ACPR
BANQUE DE FRANCE

FORUM FINTECH 2021

CYBER-SÉCURITÉ ET RISQUE INFORMATIQUE : LE POINT SUR LA NOUVELLE RÉGLEMENTATION APPLIQUÉE AUX FINTECHS

CYRIL GRUFFAT & THIÉBAUT MEYER (DIRECTION DES AFFAIRES INTERNATIONALES)
VALÉRIE PIQUET (DIRECTION DES CONTRÔLES SPÉCIALISÉS ET TRANSVERSAUX)

11 OCTOBRE 2021

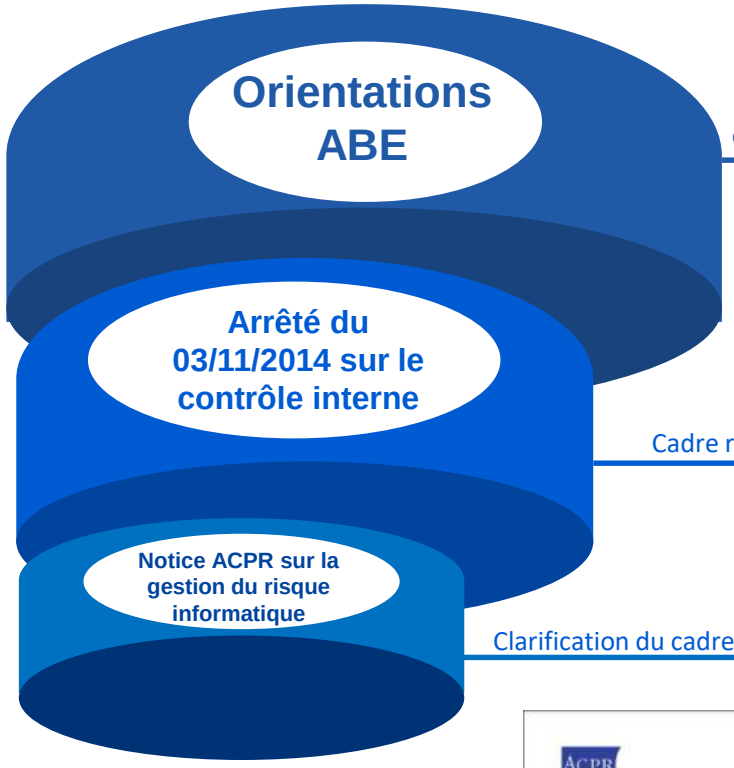
SOMMAIRE

1. Le cadre de référence
2. Les attentes du superviseur
3. À venir : le cadre européen DORA

1. LE CADRE DE RÉFÉRENCE

LE CADRE DE RÉFÉRENCE

CADRE RÈGLEMENTAIRE BANCAIRE FRANÇAIS



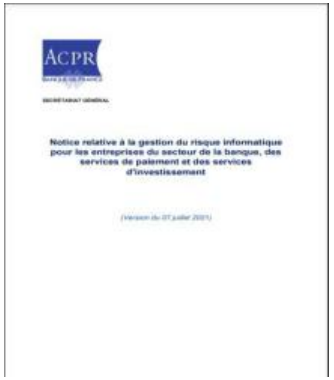
Cadre européen harmonisé → **ACPR déclarée conforme**

- EBA/GL/2019/04 : orientations sur la gestion du risque et de la sécurité informatique (11/2019)
- EBA/GL/2021/05 : orientations sur la gouvernance interne (07/2021)
- EBA/GL/2019/02 : orientations sur l'externalisation (02/2019)

Cadre règlementaire → **Conforme au cadre européen depuis 02/2021**

- Gouvernance / organisation du contrôle interne (titre 2, chapitre 1)
- Externalisation (titre 5, chapitre 2)
- Gestion de la continuité (article 215)
- Gestion du risque informatique (titre VI bis)

Clarification du cadre règlementaire → **Points de vigilance, bonnes pratiques**



- Gouvernance et dispositif de gestion du risque informatique (section 1)
- Gestion des opérations informatiques (section 2)
- Gestion des projets informatiques et des changements (section 3)
- Sécurité du système d'information (section 4)
- Gestion de la continuité d'activité (section 5)

LE CADRE DE RÉFÉRENCE

CADRE RÈGLEMENTAIRE ASSURANCE FRANÇAIS

Règlement délégué Solvabilité II (UE) 2015/35 du 10 octobre 2014

Orientations AEAPP relatives à la sous-traitance à des prestataires en nuage (EIOPA-BoS-20-002)

Cadre européen harmonisé

Dispositions prudentielles d'application directe

ACPR déclarée conforme

- Dispositions d'ordre général sur la gouvernance, la gestion des risques et le contrôle interne, applicables y compris aux technologies de l'information et de la communication
- Politique de sous-traitance, évaluation des risques induits et surveillance, gouvernance, contractualisation et pilotage, notifications, documentation

Code des Assurances

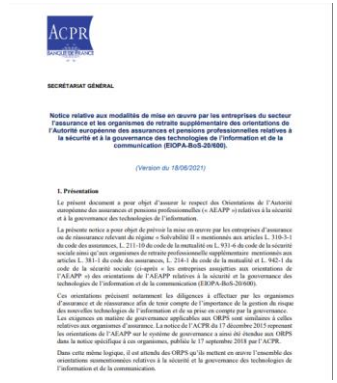
Cadre règlementaire

Dispositions générales couvrant de fait la gestion des risques inhérents aux systèmes d'information

- Articles L. 354-1 à L. 354-3 : système de gouvernance, système de gestion des risques et système de contrôle interne, gestion de la sous-traitance, continuité d'activité

Notice ACPR relative à la mise en œuvre des orientations AEAPP sur la gouvernance et la sécurité des TICs

Clarification du cadre règlementaire



ACPR

SECRÉTARIAT GÉNÉRAL

Notice relative aux modalités de mise en œuvre par les entreprises du secteur l'assurance et les organismes de retraite supplémentaire des orientations de l'Autorité européenne des assurances et pensions professionnelles relatives à la sécurité et à la gouvernance des technologies de l'information et de la communication (EIOPA-BoS-20/600).

(Version du 18/06/2021)

1. Présentation

Le présent document a pour objet d'assurer le respect des Orientations de l'Autorité européenne des assurances et pensions professionnelles (« AEAPP ») relatives à la sécurité et à la gouvernance des technologies de l'information.

La présente notice a pour objet de préciser la mise en œuvre par les entreprises d'assurance ou de réassurance relevant du régime « Solvabilité II » mentionnés aux articles L. 310-3-1 du code des assurances, L. 211-10 du code de la mutualité ou L. 931-6 du code de la sécurité sociale ainsi qu'aux organismes de retraite professionnelle supplémentaire mentionnés aux articles L. 381-1 du code des assurances, L. 214-1 du code de la mutualité et L. 942-1 du code de la sécurité sociale (ci-après « les entreprises assujetties aux orientations de l'AEAPP ») des orientations de l'AEAPP relatives à la sécurité et la gouvernance des technologies de l'information et de la communication (EIOPA-BoS-20/600).

Ces orientations précisent notamment les diligences à effectuer par les organismes d'assurance et de réassurance afin de tenir compte de l'importance de la gestion du risque des nouvelles technologies de l'information et de sa prise en compte par la gouvernance. Les exigences en matière de gouvernance applicables aux ORPS sont similaires à celles relatives aux organismes d'assurance. La notice de l'ACPR du 17 décembre 2015 reprenant les orientations de l'AEAPP sur le système de gouvernance a ainsi été étendues aux ORPS dans la notice spécifique à ces organismes, publiée le 17 septembre 2018 par l'ACPR.

Dans cette même logique, il est attendu des ORPS qu'ils mettent en œuvre l'ensemble des orientations nonobstant les orientations relatives à la sécurité et la gouvernance des technologies de l'information et de la communication.

Reprises des orientations (EIOPA-BoS-20/600)

- Proportionnalité, gouvernance et cadre de maitrise des risques (orientations 1 à 5)
- Gestion de la sécurité (orientations 6 à 13)
- Gestion des opérations et des incidents (orientations 14 et 15)
- Gestion des changements (orientations 16 à 18)
- Gestion de la continuité d'activité (orientations 19 à 24)
- Gestion de l'externalisation (orientation 25)

2. LES ATTENTES DU SUPERVISEUR

LES ATTENTES DU SUPERVISEUR

- La gouvernance
- La gestion du risque de tiers
- La cybersécurité

LA GOUVERNANCE

Carences constatées

- Manque d'implication des instances dirigeantes
- Insuffisante formalisation d'une stratégie informatique
- Asymétrie entre les ressources informatiques et les besoins
- Non respect du cadre règlementaire en matière d'organisation du contrôle interne du risque informatique en 3 niveaux
- Cadre de gestion du risque à compléter

Références règlementaires

Secteur Banque

- Art. 12, 270-1 et 270-2 de l'arrêté du 3 novembre 2014 sur le contrôle interne
- Section 1 de la Notice ACPR sur la gestion du risque informatique

Secteur Assurance

- Art. 258 – 261 bis, 266 – 273 du Règlement délégué SII
- Orientations 1 à 5 de la notice ACPR TICs 07/2021

Attentes du superviseur

- **Implication des dirigeants effectifs et du Conseil d'administration** dans les grandes décisions structurantes (définition et suivi de la stratégie informatique, assurance de la bonne allocation des ressources, participation au processus de décision du recours aux prestataires pour les prestations essentielles et importantes, décision et suivi des projets informatiques les plus importants…)

- **Allocation budgétaire claire et suffisante**, et cohérence entre stratégie informatique et budget informatique

- Disposer d'une **deuxième ligne de défense suffisante**, y compris dans le cas où le RSSI est positionné en première ligne.
  - Cas particulier des établissements dont la « *taille ne justifie pas de confier les responsabilités du contrôle permanent et du contrôle périodique à des personnes différentes* » (art. 18 arrêté du 03/11/14)

- Disposer d'une **cartographie complète des risques comprenant toutes les dimensions du risque informatique** et d'un **cadre d'appétit pour le risque adapté** (limites d'appétit pour le risque, indicateurs de suivi quantitatifs, processus prévu en cas de dépassement des limites, responsabilités des parties prenantes, modalité de révision du cadre, …)

- **Inventorier tous les actifs informatiques** en appréciant leur niveau d'importance pour la bonne gestion des processus informatiques

LE RISQUE DE TIERS

Carences constatées

- Gouvernance imparfaite (manque d'implication des dirigeants, absences de stratégie claires d'externalisation, etc.)
- Maîtrise du risque insuffisante due à un manque d'anticipation
- Méconnaissance de la chaîne complète d'externalisation
- En particulier sur les services de Cloud public :
  - Relation asymétrique au détriment de l'institution financière (et ses conséquences sur la relation contractuelle, et notamment le droit d'audit)
  - Risque de concentration

Références règlementaires

<u>Secteur Banque</u>

- Art. 231 à 240 de l'arrêté du 3 novembre 2014 sur le contrôle interne
- Points 3 et 7 de la Notice ACPR sur la gestion du risque informatique

<u>Secteur Assurance</u>

- Art. 274 du Règlement délégué SII
- Orientation 25 de la notice ACPR TICs 07/2021

Attentes du superviseur

- **Gestion du risque ex-ante**
  - Analyse de risques préalable
  - Réversibilité
  - Vigilance sur les contrats (doits d'accès et d'audit, accès du superviseur, cycle de vie des données, réversibilité, etc.)
  - Compétences internes suffisantes
  - Définition de mesures adéquates (ex : chiffrement)
  - Identification des principaux sous-traitants du prestataire
- **Suivi et pilotage** de la prestation (ex : procédure de traitement des incidents opérationnels ou de sécurité)
- **Harmonisation** des registres

ACPR
BANQUE DE FRANCE

LES MESURES DE SÉCURITÉ LOGIQUE ET CONTINUITÉ D'ACTIVITÉ

Carences constatées

- Points de faiblesse identifiés concernant les mesures de sécurité logique
  - ➢ *Ex : postes de télétravail peu sécurisés (notamment durant la crise Covid-19)*
- Incidents détectés tardivement
- Tests d'intrusion incomplets
- Plans de continuité / analyses d'impacts imparfaits

Références règlementaires

Secteur Banque

- Articles 270-3 et 215 de l'arrêté du 3 novembre 2014 sur le contrôle interne
- Sections 4 et 5 de la Notice ACPR sur la gestion du risque informatique

Secteur Assurance

- Art. 258 (1 j), 258 (3) et 274 (4 e) du Règlement délégué SII
- Orientation 8 de la notice ACPR TICs 07/2021

Attentes du superviseur

- **Effectuer des analyses de risque** régulières et les maintenir à jour
- **Adapter les mesures** de sécurité logiques (segmentation réseau, authentification multi-facteurs, chiffrement, mises à jour de sécurité, etc.)
- Formaliser et mettre en place un processus de **gestion des droits d'accès**
- Formaliser et mettre en place des mécanismes de **détection des anomalies et des incidents**
- **Définir un cadre de tests** de la sécurité du SI prenant en compte ses particularités et l'actualité des menaces
- Établir un dispositif de **gestion de la continuité d'activité**
  - ➢ Maintien des services
  - ➢ Limitation de l'impact
  - ➢ Prise en compte des critères d'intégrité et de confidentialité

3. À VENIR : LE CADRE EUROPÉEN DORA

A VENIR : LE CADRE EUROPÉEN DORA

DIGITAL OPERATIONAL RESILIENCE ACT (EN COURS DE NÉGOCIATION)

Périmètre très large (banques, assurance, CSD, CCP, etc.)

Règlement européen DORA

Première version publiée le 24 septembre 2020

La gestion du risque informatique

- Des règles homogènes
- Une gouvernance appropriée
- Des mesures techniques

Une meilleure prise en compte des incidents de sécurité

- Améliorer la réponse aux incidents
- Catégorisation des incidents
- Notifier au superviseur les incidents majeurs

Les tests de sécurité

- Évaluer le niveau de sécurité
- Formaliser une stratégie de tests
- Tests de sécurité « avancés » (*TLPT*)

La gestion du risque de tiers

- Gérer les risques liés aux prestataires de services informatiques
- Surveillance des prestataires critiques par les AES
  - Création d'un *Oversight Forum* européen

MERCI DE VOTRE ATTENTION