la GRC.

En conclusion, derrière les buzzwords, la GRC incarne une fonction stratégique critique pour les entreprises. En dépassant les concepts pour se concentrer sur l'action, nous pouvons renforcer la gouvernance, gérer les risques de manière plus efficace et garantir une conformité robuste. La clé réside dans l'adoption de la digitalisation et dans une approche intégrée qui favorise la collaboration et l'efficience. Ensemble, nous pouvons naviguer vers un avenir où la GRC est non seulement une obligation mais une véritable force propulsive pour l'entreprise.

02

Sapin 2, Compliance, Risk & Thirdparty Management

Intégration et pragmatisme : les nouvelles frontières de la conformité

Jean-Philippe Bernard
Associé RSM France
M. jean-philippe.bernard@rsmfrance.fr
Se connecter sur Linkedin!

Découvrir l'accompagnement RSM :
Risk Advisory

> La réglementation évolue, et avec elle, notre conception de la conformité qui s'étend au-delà de nos clients jusqu'à l'ensemble de notre écosystème.
>
> **Jean-Philippe Bernard** | Associé RSM France

Décryptage

Dans un environnement réglementaire en constante évolution, les entreprises sont confrontées à un défi majeur : Comment intégrer de manière fluide et efficace les exigences de conformité sans se laisser submerger ?

Au-delà de l'empilement des obligations

La conformité, dans son essence, ne devrait pas être perçue comme un empilement d'obligations mais comme une opportunité d'intégrer de manière native ces exigences dans nos processus d'affaires. L'objectif est de dépasser cette logique d'empilement pour travailler de façon plus fluide et intégrée, alignant les démarches de conformité avec les objectifs business de l'entreprise.

L'entreprise étendue et la maîtrise des tiers

La réglementation évolue, et avec elle, notre conception de la conformité s'étend au-delà de nos clients jusqu'à l'ensemble de notre écosystème. Cela inclut les fournisseurs, les partenaires et toutes les parties prenantes avec lesquelles nous interagissons. Cette "entreprise étendue" nous impose de maîtriser nos relations d'affaires non seulement pour satisfaire les exigences réglementaires mais également pour assumer notre responsabilité sociétale et environnementale.

La digitalisation au cœur de la conformité

La digitalisation est un pilier qui permet de connecter et de rationaliser nos efforts de conformité. En adoptant une approche numérique, nous pouvons assurer une cohérence entre les différentes cartographies des risques et développer des programmes de conformité qui sont non seulement intégrés mais également transparents pour les utilisateurs finaux. Cela permet de dépasser la simple satisfaction des obligations pour faire de la conformité un avantage compétitif.

Une méthodologie convergente

Développer des programmes de conformité natifs exige de nous que nous prenions en compte nos processus et objectifs d'affaires dès le départ. Cela signifie identifier les risques, allouer les rôles et responsabilités adéquatement et intégrer les bonnes pratiques directement dans nos opérations quotidiennes. Une telle approche ne simplifie pas seulement la conformité mais la rend plus efficace et adaptée aux réalités de notre environnement d'affaires.

Vers une architecture de conformité cohérente

En fin de compte, l'objectif est de construire une architecture de conformité qui soit logique, méthodologique et convergente. En adoptant une approche pragmatique et proportionnelle, basée sur l'identification des risques et l'intégration des contrôles, nous pouvons créer des programmes qui répondent non seulement aux diverses obligations réglementaires mais qui soutiennent également les objectifs stratégiques de l'entreprise.

En conclusion, la conformité ne doit pas être vue comme un fardeau mais comme une opportunité d'améliorer nos opérations et de renforcer notre positionnement sur le marché. En adoptant une approche intégrée, pragmatique et numérisée, nous pouvons transformer les défis de la conformité en avantages compétitifs, soutenant ainsi la croissance et la résilience de notre entreprise dans un monde en constante évolution.

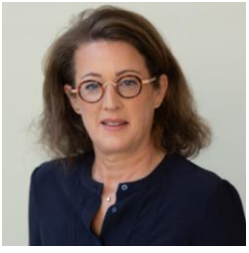
En savoir plus

- Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique

03

CSRD, ESG,
Taxonomie verte, ESRS

Révolution de la conformité et de la RSE dans le sillage de la CSRD



Amandine Duquesne
Associé RSM France
M. amandine.duquesne@rsmfrance.fr
Se connecter sur Linkedin !

Découvrir l'accompagnement RSM :
RSE & Finance durable

> La CSRD exige des entreprises qu'elles fournissent des informations détaillées sur leur performance en matière de RSE, allant bien au-delà de simples déclarations de bonnes intentions.

Amandine Duquesne | Associée RSM France

Décryptage

À l'aube d'une nouvelle ère de responsabilité et de transparence pour les entreprises européennes, la directive Corporate Sustainability Reporting Directive (CSRD) marque un tournant décisif dans la manière dont les enjeux de Responsabilité Sociale des Entreprises (RSE) et de reporting Environnemental, Social et de Gouvernance (ESG) sont appréhendés.

De la soft law à la hard law : un changement de paradigme

L'Union européenne, à travers le Green Deal et ses ambitions de neutralité carbone d'ici 2050, a pris des mesures décisives pour assurer que les entreprises contribuent de manière significative à ces objectifs. La directive CSRD est un pivot central de cette stratégie, visant à normaliser l'information extra-financière des entreprises, qui devra être auditée par un tiers indépendant. Ce qui était autrefois une démarche principalement volontaire devient désormais un impératif réglementaire, reflétant la nécessité d'une action plus cohérente et contrôlée en matière de RSE.

L'impact de la CSRD sur les entreprises

La CSRD exige des entreprises qu'elles fournissent des informations détaillées sur leur performance en matière de Durabilité, allant bien au-delà de simples déclarations de bonnes intentions. Cette directive élargit le spectre des entreprises concernées, passant de 10 000 à 50 000, et étend le périmètre de reporting à l'ensemble de la chaîne de valeur. Cela signifie que même les plus petites entreprises seront affectées, directement ou indirectement, car les grandes entreprises demanderont des comptes sur les pratiques en matière de Durabilité de leurs fournisseurs et partenaires.

Les normes ESRS et la taxonomie verte

La CSRD introduit des normes extra-financières, les ESRS (European Sustainability Reporting Standards), qui catégorisent les informations les plus matérielles à fournir en matière d'environnement, de social, et de gouvernance.

Ces normes, obligatoires lorsque jugées matérielles pour l'entreprise, constituent le cadre de reporting le plus détaillé à ce jour, avec potentiellement jusqu'à 1 778 points de données à couvrir.

La Taxonomie verte de l'UE, chapitre intégré du Rapport de Durabilité de la CSRD, classe les activités économiques selon leur degré d'alignement avec 6 objectifs environnementaux : adaptation au changement climatique, atténuation du changement climatique, pollution, protection des eaux, économie circulaire, biodiversité. Ce système de classification nécessite une analyse rigoureuse des activités des entreprises pour déterminer leur contribution à ces objectifs. Cette convergence entre information financière et extra-financière impose une collaboration étroite entre les différentes directions de l'entreprise, marquant une intégration totale de la RSE dans toutes les pratiques d'entreprise.

Vers une intégration complète de la RSE

Nous assistons à une époque où la RSE ne peut plus être confinée à des départements isolés au sein des entreprises. La directive CSRD, avec son approche rigoureuse et normalisée, exige que l'information extra-financière soit traitée avec le même niveau de précision et d'audit que l'information financière. Cela requiert une transformation profonde des pratiques d'entreprise, où la RSE devient un pilier central, influençant de manière significative les décisions stratégiques et opérationnelles.

En conclusion, la directive CSRD est un jalon crucial dans l'évolution de la RSE et du reporting ESG, signalant un mouvement vers une plus grande transparence, comparabilité, et responsabilité dans le reporting extra-financier. Elle représente une opportunité pour les entreprises de réexaminer leurs modèles d'affaires, de renforcer leur engagement envers la durabilité, et d'aligner leurs pratiques avec les ambitions globales de l'Union européenne pour un avenir durable.

En savoir plus

- Ordonnance n° 2023-1142 du 6 décembre 2023
- Directive (UE) 2022/2464 du parlement européen et du conseil

04

DORA, NIS2, IT Governance

Piloter la cybersécurité et la résilience IT à travers la gouvernance

Jean-Philippe Isemann
Associé RSM France
M. jean-philippe.isemann@rsmfrance.fr
Se connecter sur Linkedin!

Découvrir l'accompagnement RSM :
Transformation digitale

> La mise en place d'une gouvernance IT efficace est essentielle pour réussir cette transformation, garantissant que les initiatives de cybersécurité et de résilience sont alignées avec les stratégies globales de l'entreprise.
>
> **Jean-Philippe Isemann** | Associée RSM France

Décryptage

Dans un monde numérique où la frontière entre le virtuel et le réel s'estompe de jour en jour, la sécurité informatique et la résilience sont devenues des préoccupations centrales pour les entreprises de tous secteurs.

Au cœur de cette évolution réglementaire, la gouvernance IT se révèle être un levier stratégique essentiel, garantissant une approche cohérente et intégrée à la sécurité informatique au sein des organisations.

L'essence de la gouvernance IT

La gouvernance IT ne se résume pas à une série de pratiques techniques isolées ; elle représente plutôt une démarche stratégique visant à aligner les efforts de sécurité informatique et de continuité d'activité avec les objectifs globaux de l'entreprise. Cette approche nécessite une implication active des plus hautes instances dirigeantes, affirmant ainsi que la cybersécurité et la résilience ne sont pas uniquement l'affaire des départements IT, mais une responsabilité partagée à l'échelle de l'organisation. L'adoption de référentiels tels que COBIT et les initiatives de l'ANSSI soulignent cette tendance vers une gestion intégrée et une maturité accrue en matière de gouvernance IT.

DORA : une uniformité dans le secteur financier

DORA s'adresse spécifiquement au secteur financier, soulignant la nécessité d'adopter des pratiques uniformes en matière de résilience opérationnelle et de sécurité informatique. Cette réglementation met en lumière l'importance de la continuité des opérations soutenues par les technologies de l'information et la nécessité de traiter la cybersécurité comme un enjeu stratégique transversal. En exigeant une harmonisation des pratiques à travers l'UE, DORA vise à éliminer les incohérences et à promouvoir une gestion cohérente des risques IT dans le secteur financier.

NIS2 : élargir le spectre de la cybersécurité

Contrairement à DORA, la directive NIS2 s'applique à un éventail plus large d'acteurs, dépassant le cadre du secteur financier pour inclure des entreprises considérées comme vitales ou importantes dans divers secteurs d'activité.

Cette extension du périmètre vise à renforcer la sécurité des systèmes d'information à une échelle beaucoup plus large, intégrant la gestion des risques IT dans les pratiques courantes de toutes les organisations concernées. NIS2 encourage également une collaboration renforcée entre les autorités nationales de cybersécurité pour standardiser les pratiques de sécurité à travers l'UE.

Vers une intégration complète de la RSE

Les efforts pour se conformer à DORA et NIS2 offrent aux organisations l'opportunité de rationaliser et d'intégrer leurs pratiques de gestion des risques IT. Cela implique de revoir et d'optimiser les processus existants, de promouvoir une culture de la sécurité informatique et de la gestion des risques à tous les niveaux, et d'adopter une approche holistique qui dépasse les silos organisationnels. La mise en place d'une gouvernance IT efficace est essentielle pour réussir cette transformation, garantissant que les initiatives de cybersécurité et de résilience sont alignées avec les stratégies globales de l'entreprise.

DORA et NIS2 représentent des défis significatifs mais également des opportunités pour les organisations de renforcer leur posture de sécurité et de résilience informatique. À travers l'adoption de bonnes pratiques de gouvernance IT, les entreprises peuvent non seulement répondre aux exigences réglementaires, mais également améliorer leur capacité à opérer de manière sécurisée et résiliente dans un environnement numérique en évolution rapide.

En savoir plus

- Définition de la directive NIS 2
- Cybersécurité et risques informatiques : l'AMF appelle les acteurs à se préparer à l'entrée en application du règlement européen DORA

RSM France

26, rue Cambacérès

75008 Paris

T. +33 (0)1 56 88 31 20

M. informations@rsmfrance.fr

www.rsmfrance.fr