ACADEMY & FINANCE

Gestion des risques opérationnels

> Nouveaux enjeux opérationnels : extension des heures d'ouverture des places boursières, accélération du processus de settlement, intégration de la blockchain et de l'IA
> Résilience opérationnelle des fonctions critiques : établir la tolérance aux perturbations, mesures préventives de remédiation, gestion des incidents et des crises
> Gestion des risques TIC, cyber, Third Party Risk Management, IA externalisée

Jérôme Desponds,
Consultant en gouvernance, gestion des risques et organisation de projets (ex-Chief Risk Officer dans le domaine bancaire)

Liburn Mehmetaj,
Avocat, MLaw, LL.M., Associé,
Walder Wyss, Genève

Jean-Noël Ardouin,
Partner, Financial Services Risk Consulting,
EY, Genève

Matthieu Neige,
Manager, Financial Services Risk Consulting,
EY, Genève

Hans Ulrich Bacher
Partner, Head of Risk Consulting, Financial Services,
KPMG Switzerland, Zurich

Benoit de Jocas,
Senior Manager,
Cybersecurity & Privacy,
PwC, Genève

Sébastien Rochat,
co-fondateur,
Mase Partners SA

Les nouveaux défis

8.40 **Nouveaux enjeux opérationnels : facteurs de risques, fonctions impactées et pistes de réflexion**
Les pratiques de marché requièrent une adaptation rapide et significative des processus opérationnels bancaires (extension des heures d'ouverture des places boursières, accélération du processus de settlement, intégration de la blockchain et de l'intelligence artificielle):
• quels sont les facteurs à prendre en compte ?
• comment les intégrer dans l'analyse des risques opérationnels ?
• quelles sont les parties prenantes concernées ?
• quelles sont les mesures à envisager ?
Jérôme Desponds

9.20 **Quelles sont les exigences réglementaires suisses et européennes en matière d'applications d'intelligence artificielle ? Quelles précautions prendre face aux risques de l'IA externalisée ?**
• Attentes de la FINMA : gouvernance et responsabilité ; robustesse et fiabilité ; transparence et explicabilité,
• Le nouveau règlement européen sur l'intelligence artificielle
• Risques de l'IA externalisée : les données restent en Suisse, bien que les « moteurs » soient à l'étranger
Liburn Mehmetaj

Résilience opérationnelle des fonctions critiques

10.00 **Qu'est-ce que la résilience opérationnelle ? Quelle profonde différence avec le Business Continuity Management (BCM) ?**
• Différence entre les objectifs du BCM (remédier à des défaillances isolées) et résilience opérationnelle (réussir à surmonter une crise majeure / générale, face à laquelle les mesures traditionnelles de gestion de la continuité seront inefficaces).
• La résilience opérationnelle porte sur l'ensemble de la chaine de valeur et non sur des processus et système TIC isolés
• Signification des tolérances qu'il faut établir et documenter pour chaque fonction critique : les tolérances devront définir le niveau minimum de service et de résultats requis de la part d'une fonction critique pour fonctionner pendant une crise
Jean-Noël Ardouin et Matthieu Neige

10.30 Pause-café

10.50 **Le processus pour établir la tolérance aux perturbations et le service minimum en cas de crise : rationalité, justification, documentation**
• La définition de la tolérance aux perturbations des fonctions critiques est une tâche plus complexe que prévu au départ
• Recueillir les données pour rationaliser le service minimum et les résultats définis
• Documenter la tolérance de perturbation sous forme d'une déclaration d'objectif basée sur les résultats et documenter les justifications et les données / preuves supplémentaires pour lesquelles la tolérance de perturbation respective a été choisie
• Evaluation des travaux effectués pour déterminer les tolérances des fonctions critiques ; points mal compris, pratiques défaillantes, bonnes pratiques
• Pratiques / choix des tolérances de perturbations pour les fonctions critiques telles que paiements, titres, trésorerie
Hans Ulrich Bacher

11.30 **Vulnérabilités et mesures préventives de remédiation**
• Exigences réglementaires en matière d'identification des vulnérabilités et de mise en place de mesures de remédiation- Les mesures préventives pour réduire les vulnérabilités (exemples), les mesures de défense (protective measures)
• La pratique par rapport aux fonctions critiques telles que paiements, titres, trésorerie
Jean-Noël Ardouin et Matthieu Neige

12.00 **Gestion des incidents et des crises : les attentes du régulateur, leçons des expériences de crise subies par les intermédiaires financiers**
• Exigences en matière de préparation de la gestion des crises
• Différences entre incident / crise / attaque ; défaillance isolée, crise générale
• Scenario based preparation,
• Détecter les crises
• Comment gérer / agir pendant la crise, durant l'attaque ; recovery measures, rétablissement du fonctionnement normal en temps de crise
• Les priorités en temps de crise
• Les leçons de la pratique d'intermédiaires financiers qui ont subi des crises
Hans Ulrich Bacher

12.50 Déjeuner

GENÈVE, JEUDI 5 JUIN 2025, 8.40-16.30, HÔTEL PRÉSIDENT / ONLINE (ZOOM)

Risques TIC et risques cyber

14.10 **La gestion des risques TIC/ICT**
• Objectifs et attentes selon la circulaire 2023/1 :
- Stratégie et gouvernance TIC,
- Gestion des changements
- Exploitation TIC
- Gestion des incidents
• Pratiques du marché & principaux manquements identifiés
Benoit de Jocas

14.40 **La gestion des cyber risques**
• Objectifs et attentes selon la circulaire 2023/1 :
- Gouvernance et reporting
- Gestion des risques cyber
- Mesures de protection
- Mesures de détection et réponse aux incident cyber
- Reprise et résilience
- Gestion des vulnérabilités et tests de pénétration
• Enseignements des « Supervisory Review » menées par la FINMA et des audits réalisés par PwC
• Points clés et bonnes pratiques.
Benoit de Jocas

15.20 Pause-café

Third Party Risk Management

15.40 **Quelles sont les nouvelles exigences par rapport aux externalisations/ outsourcings et à la surveillance des fournisseurs**
• Rappel des exigences découlant de la circulaire FINMA 2018/3 « outsourcing »
Approches théoriques et attentes de la FINMA
• Qu'est-ce qui a changé avec la nouvelle LPD ?
- Distinctions entre les autorités et les buts (données à protéger vs données critiques)
- Conformité avec la LPD à ajouter dans les contrats
- Adaptation aux contraintes européennes
• Qu'est-ce qui a changé avec la circulaire FINMA 23/1 « Risques et résilience opérationnels- banques ?
• Monitorage des risques FINMA 2024 : Que ressortir du rapport en matière de risques d'externalisation et cyber risques ? Qu'en est-il des autres risques sur lesquels effectuer une surveillance particulière ?
• Qui est responsable en cas de panne / défaut de résilience opérationnelle : entreprise ou prestataire ?
- Vision LPD : responsabilité du responsable de traitement (donc pas du prestataire) ; panne = perte de données ?; vol de données
- Résilience opérationnelle = continuité, ce qui sous-entend définir les processus critiques, etc.
- Hypothèse de la non-fourniture d'électricité suite à une guerre touchant un pays producteur
• Quelle est l'étendue des obligations de surveillance par rapport aux prestataires, à leurs employés, à leurs sous-traitants
• Comment doit être conduite l'évaluation des fournisseurs
- Evaluation contractuelle
- Remontée des incidents
- Entretien au moins annuel
- Approche risque sur la résilience opérationnelle et les fournisseurs qui sont liés, adapter les principes et la fréquence de la surveillance en fonction du risque représenté
Sébastien Rochat

16.30 Fin de la conférence

INFORMATION & INSCRIPTION
Tel: +41 22 849 01 11
info@academyfinance.ch
Academy & Finance SA
Rue Neuve-du-Molard 3, CP 3039,
CH-1211 Genève 3
www.academyfinance.ch

PRIX
1160 CHF (+ TVA 8.1%)
Inscriptions supplémentaires de la même société : -50%

AF 1423

☐ Je m'inscris au séminaire "Gestion des risques opérationnels" le 5 juin 2025.
☐ Je participerai dans la salle ☐ Je participerai online sur Zoom

Nom et prénom .....

Fonction .....

Société.....

Adresse .....

Code postal et ville .....

Tel .....Email..... .....

Date ..... Signature ... .