ADAPTER LE SYSTÈME D'INFORMATION AUX ÉVOLUTIONS RÉGLEMENTAIRES :

UN IMPÉRATIF STRATÉGIQUE POUR LES ENTREPRISES

Les entreprises évoluent aujourd'hui dans un environnement où les réglementations se multiplient et se renforcent, imposant des exigences croissantes et interdépendantes sur leur Système d'Information (SI). Entre le **RGPD** pour la protection des données personnelles, les réglementations **DORA** et **NIS2** pour la cybersécurité et la résilience opérationnelle, la f**acturation électronique** obligatoire, la **CSRD** pour le reporting de durabilité, ou encore la **PCI-DSS** pour la sécurité des transactions, les contraintes sont à la fois nombreuses, complexes et en constante évolution.

En 2025, la conformité n'est plus une simple obligation légale, mais un **levier stratégique** pour renforcer la sécurité, la transparence et la compétitivité des entreprises. Les sanctions pour non-conformité peuvent atteindre des millions d'euros (jusqu'à **4 % du chiffre d'affaires mondial** pour le RGPD, **10 millions d'euros** pour DORA, ou des **amendes proportionnelles** pour NIS2), sans compter les risques réputationnels et opérationnels (perte de confiance des clients, interruption d'activité, etc.).

Dans ce contexte, adapter le SI aux évolutions réglementaires devient un **enjeu clé** pour les DSI et les directions métiers. Cet article propose une **vision intégrée** des contraintes, des risques et des solutions pour **transformer ces défis en opportunités.**

LES DÉFIS MAJEURS : ENTRE COMPLEXITÉ, RISQUES ET SANCTIONS

DÉFI N°1 : BIEN ÉVALUER L'IMPACT DES ÉVOLUTIONS RÉGLEMENTAIRES

De nombreuses entreprises considèrent encore la conformité comme un processus ponctuel, alors qu'il s'agit d'un **engagement continu.**

Par exemple, si la majorité des organisations se sont mises en conformité avec la réglementation sur les données personnelle depuis 2018, elles doivent **sans cesse actualiser leurs procédures, leurs registres et leurs systèmes**, et prendre en compte les exigences du RGPD dans les nouveaux projets et la CNIL augmente chaque année le nombre de contrôles réalisés. En 2025, **la CNIL a renforcé ses contrôles** et infligé une amende record de **325 millions d'euros à Google** pour non-respect des règles de consentement et de gestion des cookies.

Comment y parvenir ?

- Mettre en place une **veille réglementaire active** pour anticiper les évolutions (RGPD, DORA, NIS2, CSRD, etc.).
- Intégrer la conformité **dès la conception** des systèmes (privacy by design, sécurité by default).
- **Former régulièrement** les équipes aux nouvelles exigences.
- **Anticiper les échéances clés** pour évaluer les impacts et planifier les actions nécessaires.

DÉFI N°2 : RÉUSSIR L'INTÉGRATION AVEC LES SYSTÈMES EXISTANTS

Adapter les systèmes aux nouvelles exigences réglementaires se heurte souvent à la rigidité des architectures informatiques existantes. Par exemple :

- Pour le **RGPD**, de nombreuses entreprises, notamment dans la grande distribution et le e-commerce, ont rencontré des difficultés pour intégrer des solutions de gestion des **consentements aux cookies** avec leurs systèmes legacy. Ces retards ont parfois entraîné **des sanctions de la CNIL** pour non-respect des règles de consentement, comme en témoignent les amendes infligées à des acteurs majeurs pour des bandeaux de cookies non conformes.

- Pour **DORA**, les banques et assurances doivent réviser leurs contrats avec les prestataires SI et mettre à jour leurs politiques de cybersécurité avant janvier 2025. Cela implique souvent une refonte partielle de leur SI pour intégrer des mécanismes de **détection des incidents et de tests de résilience**.

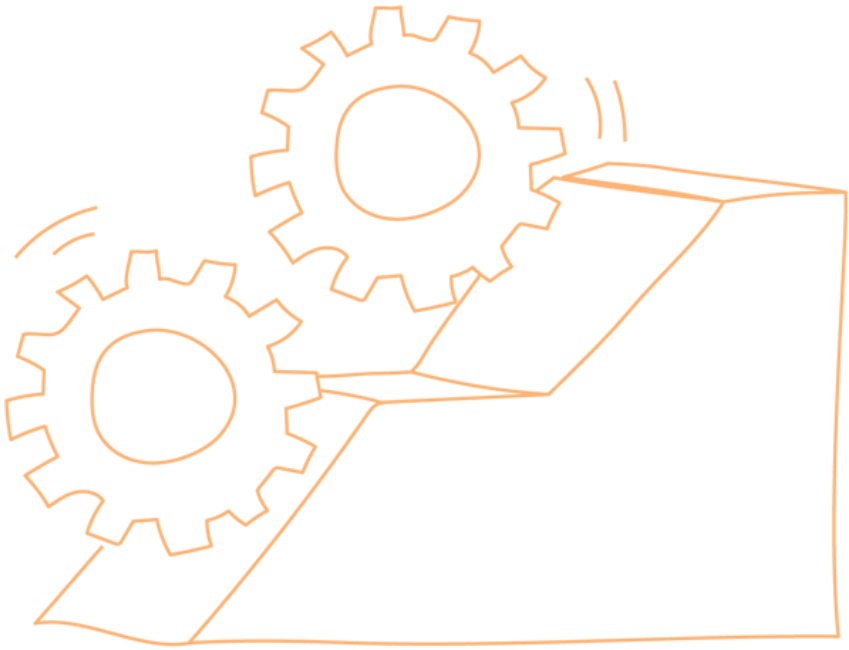
- La **facturation électronique**, obligatoire à partir de septembre 2026 (au moins pour la réception), impose aux entreprises d'adapter leurs processus comptables et de choisir une plateforme de dématérialisation agréée (PDP). Cette transition peut être complexe pour les PME et les micro-entreprises, qui doivent souvent moderniser leurs outils de gestion.

Comment y parvenir ?

- Auditer régulièrement l'architecture du SI pour identifier les points de friction et les dépendances legacy.

- Privilégier des solutions modulaires et interopérables (API, cloud sécurisé, outils de gestion des consentements) pour faciliter l'intégration des nouvelles exigences.

- Collaborer avec des experts en transformation digitale pour accompagner la migration vers des systèmes conformes, en particulier pour les réglementations transverses comme le RGPD, DORA ou NIS2.



DÉFI N°3 : GÉRER LES RISQUES LIÉS À LA SÉCURITÉ ET À LA PROTECTION DES DONNÉES

Les **risques de fuite de données et de cyberattaques** sont accrus dans le contexte actuel, et la gestion des données sensibles devient encore plus cruciale avec l'évolution des lois, surtout dans des secteurs comme la **santé** ou la **finance** :

- La **certification HDS** (Hébergement des Données de Santé) impose des standards rigoureux pour assurer la sécurité des données sensibles et la résilience des systèmes.
- **NIS2** élargit le périmètre des entreprises soumises à des obligations de cybersécurité, couvrant **18 secteurs critiques** (énergie, transports, santé, numérique, etc.).
- Les entreprises doivent mettre en place des **mesures de gestion des risques**, de détection des incidents, et de notification aux autorités (ANSSI, CNIL, ACPR).

Comment les atténuer ?

- Investir dans des **solutions de cryptage**, de gestion des accès, et de détection des intrusions dans les différents systèmes de l'entreprise.

- Mettre en place des **processus de gestion des incidents** et de notification des violations et former les collaborateurs aux risques et aux moyens de prévention.

- S'assurer que les **sous-traitants respectent les mêmes standards de sécurité** (RGPD, NIS2, DORA), avec des dispositions contractuelles contraignantes et des audits réguliers.

QUELQUES PISTES POUR FACILITER L'ADAPTATION DU SI AUX ÉVOLUTIONS RÉGLEMENTAIRES

UNE GOUVERNANCE AGILE POUR ANTICIPER LES CHANGEMENTS

Pour rester conforme, il est essentiel de mettre en place une **gouvernance SI flexible et évolutive**, intégrant :

Un **comité dédié à la conformité**, associant DSI, juristes, métiers et RSSI.

Des **outils de veille réglementaire** pour anticiper les évolutions (RGPD, DORA, NIS2, CSRD, facturation électronique, etc.).

L'intégration de la conformité dans les **cycles de développement des projets informatiques**.

Il est aussi recommandé d'adopter des approches intégrées pour gérer les réglementations RGPD, DORA et NIS2, avec des **tableaux de bord centralisés**, permettant un suivi en temps réel des obligations et une réduction des risques de non-conformité.

AUTOMATISATION ET INDUSTRIALISATION DE LA CONFORMITÉ

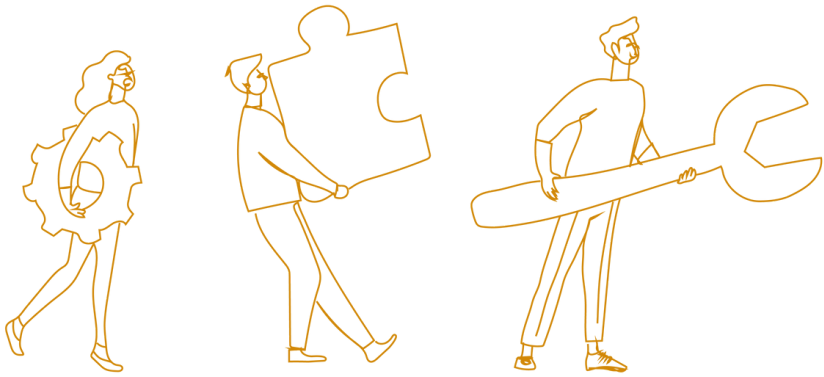
Les outils d'automatisation permettent de simplifier la gestion des consentements, les rapports de conformité, et la mise à jour des politiques de sécurité. Par exemple :

- Des logiciels comme **OneTrust** ou **StandardFusion** offrent des fonctionnalités avancées pour piloter et automatiser la mise en conformité au **RGPD, PCI-DSS, DORA et NIS2**.

- Pour la **facturation électronique**, les PDP agréées permettent de gérer les flux de factures et les déclarations fiscales.

- Des outils comme **Sami** ou **Zei** aident à consolider et à structurer les **données ESG** et à générer des rapports conforme à la **CSRD**.

L'automatisation permet de réduire les risques d'erreurs humaines (ex. : erreurs de saisie), de gagner **en efficacité** pour les équipes (ex. : génération automatique de rapports) et elle offre aussi une meilleure **traçabilité** des actions et des preuves de conformité (ex. : logs).



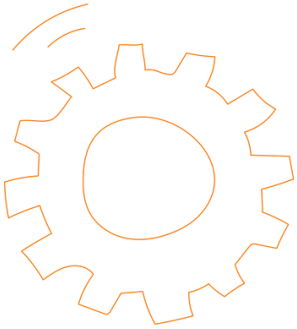
FORMATION ET SENSIBILISATION DES ÉQUIPES

La conformité ne repose pas uniquement sur les outils, mais aussi sur l**es compétences et la culture d'entreprise**. Voici pourquoi la formation est stratégique :

Une formation régulière sur les **bonnes pratiques RGPD, DORA ou NIS2** permet de limiter les violations involontaires (ex. : fuites de données, non-respect des délais de déclaration), sachant que les erreurs humaines sont à l'origine de **plus de 80 % des incidents de cybersécurité** selon l'ANSSI.

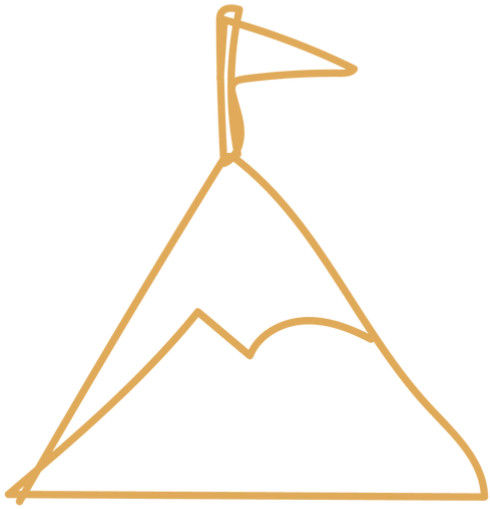
Les équipes formées aux **procédures de détection et de réponse aux incidents** réagissent plus rapidement, limitant l'impact des attaques.
La formation crée une **culture commune** de la sécurité et de la conformité, impliquant tous les collaborateurs, qui deviennent ainsi des **acteurs proactifs** dans la protection des données et la résilience du SI.

Le développement des compétences passe par des **formations régulières** sur les réglementations (RGPD, DORA, NIS2, etc.), des sensibilisations aux bonnes pratiques, ou encore par la mise en place de **communautés de pratique** pour partager les retours d'expérience.



TRANSFORMER LA CONFORMITÉ EN AVANTAGE CONCURRENTIEL

Adapter le SI aux évolutions réglementaires est un **défi permanent**, mais aussi une **opportunité** pour renforcer la sécurité, la transparence et l'agilité de l'entreprise. En combinant une **gouvernance proactive**, une **veille réglementaire rigoureuse** et des **outils d'automatisation**, les organisations peuvent transformer la conformité en un **avantage concurrentiel durable.**



Vous souhaitez évaluer la conformité de votre SI ou mettre en place une feuille de route adaptée à DORA, NIS2 ou aux autres réglementations ? Contactez-nous pour un diagnostic personnalisé et des solutions sur mesure.