Mise en place d'un cadre de prévention et gestion du risque cyber-sécurité

	ACTIONS INTIALES	ACTIONS PERIDODIQUES
1 Nomination d'un **Chief Information Security Officer**	✓	
2 Adoption d'une **police cyber-sécurité** et établissement d'un **programme de cyber-sécurité** en vue ◆ d'identifier les risques, de les détecter et y répondre ◆ de prendre les mesures adequates pour prévenir les risques ◆ de tester le système (controle interne, tests externs) ◆ de réaliser une auto-évaluation du programme ◆ d'intégrer les bonnes pratiques et autres recommandations de l'ANSSI et autres experts	✓	
3 **Plan de crise, communication et de recouvrement** en cas d'incident cyber-sécurité	✓	
4 **Extension de la couverture aux prestataires de services externalisés**	✓	
5 Analyse de la **conformité du cadre avec les réglementations en vigueur**, en particulier avec les lois gérant la protection des données (RGPD dès 2018)	✓	✓
6 **Sensibilisation des équipes au risque cyber-sécurité** ◆ Equipes informatiques et en particulier celles en charge du risque ◆ Autres équipes y compris l'organe d'administration de gestion ou de contrôle (AMSB)	✓	✓
7 **Comité des risques** ◆ Analyse de la cartographie des risques, revue post-mortem des évènements et plans d'action ◆ Revue de l'efficience / validation du programme et de la police cyber sécurité ◆ Revue des exercices à blanc d'exécution des plans de crise, communication et recouvrement ◆ Définition / validation de la couverture du risque	✓	✓
8 **Rapport ORSA** ◆ Création de l'enregistrement ORSA ◆ Rédaction du paragraphe sur le risque cyber-sécurité	✓	✓

MPG PARTNERS

Document établi sur la base du document de la DFS de l'Etat de NY,USA, les bonnes pratiques observées et la réglementation Solvabilité 2