Le règlement DORA :
Comment s'y préparer de manière pragmatique ?

La transformation numérique des services financiers se caractérise par l'ouverture des données et par de fortes interconnexions des infrastructures. Si cette évolution offre des avantages indéniables en matière d'innovation et d'amélioration de l'expérience client, elle s'accompagne aussi d'une croissance significative des menaces cyber et des risques d'incidents numériques.

La menace cyber s'est maintenue à un niveau élevé en 2022, avec une augmentation constante du degré de sophistication des attaques[1]. La France, où les moyens consacrés à la cybersécurité sont moins importants que partout ailleurs en Europe[2], est le 1er pays européen concerné[3].

La dépendance croissante du secteur financier vis-à-vis des technologies de l'information et de la communication expose également à une augmentation proportionnelle du risque de défaillance des systèmes d'informations, qui peut entraîner des conséquences extrêmement dommageables pour les utilisateurs, comme la fuite de leurs données personnelles.

Pour les acteurs du secteur, la maîtrise des risques liés aux technologies de l'information et de la communication (TIC) devient alors un enjeu majeur, pour maintenir la continuité de leurs activités et préserver leur réputation.

Face à ces menaces, en septembre 2020, la Commission Européenne a proposé au Parlement Européen de mettre en place un cadre permettant aux services financiers d'exploiter tout le potentiel des évolutions technologiques, en garantissant la stabilité et la sécurité du système financier.

Synaxia Conseil a voulu comprendre quels étaient les objectifs précis de DORA, ainsi que les enjeux pour les assureurs, et a travaillé à l'élaboration d'une démarche de mise en conformité.

1 Le règlement DORA pour une cybersécurité renforcée

Le règlement DORA (Digital Operational Resilience Act), initié par la Commission Européenne et entré en vigueur le 16 janvier 2023, marque une avancée importante de l'Union Européenne dans la lutte pour la protection du système financier. Il s'agit d'un nouveau cadre légal qui vient consolider le corpus réglementaire existant pour renforcer la maîtrise des risques liés aux technologies de l'information et de la communication. Les objectifs poursuivis sont les suivants :

- Renforcer la maîtrise des risques liés aux technologies de l'information et de la communication et garantir la sécurité des données pour mieux protéger les utilisateurs,

[1] www.cyber.gouv.fr
[2] Etude Cybersécurité Solutions - Les entreprises françaises seraient plus vulnérables aux cyberattaques que leurs homologues européennes
[3] Etude Cybersécurité Solutions - Cyberattaques : les organisations françaises seraient les plus touchées d'Europe

- Garantir la résilience opérationnelle numérique, c'est à dire la capacité à maintenir les opérations malgré les perturbations numériques qui peuvent venir entraver la bonne marche des activités (cyberattaques, interruptions de services etc.…),
- Harmoniser les pratiques de gestion des risques et de suivi des incidents pour une supervision des autorités de contrôles facilitée,
- Inciter à la coopération dans la lutte contre la cybercriminalité au sein de l'Union Européenne pour augmenter les capacités de défense dans un environnement géopolitique incertain.

L'entrée en application du règlement DORA est prévue pour le 17 janvier 2025. D'ici là, des normes techniques (RTS pour Regulatory Technical Standards et ITS pour Implementing Technical Standards) seront publiées pour apporter certaines précisions au règlement. Deux projets de normes seront soumis à la Commission Européenne : en janvier 2024 et en juillet 2024.

2 Les conséquences opérationnelles pour les assureurs

Le règlement DORA articule les exigences au travers de 5 piliers : la gestion des risques, la gestion des incidents, les tests de résilience opérationnelle numérique, la gestion des risques des prestataires et la collaboration en matière de cybersécurité. Il permet ainsi aux acteurs du secteur de définir leur feuille de route d'ici début 2025.

1er pilier : la gestion des risques

Les assureurs doivent enrichir leur dispositif de gestion des risques pour y intégrer le prisme de la résilience numérique. Un travail d'approfondissement des risques opérationnels doit ainsi être mené pour identifier et évaluer les risques TIC en distinguant les activités critiques et importantes. L'objectif de ce travail est d'obtenir une vision précise de son profil de risques TIC compte tenu de sa stratégie, ses enjeux et son fonctionnement. Du point de vue organisationnel, l'organe de direction est responsable de la stratégie de risques TIC. Il doit également définir le cadre de gouvernance et de gestion des risques qui permettra de garantir une gestion des risques TIC efficace, notamment en se posant la question de la place du RSSI dans l'organisation.

2ème pilier : la gestion des incidents

Les assureurs doivent faire évoluer leur dispositif de gestion des incidents TIC pour qu'il réponde aux nouvelles exigences du règlement DORA. Les critères de classification et les seuils d'incidents seront précisés dans le 1er lot de normes techniques qui sera publié en début d'année 2024. Un modèle de rapport de notification des incidents majeurs sera également mis à disposition dans le 2ème lot de normes techniques. L'enjeu pour les autorités de contrôle est d'être informé rapidement des incidents majeurs grâce à des reportings standardisés qui leur seront transmis par les entités.

3ème pilier : les tests de résilience opérationnelle numérique

Le règlement DORA établit des normes pour la mise en œuvre des tests de résilience opérationnelle numérique. De plus, il élargit le périmètre d'éligibilité des entités susceptibles de devoir réaliser ces tests de manière obligatoire et régulière. Toutefois, les exigences varient en fonction de la taille, de l'activité et du profil de risque des entités. Des tests avancés de pénétration fondés sur la menace sur les activités critiques ou importantes devront aussi être menés par les entités considérées comme importantes par les autorités compétentes. Les modalités de mise en

œuvre de ces tests feront l'objet de précisions dans le cadre du projet de normes techniques soumis en juillet 2024 à la Commission Européenne.

4ème pilier : la gestion des risques des prestataires

La stratégie d'externalisation des services TIC doit être revue à l'aune des risques TIC. Selon le degré d'externalisation des activités, le travail de mise en conformité des contrats sera plus ou moins important. Le principal défi est de renégocier les clauses contractuelles avec les prestataires tiers gérant des fonctions importantes ou critiques pour intégrer les nouveaux standards imposés par DORA (normes de sécurité, coopération dans la mise en œuvre des tests et le reporting des incidents, …). Par ailleurs, les contrats devront être listés dans un registre d'informations qui aura vocation à être transmis aux autorités de contrôles. Le contenu des accords contractuels et le modèle de registre d'informations seront fournis dans le cadre des normes techniques à venir courant 2024.

5ème pilier : la collaboration en matière de cybersécurité

Enfin, les entités sont encouragées à partager entre elles des informations concernant les cyberattaques qu'elles ont subies. L'objectif est de mieux détecter les menaces et élaborer des stratégies de réponse pour développer les capacités de défense et de rétablissement du système financier. Ce 5ème pilier ne constitue pas une obligation mais vise à inciter à plus de collaboration au sein du secteur financier.

3 Pour Synaxia Conseil, les délais courts imposent la mise en œuvre d'une approche pragmatique

Plus que 12 mois avant l'entrée en application de DORA, et seule une approche pragmatique permettra aux acteurs de l'assurance d'être au rendez-vous le 17 janvier 2025 !

Pour Synaxia Conseil, les quatre points clés de cette approche pragmatique sont les suivants :

1. ***Mobiliser les compétences en transverse*** : il est primordial d'impliquer l'ensemble des fonctions parties prenantes au projet ; évidemment la Conformité et les Risques, mais aussi le Juridique, les Achats et les Métiers. DORA est un sujet éminemment opérationnel qui dépasse le spectre de la Direction des Systèmes d'Informations et qui nécessite l'engagement de la Direction Générale.
2. ***Procéder par écart avec l'existant*** : il s'agit de passer en revue le dispositif de gestion des risques existant et d'identifier les zones qui nécessitent un approfondissement au regard des exigences DORA ; ceci en intégrant le prisme de la résilience numérique.
3. ***Cibler les efforts*** : il est important de concentrer ses efforts là où la marche est la plus haute à franchir. Selon le contexte, il s'agira de renégocier les contrats avec les prestataires, de réduire le risque de concentration sur certains prestataires de services TIC, de mieux analyser ses vulnérabilités pour augmenter sa capacité de résilience, d'approfondir la connaissance de ses risques TIC et de revoir sa stratégie, ou encore de consolider le cadre de gouvernance et de sensibiliser le top management.
4. ***Adapter la mise en application*** : un vrai travail d'appropriation des textes est nécessaire pour concevoir une déclinaison opérationnelle adaptée au contexte, à l'organisation et aux

enjeux stratégiques de l'entreprise. Le principe de proportionnalité doit être appliqué et doit notamment s'appuyer sur une première analyse de la criticité des activités.

De notre point de vue, les premières actions à mener pour les assureurs sont les suivantes :

- Lancer la dynamique de projet au niveau de l'entreprise en réunissant les compétences transversales autour du chef de projet et impliquer la Direction Générale,
- Réaliser l'analyse d'écart entre les exigences DORA et le cadre de gestion des risques existant sur l'ensemble des domaines du règlement : cela implique un travail important de collecte et d'analyse de la documentation existante,
- Délimiter le périmètre d'application DORA à partir de l'étude des cartographies des systèmes d'informations et des processus en distinguant les activités critiques et les activités importantes,
- Lister les prestataires de services TIC, recenser les contrats et faire l'état des lieux des clauses contractuelles,
- Définir sa stratégie vis-à-vis des TIC et des risques associés,
- Définir la feuille de route en priorisant les sujets pour lesquels le niveau de maturité est le plus faible et les sujets qui apporteront des résultats rapides.

En conclusion, selon nous, la stratégie gagnante est de capitaliser sur les expériences et les résultats des nombreux projets de mise en conformité, dont Solvabilité 2, afin de procéder aux seuls ajustements nécessaires !

A propos de Synaxia Conseil

Fondé en 2017, Synaxia Conseil est un cabinet de conseil en stratégie et organisation, spécialisé sur le secteur de l'assurance.

Ses consultants accompagnent les acteurs du secteur sur l'ensemble de la chaîne de valeur : stratégie, organisation, marketing et innovation, distribution, opérations et pilotage.

Pour en savoir plus : www.synaxia-conseil.fr

Et suivez Synaxia Conseil sur X [@SYNAXIA_CONSEIL] et LinkedIn.