Publication d'octobre 2019

de la Revue de l'ACPR

La stratégie de l'ACPR de supervision du risque informatique

Le risque informatique des établissements du secteur financier devient une préoccupation majeure des autorités de supervision, notamment en raison de la complexité croissante des environnements techniques, mais aussi de la montée des cyber-menaces. L'ACPR structure son action en élaborant sa stratégie d'action en la matière.

Pour répondre à l'exposition croissante du secteur financier au risque informatique, l'ACPR a développé une stratégie selon les trois axes de la règlementation, du contrôle et de la coopération.

Réglementation

A ce titre, il s'agit de **travailler à l'adaptation de la règlementation et des « bonnes pratiques » d'encadrement du risque informatique.** Il est depuis longtemps reconnu comme une composante du risque opérationnel, mais il n'était pas décrit et analysé dans sa singularité jusqu'à récemment : vu comme un risque technique, il n'était que très faiblement encadré par la réglementation. En pratique, les normes professionnelles (comme les normes ISO notamment) étaient les principales références utilisées.

L'effort des superviseurs est désormais d'encadrer plus directement les obligations applicables. À son niveau, l'ACPR défend une vision claire et proportionnelle des différentes obligations qui devraient s'imposer et a notamment publié pour cela un document de réflexion sur le risque informatique[1]. Elle prend également activement part aux travaux européens pour y défendre ses positions. Parmi les enjeux qui relèvent de cette priorité, il s'agit d'aligner le niveau des exigences applicables aux différentes composantes du secteur financier européen. Récemment, l'ACPR a ainsi été co-auteure des futures *Guidelines on information and communication technologies (ICT) and security risk management* de l'Autorité Bancaire Européenne (ABE) et s'investit actuellement dans des travaux comparables auprès de l'Autorité Européenne des Assurances et des Pensions Professionnelles (AEAPP). Pour se conformer à ces travaux, une refonte du cadre règlementaire français relatif au risque informatique devra être envisagée.

[1] https://acpr.banque-france.fr/sites/default/files/medias/documents/819017_acpr_risque-informatique_fr_web.pdf

Contrôle

Face aux menaces grandissantes, notamment les cyber-attaques, les actions de contrôle ont également été renforcées. L'ACPR y prend part au travers du Mécanisme de supervision unique européen (MSU) ou directement pour les entités sous sa seule supervision. Le risque informatique – et tout particulièrement le cyber risque – a ainsi été érigé en **priorité de contrôle des banques et des organismes d'assurance**.

Les équipes de contrôle permanent procèdent par conséquent à des évaluations sous la forme de questionnaires. Les équipes de contrôle sur place mènent, pour leur part, des contrôles approfondis des systèmes d'information des établissements et réalisent des tests d'intrusion en s'appuyant notamment sur le *Computer Emergency Response Team* (CERT) de la Banque de France. Parmi les enjeux qui relèvent de ces actions, se trouve la nécessité de disposer d'informations fiables et rapides en cas d'incidents. Dans cette optique l'ACPR travaille à une catégorisation des incidents informatiques (de toutes natures et pas seulement « cyber ») ayant vocation à être utilisée à des fins de *reporting* d'incidents. Elle proposera cette démarche prochainement aux autres autorités des pays du G7 et à la BCE.

Coopération

Le dernier axe de la stratégie consiste à **renforcer la coopération de l'ACPR avec les différentes parties prenantes** en matière de risque informatique, et ce, à plusieurs niveaux.

L'intervention grandissante des superviseurs sur le risque informatique est un mouvement mondial. L'ACPR y prend part tant pour bénéficier de l'expérience des autres superviseurs que pour contribuer aux efforts communs en apportant son expertise. Sa participation aux travaux internationaux des normalisateurs (G7, Conseil de Stabilité Financière, Comité de Bâle sur le Contrôle Bancaire ou Association Internationale des Contrôleurs d'Assurance notamment) s'inscrit dans cette optique, tout comme les accords de coopération (*Memorandum of Understanding* - MoU) qu'elle signe avec certaines autorités étrangères (notamment pour partager des informations sur ces problématiques). L'enjeu principal de toutes ces démarches est d'harmoniser les approches des différentes juridictions pour éviter l'arbitrage règlementaire. Au plan international, l'ACPR a ainsi plaidé lors de la présidence française du G7 pour une mise en cohérence et une rationalisation des travaux normatifs des différents régulateurs. Au niveau national, elle travaille avec les autorités partenaires et notamment avec l'Autorité Nationale de Sécurité et de défense des Systèmes d'Information (ANSSI), qui dispose de l'expertise technique et de la vision transsectorielle des problèmes de cybersécurité. L'ACPR souhaite par ailleurs mobiliser de plus en plus la Place.

Des sujets parallèles viennent aussi nourrir les travaux et les actions de supervision puisqu'ils ont une incidence directe sur l'importance du risque et son atténuation (cyber assurance, intelligence artificielle et technologies financières par exemple).

Naturellement, pour mener à bien cette stratégie, l'ACPR doit aussi, comme les institutions contrôlées, développer ses ressources et ses compétences. Ainsi, la mise en œuvre de cette stratégie est progressive et s'adaptera à l'évolution du risque informatique, à la maturité des entités contrôlées et aux priorités fixées aux niveaux international et européen.