Aperçu des capacités de Gouvernance, de Risque et de Conformité (GRC) d'Insight

Insight

Introduction

En résumé, la GRC consiste à instaurer la confiance : envers vos clients, les régulateurs et au sein de votre organisation que vous opériez de manière responsable et résiliente.

Piliers clés de la GRC :

1 Governance

Transformer en politiques claires les orientations données par la direction de l'organisation. Il s'agit de l'engagement du leadership à procéder de la bonne manière, de l'éthique des données à la responsabilité d'entreprise. Une gouvernance solide signifie que vos équipes disposent d'un repère pour prendre des décisions alignées sur vos objectifs et valeurs commerciaux.

2 Gestion du risque

Identifier ce qui pourrait poser problème (de la perte accidentelle de données aux attaques par rançongiciel) et l'atténuer de manière proactive. Il s'agit de prédire ce qui pourrait se passer et d'être préparé. Les entreprises qui gèrent bien les risques ont moins de crises et, lorsque des problèmes surviennent, elles les gèrent rapidement et efficacement. Vous gagnez en confiance pour prendre des bonnes décisions parce que vous êtes prémunis contre les impondérables.

3 Conformité

Jouer selon les règles – qu'il s'agisse de lois telles que le RGPD, de normes industrielles telles que l'ISO ou de codes de conduite internes. Il ne s'agit pas seulement de « rendre les régulateurs heureux » ; il s'agit de démontrer à vos clients et partenaires que la sécurité et la confidentialité est au coeur de vos priorités. La conformité instaure la confiance et ouvre des portes – par exemple, être certifié (p. ex. ISO 27 001) peut être un accélerateur business avec vos clients exigant des preuves de bonnes pratiques.

Valeur commerciale de la GRC

Négliger la gouvernance, la gestion des risques ou la conformité peut exposer une organisation à de graves conséquences :

- **Perte financière :** Les violations de données, la fraude ou les sanctions réglementaires peuvent entraîner des coûts financiers directs – amendes, frais juridiques, dépenses de remédiation aux violations – ainsi que des pertes de revenus dues à l'interruption de l'activité. Notamment, les études montrent que les coûts de non-conformité sont bien plus élevés pour les entreprises que les coûts de conformité.
- **Perturbation opérationnelle :** Les risques non gérés (comme les cyberattaques ou les défaillances de processus) peuvent interrompre les opérations et entraîner des temps d'arrêt, ce qui nuit à la productivité et à la prestation de services. Par exemple : une attaque par ransomware pourrait bloquer des systèmes critiques pendant des jours. Les pratiques GRC aident à identifier et à atténuer ces risques avant qu'ils ne se matérialisent, préservant ainsi la continuité des activités.
- **Atteinte à la réputation :** La confiance est difficile à gagner et facile à perdre. Les manquements à la conformité ou les lacunes éthiques érodent la confiance des clients et des parties prenantes. Une violation de données publiée ou un scandale de conformité. Peuvent ternir une marque pendant des années, incitant les clients à fuir. Une gouvernance et une conformité solides démontrent au public, aux partenaires et aux régulateurs que l'organisation est responsable et digne de confiance.
- **Pénalités réglementaires :** Les régulateurs appliquent de plus en plus de lois avec de lourdes amendes et même des sanctions pénales pour non-conformité. Par exemple, en vertu du RGPD de l'UE, les amendes peuvent atteindre. 20 millions € ou 4 % du chiffre d'affaires annuel mondial pour les infractions graves.

Les régulateurs européens ont imposé des amendes de 5,88 milliards € au titre du RGPD depuis 2018, y compris une amende record de 1,2 milliard € à l'encontre d'une seule entreprise. La GRC permet de s'assurer que tous les contrôles et rapports requis sont en place pour éviter ces amendes.

En résumé, investir dans la GRC est beaucoup moins cher et plus sûr que de faire face aux conséquences des défaillances de conformité ou des incidents majeurs. Un programme GRC cohérent protège la **santé financière, la continuité opérationnelle et la réputation publiquede** l'organisation, tout en permettant une meilleure prise de décision et un meilleur alignement stratégique. Comme l'a résumé une étude, « *la non-conformité coûte près de trois fois plus cher que la conformité* »

En moyenne, les organisations dépensent 5,47 millions $ par an pour la conformité, mais 14,82 millions $ en cas de non-conformité – le coût de la non-conformité est environ 2,7 fois plus élevé. Ces pertes incluent les temps d'arrêt de l'activité, la réponse aux incidents et la perte de clients.

Principaux cadres et réglementations

Dans le périmètre de la GRC, il existe de nombreuses normes, cadres et réglementations que les organisations peuvent avoir besoin de suivre. Vous trouverez ci-dessous un aperçu des principaux, ce qu'ils sont et comment ils s'appliquent aux différentes organisations :

Cadre réglementaire	Objet	Applicabilité	Implications clés de la GRC
ISO/IEC 27 001	Établit un système de gestion de la sécurité de l'information (SMSI) pour sécuriser systématiquement les informations.	Tous les secteurs dans le monde (finance, technologie, fabrication, etc.).	La base de référence pour la gouvernance de la cybersécurité, qui se chevauche souvent avec la directive NIS2 et d'autres cadres réglementaires. La certification démontre une solide posture en matière de sécurité.
Cyber Essentiels Plus	Programme soutenu par le gouvernement UK pour la bonne cyber-santé via cinq contrôles clés.	Entreprises basées au Royaume-Uni, en particulier les PME et les fournisseurs du gouvernement.	Assure des protections essentielles. Audit indépendant requis pour le niveau « Plus ». Souvent le point d'entrée pour structurer la sécurité.
CAF (Cyber Assessment Framework)	Développé par le NCSC du Royaume-Uni, le CAF fournit une approche structurée pour évaluer la cyberrésilience des organisations qui exercent des fonctions critiques.	Organisations au UK dans les secteurs des infrastructures nationales critiques (CNI) et opérateurs de services essentiels, en particulier en vertu des réglementations NIS UK.	Aligne les contrôles techniques sur les résultats de gouvernance. Aide à démontrer la maturité par rapport aux principes alignés sur la directive NIS. Soutient les décisions basées sur les risques et le dialogue réglementaire. Souvent utilisé avec la norme ISO 27 001 ou les politiques d'assurance interne.
Acte UE sur l'IA	Législation de l'UE régissant les systèmes d'IA par catégorie de risque (par exemple, systèmes à haut risque tels que la notation de crédit).	Toute organisation proposant de l'IA sur le marché européen.	L'IA à haut risque nécessite une documentation, une gestion du risque et une supervision continue. Une gouvernance solide de l'IA aide à garantir la conformité et l'accès au marché.
Directive NIS2	Règles de cybersécurité à l'échelle européenne pour les infrastructures critiques et numériques.	Entités de taille moyenne dans des secteurs clés (énergie, télécommunications, cloud, fabrication, soins de santé, etc.) y compris les prestataires non européens au service de l'UE.	Nécessite une sécurité basée sur la détection des risques, le signalement des incidents et la sécurité de la chaîne logistique. Les pénalités sont conformes aux amendes au niveau du RGPD. Chevauchement significatif avec la norme ISO 27 001.

Cadre réglementaire	Objet	Applicabilité	Implications clés de la GRC
RGPD	Règlement de l'UE relatif au traitement des données à caractère personnel, au consentement, aux droits à la vie privée, à la notification des violations, etc.	Toute organisation traitant des données à caractère personnel de résidents de l'UE.	La protection des données devient une préoccupation au niveau du conseil d'administration. Nécessite une gouvernance solide, des inventaires de données, des DPO et un signalement rapide des violations. Amendes importantes pour non-conformité.
SOC 2	Cadre développé aux États-Unis pour évaluer les contrôles internes en matière de protection des données, en particulier dans le Cloud/SaaS.	Fournisseurs de technologies et de services, en particulier en B2B ou SaaS.	Volontaire mais souvent requis par contrat. Fait preuve d'une grande sécurité opérationnelle et instaure la confiance.
PCI-DSS	Standard industriel mondial pour protéger les données des titulaires de cartes et réduire la fraude.	Toute entité qui stocke, traite ou transmet des données de carte de crédit.	Obligatoire pour les commerçants et les processeurs de paiement. Nécessite des contrôles stricts et des audits réguliers par des auditeurs certifiés.
DORA (Règlement sur la résilience opérationnelle numérique)	Règlement de l'UE visant à garantir que les entreprises du secteur financier peuvent résister et se remettre des perturbations liées aux TIC.	Entités financières opérant dans l'UE, y compris les banques, les assureurs, les sociétés d'investissement et les fournisseurs tiers critiques.	Nécessite une gestion solide des risques TIC, un reporting des incidents, des tests de résilience opérationnelle numérique et une supervision des risques liés aux tiers. Compléments NIS2 et RGPD.

Conformité à plusieurs réglementations/cadres

Aujourd'hui, les organisations sont rarement confrontées à un seul ensemble d'exigences de conformité. Le plus souvent, ils sont confrontés à un patchwork de législations, d'obligations réglementaires et de cadres sectoriels qui se chevauchent. Qu'il s'agisse du RGPD, de la NIS2, de l'ISO 27 001, du DORA ou de normes spécifiques au secteur telles que le PCI-DSS, le paysage de la conformité peut rapidement devenir complexe et difficile à gérer.

Cependant, de nombreuses organisations ne se rendent pas compte du chevauchement entre ces différentes exigences. Les principes fondamentaux tels que l'évaluation des risques, le contrôle d'accès, la réponse aux incidents et la gouvernance sont des principes courants dans la plupart des réglementations en matière de cybersécurité et de confidentialité. Ainsi, une approche intelligente et intégrée de la conformité peut réduire considérablement les doublons.

Plutôt que de traiter chaque réglementation de manière isolée, les principales organisations adoptent une approche unifiée : cartographier les contrôles et les processus sur plusieurs normes et construire une posture de sécurité qui satisfait les exigences de manière collective. Par exemple, une organisation certifiée ISO 27 001 est déjà sur la bonne voie pour répondre aux exigences de sécurité de la norme NIS2 – cela peut déjà couvrir 80 % des exigences .

En créant un cadre de conformité centralisé et basé sur les contrôles, les organisations peuvent rationaliser les audits, réduire les coûts et s'assurer que la sécurité devient une pratique durable et alignée sur l'entreprise de manière préventive.

Outils d'automatisation de la conformité

Le suivi des exigences dans des cadres tels que ISO 27 001, NIS2, RGPD, PCI-DSS et autres peut rapidement devenir lourd, en particulier lorsque chacun apporte son propre ensemble de contrôles, de demandes de preuves et d'exigences d'audit.

C'est là que la conformité et les outils d'automatisation GRC (gouvernance, risque et conformité) entrent en jeu.

Ces plateformes aident les organisations à cartographier, gérer et surveiller les contrôles dans plusieurs cadres réglementaires, en identifiant les chevauchements et en rationalisant les efforts de conformité. Au lieu de dupliquer le travail pour chaque standard, les outils d'automatisation vous permettent de mettre en œuvre un contrôle une seule fois, par exemple, pour le contrôle d'accès ou la réponse aux incidents, puis de le cartographier selon les exigences pertinentes de plusieurs réglementations.

Les avantages sont les suivants :

- **Réduction des doublons et des reprises :** Implémentez les contrôles une fois et réutilisez-les dans tous les cadres réglementaires.
- **Conformité continue :** La collecte automatisée des preuves, la surveillance des contrôles et le workflow management vous aident à être toujours prêt pour les audits.
- **Une vision claire :** Les tableaux de bord et les rapports fournissent aux parties prenantes une vue en temps réel de l'état de conformité et de l'exposition aux risques dans l'ensemble de l'organisation.
- **Un audit efficient :** La documentation centralisée et la cartographie automatisée des contrôles rendent les audits internes et externes plus rapides et moins perturbateurs.
- **L'adaptabilité :** À mesure que les réglementations évoluent ou que de nouveaux standards apparaissent, les outils d'automatisation peuvent s'adapter, afin que vous ne réinventiez pas constamment votre programme de conformité.

Les outils de conformité vous aident à transformer un processus de recertification précipité en un processus robuste qui fonctionne toute l'année. Ainsi vous connaîtrez toujours votre position en matière de conformité et disposerez du temps nécessaire pour combler toute lacune.

Faits & chiffres

Coût de la non-conformité vs conformité : Il n'est plus à démontrer que la non-conformité est bien plus coûteuse que les investissements à réaliser pour la conformité. Une étude de référence a révélé le coût moyen de la conformité (mise en œuvre des politiques, formations, audits, etc.) pour les grandes entreprises était de ~5,5 millions $ par an, alors que le coût moyen de la non-conformité (en raison d'amendes, d'interruptions d'activité, de pertes de productivité et de remédiation) était de ~14,8 millions $, soit près de 3 fois plus élevé.
Reference: **corporatecomplianceinsights.com**

Tendances d'amendes réglementaires : Les régulateurs contrôlent activement la conformité. En matière de confidentialité des données, par exemple, les amendes du RGPD ont totalisé **5,88 milliards €** de 2018 à 2024 dans toute l'Europe.
Reference: **dlapiper.com**

De manière positive, les entreprises disposant de programmes de conformité solides peuvent souvent négocier des amendes plus faibles ou éviter complètement les violations. Alors que des réglementations telles que la loi UE sur l'IA et la directive NIS2 entrent en vigueur, nous nous attendons à ce qu'une première vague de contrôles serve d'exemple, tout comme les premières années du RGPD, renforçant davantage le besoin de capacités GRC matures.

Adoption de programmes GRC et de conformité : La plupart des organisations reconnaissent le besoin de GRC. Selon l'enquête mondiale d'Accenture, **95 % des entreprises ont créé ou développent une « culture de la conformité »** dans leur organisation. Cela indique une prise de conscience quasi universelle au niveau du leadership que la conformité et l'éthique doivent faire partie de la culture d'entreprise. Cependant, la maturité varie : seulement **36 % des organisations ont mis en place un programme formel de gestion des risques d'entreprise (ERM, Enterprise Risk Management)**. Cela suggère que, bien que la plupart des entreprises aient l'intention de se conformer, beaucoup développent encore l'infrastructure et les processus pour une GRC complète. Alors que les industries font face à de nouveaux risques (cybermenaces, perturbations de la chaîne d'approvisionnement, impacts de la pandémie), les conseils d'administration poussent de plus en plus pour une meilleure surveillance des risques. **36 % des organisations prévoient d'augmenter leurs investissements dans la gestion des risques et la conformité au cours des deux prochaines années.**
Reference:**procurementtactics.com**

Volume de changement réglementaire : L'un des plus grands défis en matière de conformité est de suivre le rythme des nouvelles lois et des mises à jour. Dans le monde entier, des centaines d'agences réglementaires publient des mises à jour quotidiennes. Ce rythme n'a fait qu'augmenter ces dernières années avec les réglementations en matière de confidentialité et de finances. Ce « tsunami » de réglementations signifie que les organisations ont besoin de mécanismes (souvent axés sur la technologie, comme les flux réglementaires dans les systèmes GRC ou l'abonnement à des services de mise à jour de conformité) pour suivre les changements pertinents.

Croissance du marché et avenir de la GRC : Le marché des technologies GRC connaît une croissance rapide car les organisations recherchent des logiciels pour gérer ces complexités. Selon certaines estimations, le **marché mondial des logiciels GRC** était d'environ 5 milliards $ en 2023 et devrait presque doubler **d'ici 2029** (près de 9 à 10 milliards $) à mesure que la demande d'outils intégrés de gestion des risques augmente.
Reference: **verdantix.com**

Assurance cybersécurité et GRC : Les assureurs qui fournissent des cyberassurances examinent désormais les mesures GRC de leurs clients (clientèle qui suit des cadres réglementaires tels que la norme ISO27001 ou qui dispose de certaines certifications de conformité) lors de la souscription de polices d'assurances. Un programme GRC solide peut ainsi réduire les primes d'assurance et fournir une autre incitation financière aux organisations à investir dans la conformité et la gestion des risques.

Êtes-vous prêt pour la gouvernance, les risques et la conformité ?

1. Gouvernance – Direction et responsabilité

- ☐ Disposez-vous d'un cadre de gouvernance formel qui définit les politiques, les rôles et les responsabilités en matière de risque et de conformité ?
- ☐ Votre conseil d'administration/Comex est-il/elle impliqué(e) dans la prise de décision en matière de risque et de conformité ?
- ☐ Effectuez-vous des revues régulières des politiques de gouvernance pour vous assurer qu'elles sont conformes aux objectifs commerciaux et aux changements réglementaires ?
- ☐ Disposez-vous d'un code d'éthique et de conduite documenté pour les collaborateurs et la direction ?
- ☐ Les fournisseurs et partenaires tiers sont-ils soumis à une gouvernance et à une surveillance des risques ?

Si vous avez répondu « Non » à l'une de ces questions, il se peut que vous ayez des lacunes dans la supervision de la gouvernance.

2. Gestion du risque – Identification et atténuation des menaces

- ☐ Tenez-vous à jour un registre des risques qui documente les risques commerciaux, de cybersécurité, financiers et opérationnels ?
- ☐ Les risques sont-ils évalués et hiérarchisés en fonction de l'impact et de la probabilité ?
- ☐ Effectuez-vous régulièrement des évaluations de risque (cybersécurité, opérationnels, financiers, réputationnels, chaîne d'approvisionnement, etc.)) ?
- ☐ Disposez-vous d'une stratégie formelle d'atténuation des risques qui désignent des responsables et des délais pour les actions correctives ?
- ☐ Existe-t-il un plan de continuité des activités et de reprise après sinistre pour les systèmes et opérations clés ?

Si vous avez répondu « Non » à l'une de ces questions, vous pourriez être exposé à des risques non traités.

3. Conformité – Réunions réglementaires et standards industriels

- ☐ Connaissez-vous les réglementations et cadres réglementaires clés applicables à votre secteur (par ex. RGPD, ISO 27 001, NIS2), PCI DSS, SOC 2, Gouvernance de l'IA, etc.) ?
- ☐ Disposez-vous de politiques de conformité formelles et de contrôles en place pour ces réglementations ?
- ☐ La conformité fait-elle l'objet d'un contrôle et d'audits internes ou externes réguliers ?
- ☐ Disposez-vous d'outils automatisés de suivi de la conformité ou de reporting ? Pouvez-vous fournir rapidement une documentation en cas d'audit réglementaire ?

Si vous avez répondu « Non » à l'une de ces questions, vous pourriez faire face à un risque réglementaire ou financier.

4. Cybersécurité et protection des données – Opérations sécurisées

- ☐ Disposez-vous d'une politique de cybersécurité documentée conforme aux exigences de conformité ?
- ☐ Avez-vous réalisé un audit des risques en matière de cybersécurité au cours des 12 derniers mois ?
- ☐ Les collaborateurs sont-ils formés à la sensibilisation à la sécurité et aux obligations de conformité ? Disposez-vous de protocoles de réponse aux incidents et de signalement des violations ?
- ☐ Les données sensibles sont-elles protégées par le chiffrement, les contrôles d'accès et la classification des données ?
- ☐ Si vous avez répondu « Non » à l'une de ces questions, il se peut que votre posture de sécurité ne soit pas conforme aux meilleures pratiques GRC.

5. Surveillance et amélioration continues

- ☐ La GRC est-elle intégrée dans la culture de votre organisation plutôt que d'être traitée comme un projet ponctuel ?
- ☐ Disposez-vous d'une plateforme technologique GRC pour gérer la gouvernance, les risques et la conformité en un seul endroit ?
- ☐ Les activités de conformité et de risque sont-elles régulièrement examinées, testées et mises à jour en fonction des nouvelles menaces ou des changements réglementaires ?
- ☐ Participez-vous à des évaluations ou des audits tiers en continu pour garantir la conformité ?
- ☐ Les rapports de conformité sont-ils automatisés et intégrés dans vos opérations commerciales ?

Si vous avez répondu « Non » à l'une de ces questions, vos efforts GRC peuvent manquer de durabilité et d'efficacité.

Comment vous aider – Votre partenaire GRC de confiance

Chez Insight, nous comprenons que la gouvernance, le risque et la conformité (GRC) ne se limitent pas à cocher des cases. Il s'agit de protéger votre réputation, de permettre une prise de décision en toute confiance et de vous assurer que vous pouvez évoluer sans craindre les angles morts réglementaires ou opérationnels.

Nous vous aidons à gérer cette complexité grâce à une approche holistique, pratique et technologique de la GRC qui offre à la fois résilience et agilité.

Services de conseil et d'audit :

Nos consultants expérimentés vous aident à comprendre vos obligations, à établir des benchmarks par rapport aux principaux standards et à établir une trajectoire claire.

Evaluations des lacunes et des performances - pour ISO 27 001, Cyber Essentials+, NIS2, CAF et plus encore.

Conception de politiques et de cadres réglementaires - élaboration de programmes évolutifs de gouvernance, de gestion des risques et de conformité adaptés à votre entreprise.

Rapports pour le Conseil d'administration et Comex - traduire la posture GRC en un aperçu utile de risques commerciaux pour la direction.

Accompagnement d'audit interne – y compris la préparation des preuves, la planification des mesures correctives et l'assurance continue.

Services Managés GRC

Si vous n'avez pas la bande passante ou l'expertise en interne, notre offre de services managés GRC garantit le bon fonctionnement de votre programme de conformité.

Gestion continue des risques et de la conformité - nous gérons vos tests de contrôle, de suivi et de reporting.

Virtual CISO ou Virtual Information Security Officer - accédez à un support expert sans le surchage d'une équipe interne complète.

Pourquoi choisir Insight

Fiable dans tous les secteurs, du secteur de la finance au secteur de la santé, en passant par le secteur industriel au secteur IT.

Certifié selon les standards que nous vous aidons à respecter, y compris ISO 27 001 et Cyber Essentials+.

Agnostique dans notre approche - nous travaillons avec les principales plateformes GRC, mais nos conseils commencent par vos objectifs, pas par un argumentaire produit.

Aligné sur votre organisation - nous saurons adresser votre comex tout comme votre back-office.