

# MISE EN ŒUVRE OPERATIONNELLE DE LA CYBERSECURITE



## CONTEXTE

L'externalisation de certains process (*back-office, compliance...*), associés aux activités commerciales, bancaires et de marchés, se multiplie depuis plusieurs années, les institutions financières souhaitant gagner en compétitivité, bénéficier des nouvelles technologies, améliorer leur flexibilité et leur efficacité ainsi que réduire leurs coûts. Dans ce contexte, l'EBA (European Banking Authority) a établi de nouvelles lignes directrices, publiées le 25 février 2019, qui viendront harmoniser les pratiques jusque-là encadrées sur le plan national (arrêté du 3 novembre 2014).

## OBJECTIFS

Le participant à cette formation aura acquis une vision claire de :

- ce qui a changé au niveau de la menace
- des nécessités d'adaptation des entreprises tant au niveau des opérations qu'au niveau de la gouvernance

## PUBLIC

- Responsables de sécurité des systèmes d'information
- Directeurs des systèmes d'information
- Responsables des risques SI
- Responsables des risques opérationnels
- *Risk managers*
- Décideurs dans les 5 domaines pré-cités

## PRÉREQUIS

- Cette formation ne nécessite pas de prérequis.

## MODALITÉS DE SUIVI ET APPRÉCIATION DES RÉSULTATS

- Questionnaire préalable à la formation
- Feuille d'émargement
- Attestation délivrée à l'issue de la formation

## PROGRAMME

### 1. INTRODUCTION ET QUELQUES RAPPELS

#### 2. CHANGEMENT DE PARADIGME

- 2.1 Évolution de la menace
- 2.2 Constats sur les anciennes approches de maîtrise des risques
- 2.3 Le développement de la réglementation, définitions
- 2.4 Caractéristiques fondamentales d'un dispositif moderne de gestion du risque cyber

### 3. L'ADAPTATION DES ENTREPRISES, DANS LE DÉTAIL

- 3.1 Principes de mise en œuvre d'un dispositif de cyber défense, maillon par maillon
- 3.2 Caractéristiques d'un dispositif de gouvernance adapté et du reporting stratégique
- 3.3 Stratification des lignes de défense
- 3.4 Caractéristiques fondamentales d'un dispositif moderne de gestion du risque cyber

### 4. QU'ATTENDRE D'UN PROGRAMME DE RENFORCEMENT CYBER ?

- 4.1 Les objectifs
- 4.2 Les écueils
- 4.3 La structuration et le positionnement du programme dans l'écosystème

### ÉCHANGES ET DÉBATS

**MERCREDI 6 OCTOBRE 2021**

Formation d'une journée  
DURÉE : 7h 8h30-16h30

#### MODALITÉS PÉDAGOGIQUES

- Présentiel
- Formation interactive et pratique : présentation théorique et cas pratiques, quizz/QCM
- Remise des supports de formation

Nombre de participants limité à 15

LIEU : 18, rue La Fayette 75009 Paris

TARIF : 1 040 € HT (1248€ TTC)

INSCRIPTION sur [rb-formation.fr](http://rb-formation.fr)

#### CONTACT

Caroline Breton :  
[formation@revue-banque.fr](mailto:formation@revue-banque.fr)  
Tél. : 01 48 00 54 04

## FORMATEUR

**Gil DELILLE** est Directeur des Risques des Systèmes d'Information du Groupe Crédit Agricole, 141.000 collaborateurs, présent dans près de 40 pays.

Après un début de carrière chez IBM teinté «grands projets», il est entré dans le monde de la sécurité en 1998. Il a, dès le départ, placé les métiers au premier plan de la démarche de renforcement de la sécurité et visé une intégration de la sécurité de l'information au fonctionnement général de l'entreprise.

Dix ans de présidence du Forum des Compétences en Sécurité des SI, lui ont permis d'appréhender les enjeux de Place et d'influencer l'adaptation du monde bancaire aux risques technologiques.

