Loi de Programmation Militaire

Regulatory

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[1] établies par l'ANSSI

Être LPM compliant : sécuriser les données sensibles

LES PRINCIPES DE LA LOI DE PROGRAMMATION MILITAIRE (LPM) → **L'OBJECTIF**

DIAGNOSTIQUER	+ RENFORCER	+ DEVELOPPER	+ SECURISER	= PROTEGER L'INVESTISSEUR FINAL
Audit du SI : identification des **failles de sécurité**	Renforcer la **résistance aux cyber-risques**	Développer des défenses adaptées à la **complexité des attaques**	Sécuriser les **projets de transformation digitale**	

Des **sanctions financières** sont possibles en cas de non respect des règles de sécurité des SI tant au niveau des **personnes morales** (Groupe) que les **personnes physiques** (dirigeants)

DECLARATION A L'ANSSI

01/01/2016
Déclaration du **calendrier de mise en œuvre du dispositif de sécurité des SIIV**

01/01/2017 au 30/03/2017
Déclaration de la **liste des SIIV**

01/11/2017 au 30/11/2017
Déclaration annuelle des **update des SIIV** et des **formulaires de déclaration**

Déclaration immédiate de toute implémentation d'un nouveau SIIV ou d'un retrait

Impacts transverses sur les OIV bancaires

SI	CONFORMITE	ORGANISATIONNEL
• Revue de **l'architecture SI** • Mise à jour du **système de sécurité** • Elaboration de la **cyber-stratégie** • Mise en place de la **cyber résilience**	• Production périodique de la **déclaration à l'ANSSI** • Revue des **indicateurs de maîtrise des risques** • Homologation de la **sécurité des SIIV**	• 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

PROCESSUS
Définition et optimisation du processus d'homologation des SIIV, mise en place du Target Operating Model, définition des responsabilités

PILOTAGE
Pilotage du programme / projet réglementaire, suivi de la mise en œuvre, coordination des parties prenantes, mise en place de la comitologie, reporting

CONDUITE DU CHANGEMENT
Accompagnement des équipes dans le processus de production du reporting, initiation à la cyber résilience, mise en place de la gouvernance

[1] *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 »

Contacts BEAM Advisory : betty.biennesca@beamadvisory.com 01 86 95 37 85 www.beamadvisory.com