



FORUM FINTECH 2020

CYBER SÉCURITÉ ET NOUVELLE RÈGLEMENTATION DU RISQUE INFORMATIQUE : QUELLE APPLICATION AUX FINTECHS ?

MARC ANDRIES (DCP)
CYRIL GRUFFAT & THIÉBAUT MEYER (DAI)

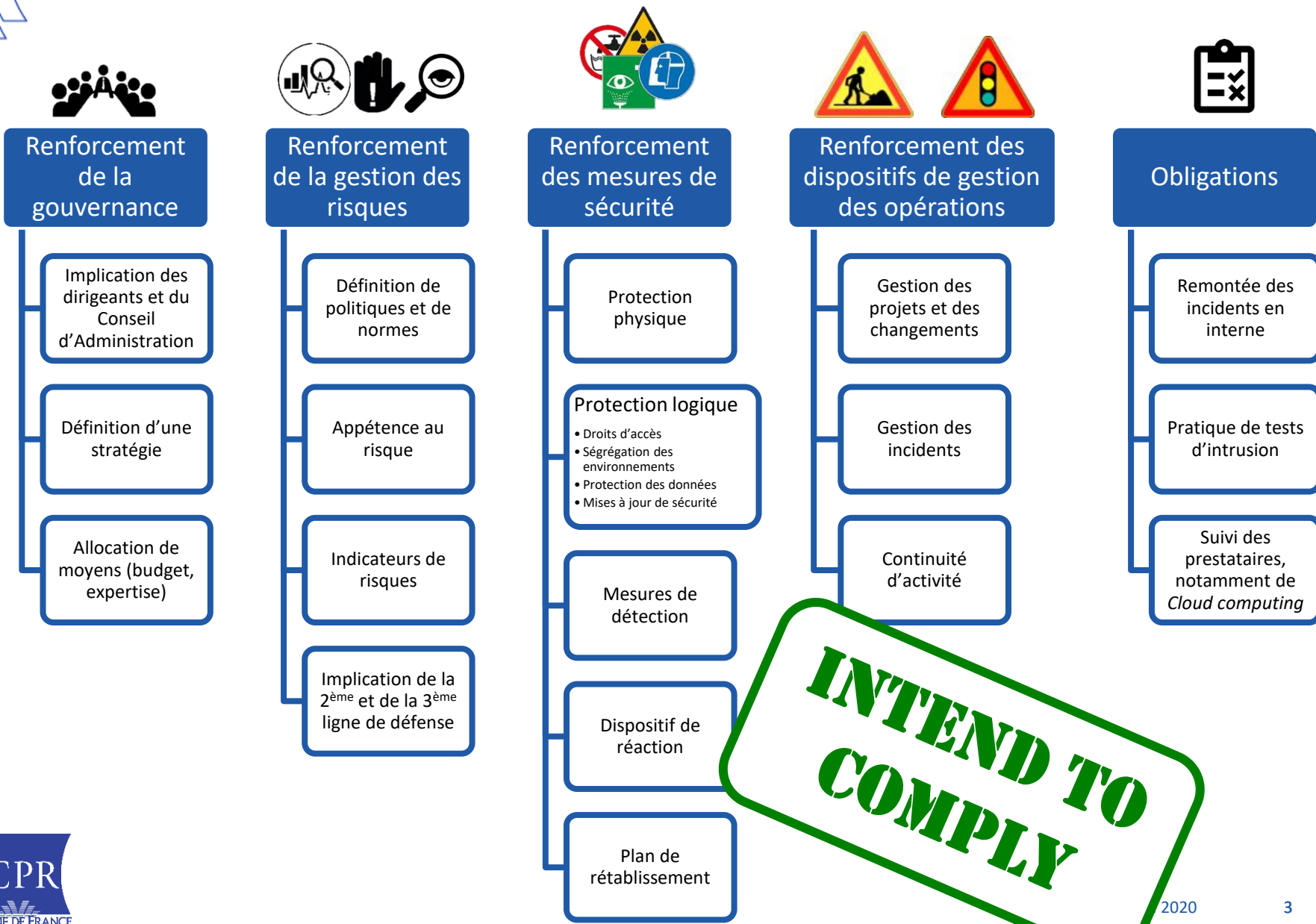
12 OCTOBRE 2020



SOMMAIRE

1. Le cadre de référence : les orientations de l'EBA
2. Les attentes du superviseur

LE CADRE DE RÉFÉRENCE : GL EBA (EBA/GL/2019/04)





LES ATTENTES DU SUPERVISEUR

- La gouvernance
- La gestion du risque
- Le risque de tiers
- La gestion des opérations
- La gestion des projets
- Les mesures de sécurité physique et logique
- Les tests de sécurité
- La continuité d'activité
- Les prestataires de service de paiement

Les objectifs

- Bâtir une approche fondée sur les risques
- Établir une gestion des risques cohérente
- Aligner cette gestion du risque sur les stratégies de l'entreprise
- Garantir une vision « extérieure » de la sécurité de SI et détachée de l'opérationnel

La réglementation

- Une stratégie du risque informatique et un appétit pour le risque approuvés par les dirigeants
- Alignement des ressources humaines et budgétaires avec les besoins de la stratégie
- Implication des dirigeants sur le recours aux tiers prestataires
- Trois lignes de défense indépendantes

Les attentes du superviseur

- Inclure les dirigeants dans les décisions portant sur la sécurité
- Définir clairement les rôles et les responsabilités de chacun
- Comprendre les enjeux liés à l'évolution et la maîtrise des systèmes d'information
- Documenter la gestion du risque (analyse de risques, mesures mises en place, risques résiduels, etc.)



LA GESTION DU RISQUE

Les objectifs

- Aligner la gestion du risque informatique avec la gestion du risque opérationnel :
 - *Assurer un challenge efficace pour la détermination de l'encadrement du risque informatique (limites d'appétit au risque, politiques de maîtrise du risque conformes)*
 - *Suivre le modèle des 3 lignes de défense.*
 - *En particulier, faire jouer à la Direction des Risques (ou une fonction de contrôle de deuxième niveau) le rôle d'encadrement et de surveillance des risques*
 - *Disposer d'un dispositif efficace, suivant les principes de gestion du risque opérationnel (identification, évaluation, contrôles, suivi)*

La réglementation

- Affirmation de l'obligation de gérer le risque informatique selon les principes de gestion des risques fixés dans les EBA *GL on internal governance* (Sept. 2017)
- Principe d'indépendance entre les activités de la 1^{ère} ligne de défense (i.e. direction informatique, équipes sécurité) et de la 2^{ème} ligne de défense (i.e. fonction de contrôle comme la Direction des risques)
- Le positionnement du RSSI est libre: il doit y avoir des équipes de sécurité dans la 1^{ère} et dans la 2^{ème} lignes.
- Exigences fortes sur l'identification et la classification des processus des métiers et des fonctions, des équipes impliquées par ces processus, des actifs informatiques et informationnels liés)
- Obligation claire sur la formation et la sensibilisation

Les attentes du superviseur

- Implication d'une fonction de contrôle indépendante, comme la fonction de gestion des risques: le risque informatique ne doit pas être laissé à la direction informatique
- Le traitement du risque informatique doit suivre les méthodologies en place pour le risque opérationnel (cartographie compatible, évaluation, contrôles, *monitoring* et *reporting*)
- Vision bout-en-bout du risque (*mapping* de toutes les interdépendances)
- Programmes clairs de formation et de sensibilisation (notamment pour la cybersécurité)

LE RISQUE DE TIERS

Les objectifs

- S'assurer que le recours à un prestataire (extérieur ou intra-groupe) n'entraîne pas une augmentation du risque opérationnel :
 - *Conserver le contrôle des opérations externalisées*
 - *Conserver un pouvoir de négociation réel vis-à-vis du prestataire*
 - *Assurer la réversibilité dès le départ*

La réglementation (*orientations EBA/GL/2019/02*, arrêté du 03/11/14 sur le contrôle interne)

- **Gouvernance** : pas de délégation de responsabilité, identification des responsabilités, implication des dirigeants, politique dédiée à l'externalisation, analyse ex-ante
- **Outils de gestion du risque** : registre des prestataires tenu à jour, dispositifs de réversibilité, chiffrage, limitation des concentrations, audit
- **Sécurité contractuelle** : contrat écrit, localisation des données, droit d'accès/d'audit, accès du superviseur au prestataire, identification des principaux sous-traitants du prestataire

Les attentes du superviseur

- **Vigilance sur les contrats** (audit, accès du superviseur, localisation des données)
- **Localisation des données** sur le territoire de l'Union Européenne
- **Recourir à des prestataires européens**, faisant eux-mêmes si possible globalement appel à des sous-traitants européens
- **Harmonisation des registres** : attention à ne pas référencer plusieurs fois un même prestataire avec des noms/acronymes différents
- **Modifications à venir dans l'arrêté du 03/11/14** : notification à l'ACPR en cas d'externalisation essentielle ou importante (art. 232) et obligation du registre des tiers prestataires (art. 238)



LA GESTION DES OPÉRATIONS

Les objectifs

- S'assurer que les services informatiques répondent aux besoins des utilisateurs
- Limiter les erreurs. Si elles surviennent, il faut être capable de :
 - *Les détecter au plus tôt*
 - *Les analyser*
 - *Les corriger*
- Gérer les incidents opérationnels ou de sécurité

La réglementation

- Mettre en place un inventaire des actifs informatiques. On y précise :
 - *Leurs caractéristiques (emplacement, classification de sécurité, propriétaire, etc.)*
 - *Leurs liens de dépendance*
- Gérer le cycle de vie des actifs informatiques et traiter les risques liés à leur obsolescence
- Surveiller la bonne performance des systèmes
- Mettre en place des procédures de sauvegarde... et de restauration !
- Mettre en œuvre un mécanisme de gestion des incidents

Les attentes du superviseur

- Un inventaire qui permet :
 - *La gestion courante*
 - *La gestion du changement*
 - *Le traitement des incidents*
- Gestion des correctifs et des mises à jour
- Adapter la politique de sauvegardes aux besoins (RTO, RPO, etc.) et la tester

LES MESURES DE SÉCURITÉ PHYSIQUE ET LOGIQUE

Les objectifs

- Protéger le SI contre les actes malveillants (sûreté : intrusion, détérioration, prise de contrôle, vol, espionnage...) et les accidents affectant l'environnement de l'entreprise (sécurité : catastrophe naturelle, incendie, fuite d'eau...), y compris les menaces
- Intégrité / confidentialité / disponibilité

La réglementation

- Politique de sécurité écrite fondée sur une analyse des risques
- Sécurité physique adaptée à l'importance et la sensibilité des bâtiments
- Sécurité logique fondée sur des principes (besoin d'en connaître, moindre privilège, séparation des tâches)
- Existence de procédures pour prévenir et traiter les problèmes de sécurité du SI
- Veille permanente relative aux menaces, et dispositifs d'identification des comportements anormaux

Les attentes du superviseur

- Approche proportionnelle : analyse des risques pour identifier les actifs et fonctions essentiels qui doivent être les mieux protégés
- A défaut de pouvoir parfaitement sécuriser, adoption de mesures compensatoires
- Des dispositifs minimum :
 - *limitation des comptes génériques/partagés,*
 - *politique de droit d'accès avec renouvellement périodique,*
 - *enregistrement des activités des utilisateurs (surtout des utilisateurs privilégiés),*
 - *mesures d'authentification avec mots de passe complexes,*
 - *détection des intrusions*



LA GESTION DES PROJETS ET DES CHANGEMENTS

Les objectifs

- Éviter que les changements (maintenance/projets/acquisition) apportés au SI n'entraînent des dysfonctionnements
- S'assurer que les modifications apportées permettent aux SI de répondre en permanence aux besoins des utilisateurs

La réglementation

- Projets : cadre de gouvernance clair, politique de gestion de projets, analyse des risques par le contrôle permanent, état d'avancement et risques associés communiqués aux dirigeants effectifs et à l'organe de surveillance
- Acquisitions : processus de gestion de l'acquisition/du développement, limitation des applications développées et gérées sans recours aux unités informatiques
- Changements : processus formalisé y compris pour les changements opérés en urgence, évaluation des conséquences sur les mesures de sécurité du SI

Les attentes du superviseur

- Des politiques et processus documentés, témoignant d'un effort d'anticipation et de pilotage effectif
- Strict séparation des environnements
- Importance des tests



LES TESTS DE SÉCURITÉ

Les objectifs

- Vérifier le niveau de sécurité du système d'information
- Vérifier la pertinence des mesures et leur bonne mise en place
- Identifier les points faibles
- Compléter l'analyse de risques

La réglementation

- Un cadre de test
 - *Qui tient compte des menaces et des particularités du SI*
 - *Qui précise les différents types de tests*
- Ce cadre doit garantir en particulier l'indépendance des équipes chargées des tests
- La récurrence des tests est fixée en fonction des risques et de la sensibilité

Les attentes du superviseur

- Les tests sont correctement ciblés en fonction de la sensibilité des systèmes et des données
- Une gradation possible en fonction de la maturité de l'établissement
 - *La comparaison avec les standards et les bonnes pratiques*
 - *Des tests d'intrusion ciblés*
 - *Des analyses de code*
 - *Red-team / tests basés une analyse préalable de la menace (« Threat Led Penetration Test » - TLPT)*
- Un appel à des prestations extérieures pour garantir l'indépendance (et la compétence) des équipes
- Les prescriptions issues des tests sont bien prises en compte... en fonction du risque !

LA CONTINUITÉ D'ACTIVITÉ

Les objectifs

- Assurer la capacité à maintenir les services
- Limiter les pertes en cas de perturbation grave
- Disposer des moyens informatiques pour y répondre

La réglementation

- Fonder le dispositif sur une analyse des impacts de perturbations graves
 - *Évaluation quantitative et qualitative*
 - *Prises en compte de toutes les données disponibles*
- Fixer des RTO et RPO et concevoir des services cohérents avec ces objectifs
- Document un Plan d'Urgence et de Poursuite d'Activité (PUPA) qui est validé par les dirigeants
- Élaborer un Plan de Reprise d'Activité (PRA) qui comporte les mesures d'urgence pour maintenir les activités essentielles, cohérent avec le PUPA
- Tester ces dispositifs
- Préparer des plans de communication (internes et externes)

Les attentes du superviseur

- Prendre en compte la sensibilité et l'importance des activités
- Mettre à jour les dispositifs (au moins annuellement) en fonction
 - *des incidents*
 - *des résultats des tests*
 - *des changements majeurs*
- Les tests des dispositifs doivent
 - *Être basés sur des scénarios pertinents et variés*
 - *Prévoir une bascule de la production vers les environnements de secours*
 - *Inclure les prestataires de services*



LES PRESTATAIRES DE SERVICE DE PAIEMENT

Les objectifs

- Aligner les règles de gestion du risque informatique et de sécurité entre EC et PSP
- Intégration des mesures du RTS art.95 PSD2 dans les nouvelles GL
- Maintien de dispositions spécifiques aux PSP pour la protection des utilisateurs de services de paiement (section 3.8)

La réglementation

- Obligation de sensibilisation des usagers à la sécurité et aux menaces sur leur service de paiement
- Le PSP doit laisser la possibilité aux usagers de :
 - *Désactiver des fonctionnalités pour sa sécurité;*
 - *Demander l'activation de fonctionnalités d'alertes de sécurité*
- Le PSP doit informer de nouvelles menaces et fournir son assistance aux usagers

Les attentes du superviseur

- Application proportionnelle des règles de gestion du risque et de sécurité aux PSP (sensibilité des activités, importance des opérations, etc.)
- Protection des paiements et maintien des règles spécifiques issues de la DSP2

MERCI DE VOTRE ATTENTION

