



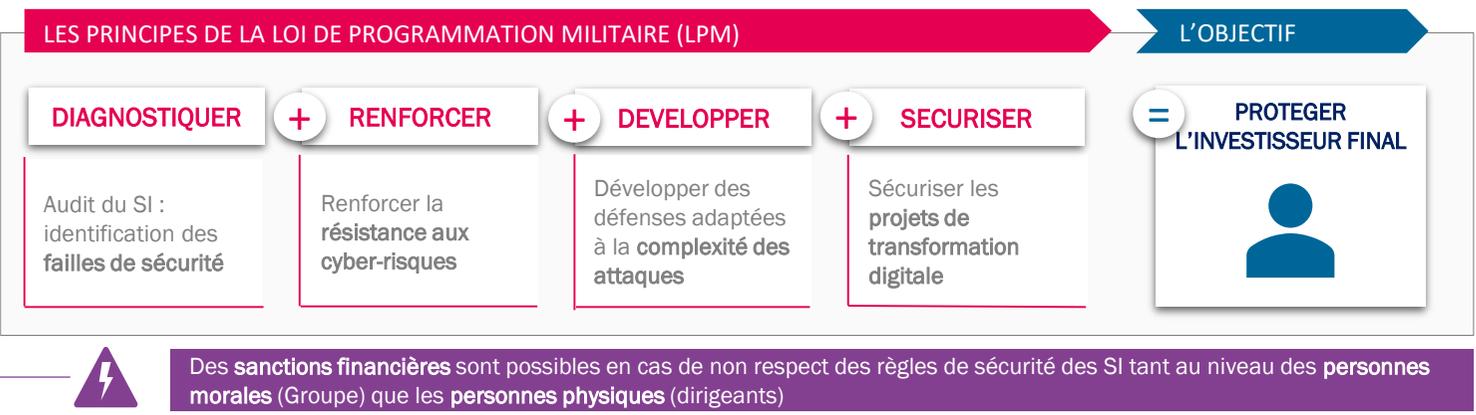
La cyber résilience, un enjeu essentiel pour les acteurs du secteur bancaire

Initiative de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), la Loi de Programmation Militaire (LPM) vise à renforcer la sécurité des différents systèmes d'information considérés comme critiques : les Opérateurs d'Importance Vitale (OIV) – organe économique participant au PIB de la nation - dont font partie les banques.

Face à la sophistication et la diversité de plus en plus accrue des cyber attaques auxquelles sont exposées les banques, être en mesure de faire face à la cyber-menace est devenu un enjeu majeur pour assurer la bonne santé financière de ces acteurs et protéger l'investisseur final. **Le volet sur la cybersécurité de Loi de Programmation Militaire contraint désormais les banques à revoir leur modèle de Sécurité des Systèmes d'Information d'Importance Vitale (SIIV) de sorte à être conforme aux règles⁽⁴⁾ établies par l'ANSSI**



Être LPM compliant : sécuriser les données sensibles



Impacts transverses sur les OIV bancaires

SI	CONFORMITE	ORGANISATIONNEL
<ul style="list-style-type: none"> Revue de l'architecture SI Mise à jour du système de sécurité Elaboration de la cyber-stratégie Mise en place de la cyber résilience 	<ul style="list-style-type: none"> Production périodique de la déclaration à l'ANSSI Revue des indicateurs de maîtrise des risques Homologation de la sécurité des SIIV 	<ul style="list-style-type: none"> Revue de la gouvernance SI Redéfinition des rôles et responsabilités de chaque SIIV Identification du reporting owner



BEAM vous accompagne

- EXPERTISE**
Analyse des impacts réglementaires, définition des indicateurs d'évaluation des risques,, analyse des obligations de reporting
- PILOTAGE**
Pilotage du programme / projet réglementaire, suivi de la mise en œuvre, coordination des parties prenantes, mise en place de la comitologie, reporting

- PROCESSUS**
Définition et optimisation du processus d'homologation des SIIV, mise en place du Target Operating Model, définition des responsabilités
- CONDUITE DU CHANGEMENT**
Accompagnement des équipes dans le processus de production du reporting, initiation à la cyber résilience, mise en place de la gouvernance

⁽⁴⁾Source : arrêté du 28 novembre 2016 du Journal Officiel fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Finances »