Les FSN du secteur financier : le point de vue de la CSSF

3 février 2020

David HAGEN
Premier Conseiller de Direction, Surveillance des Systèmes d'Informations et des PSF de support

Introduction

- Directive NIS : Périmètre cross-sectoriel,
  - Industries (énergie, transport, santé, etc.),
  - Banques, certaines infrastructures de marchés financiers,
  - Fournisseurs de services numériques.
- La loi NIS transposant cette directive désigne l'Institut Luxembourgeois de Régulation (ILR) et la CSSF comme autorités compétentes pour différents secteurs.
- L'ILR est également désigné comme « point de contact » unique, ce qui en pratique implique que les échanges d'information avec les autorités des autres pays et la Commission Européenne passent par l'ILR.

Introduction

- En relation avec la compétence de la CSSF :
  - Les exigences de la loi NIS s'appliquent uniquement aux banques et infrastructures de marchés financiers considérées comme des « Opérateurs de Services Essentiels » (OSE) et à tous les FSN .
- Les fournisseurs de services numériques (FSN) sont d'office concernés par la loi NIS et les exigences sont donc applicables pour tous. Aucun processus d'identification similaire à celui des banques et des infrastructures de marchés financiers n'est prévu par la loi NIS.

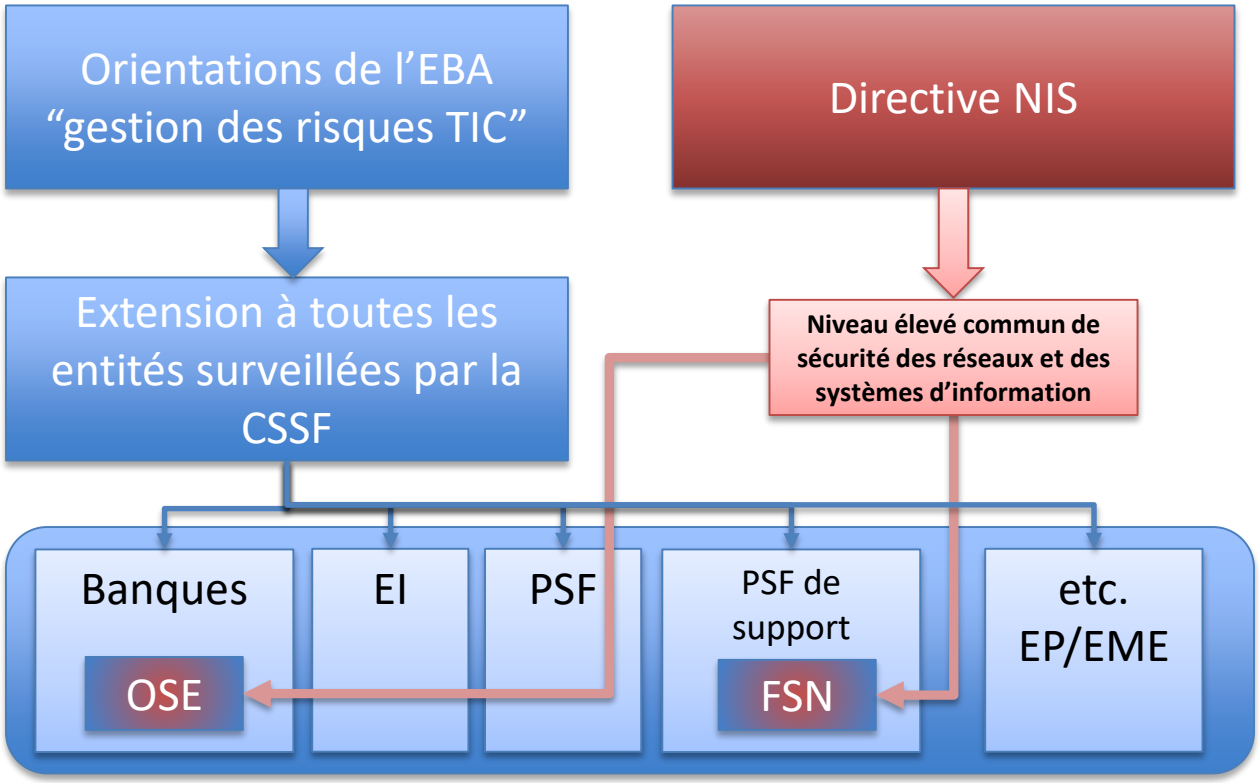
Introduction

- Introduction de nouveaux rapports / notifications obligatoires vers la CSSF, notamment :
  - Obligation pour les OSE de notifier les mesures de gestion des risques selon des modalités (format, délai, etc.) à définir par la CSSF par voie de règlement
  - Obligation pour les OSE et les FSN de notifier les incidents significatifs, là aussi selon des modalités (format, délai, etc.) à définir par la CSSF par voie de règlement.

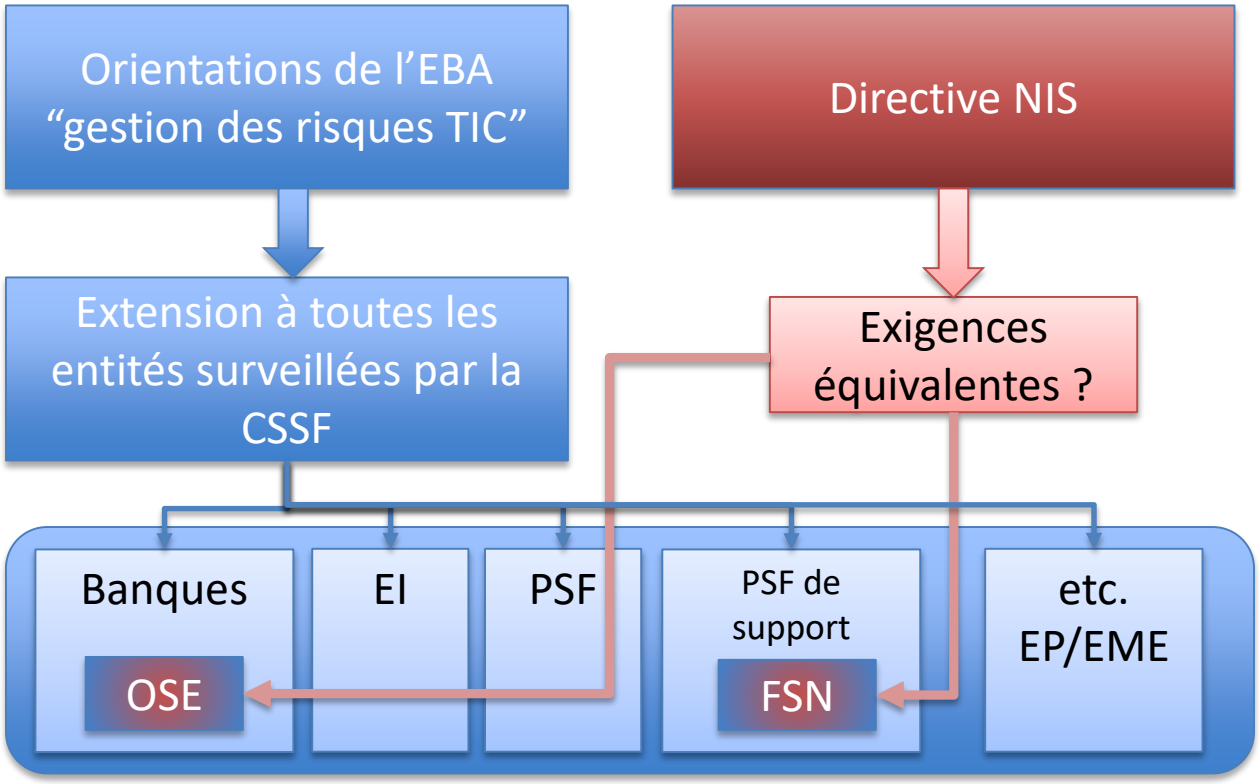
Contexte de la surveillance européenne

- L'autorité bancaire européenne (ABE)
  - A publié le 28 novembre 2019, avec application au 30 juin 2020, les orientations relatives à la gestion des risques TIC et de sécurité (EBA/GL/2019/04) qui doivent être transposées par la CSSF.
  - Ces orientations listent les mesures de gestion des risques informatiques et de sécurité à implémenter par les institutions financières.
  - Elles s'appliquent aux établissements de crédits, entreprises d'investissements, établissements de paiement et établissements de monnaie électronique

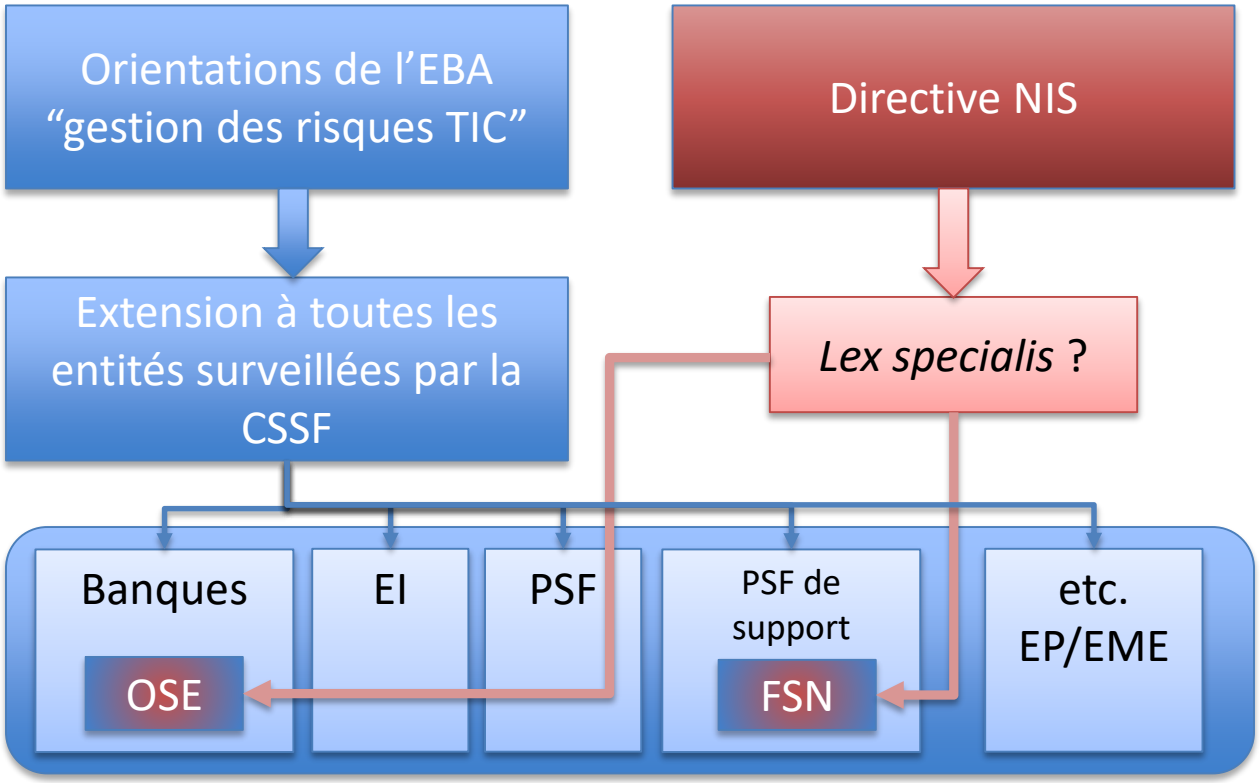
Convergence des obligations



Convergence des obligations



Convergence des obligations



Problématique *lex specialis* de la loi NIS

- L'interprétation de cette clause *lex specialis* dans la loi NIS reste incertaine.
- Bien qu'une analyse juridique soit encore en cours, la CSSF opte pour une approche prudente et ne considère pas la possibilité d'appliquer une *lex specialis*

Circulaire ou règlement ?

- Indépendamment de l'applicabilité d'une *lex specialis*, la CSSF reste contrainte de produire :
  - Un règlement définissant les services essentiels,
  - Une circulaire ou un règlement couvrant les mesures de sécurité informatiques qui font parties des orientations de l'ABE.
- Pour ce deuxième point, la loi NIS imposerait donc uniquement le format (à savoir un règlement) et quelques spécificités supplémentaires :
  - La notification des mesures de sécurité pour les opérateurs de services essentiels et
  - La notification des incidents pour les fournisseurs de services numériques).

Quels sont les FSN surveillés par la CSSF?

- Les FSN qui sont sous la surveillance de la CSSF sont les PSF de support qui sont considérés comme « Fournisseurs de services *cloud* » au sens de la circulaire CSSF 17/654
- La circulaire précise les cinq critères selon la terminologie reconnue (NIST, ENISA), auxquels s'ajoutent deux critères décisifs :
  - 5 critères / caractéristiques : libre-service à la demande, large accès au réseau, mise en commun des ressources, élasticité rapide et service mesuré
  - 2 critères supplémentaires :
    - Sauf dans des situations exceptionnelles, le fournisseur n'accède pas aux données et aux systèmes de l'ISCR (c'est-à-dire le consommateur) sans son consentement préalable et sans le mécanisme de contrôle dont dispose l'ISCR
    - Pas d'interaction manuelle du prestataire en ce qui concerne la gestion quotidienne des ressources (utilisation d'un automate/robot)

Conclusion

- La CSSF va élaborer :
  - Un **règlement** CSSF couvrant les mesures de gestion des risques informatiques et de sécurité et incluant :
    a. Les mesures de gestion des risques et de sécurité à implémenter par les institutions financières (reprises des orientations de l'ABE et le règlement d'exécution (UE) 2018/151 pour les FSN).
    b. La notification à la CSSF des mesures techniques et organisationnelles (afin de gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information) pour les OSE, les FSN , les PSPs (exigés sous PSD2) et pour les autres entités jugées à risques par la CSSF.
    c. La notification des incidents de sécurité et opérationnels pour les FSN, les OSE, les PSPs et les autres entités jugées à risques par la CSSF. En parallèle, la circulaire CSSF 11/504 relative à la notification à la CSSF des fraudes et incidents dus à des attaques informatiques externes sera révisée. Il conviendra aussi de reprendre les exigences du règlement d'exécution (UE) 2018/151 pour les FSN.

COMMISSION
DE SURVEILLANCE
DU SECTEUR
FINANCIER

Merci pour votre attention!