DORA - Résilience opérationnelle

Contexte et attentes des autorités, repères réglementaires et modalités de mise en œuvre

Des menaces grandissantes

- Sophistication croissante des attaques
- Nuisance grandissante (chiffrement, vol de données, sabotage)

Des vulnérabilités persistantes

- Défauts de gouvernance des sujets informatiques et de sécurité
- Défauts de gestion du risque
- Pertes de maîtrise du SI (complexité, sous-traitance, transformation)
- Défauts de sécurité
- Dispositifs de continuité ou de résilience insuffisant
- Exercice : partage des indicateurs et sources de menaces globales et spécifiques.

Les autorités se mobilisent ; Qui est à la manœuvre ?

- Framework international de cybersécurité
- Convention de Budapest sur la cybercriminalité : Principal traité international destiné à combattre les crimes de l'Internet.
- Textes et acteurs en Europe
    - Directives : UE) 2022/2555 NIS2, Directive (UE) 2022/2556 RESOFI, Directive (UE) 2022/2557 REC
    - Règlement général sur la protection des données (RGPD)
- Les acteurs à la manœuvre : ENISA, CERT-EU, EC3 ECSC, ETSI
- Textes et acteurs en France

Risques et incertitudes dans le domaine Cyber - Une priorité

- Une priorité des Superviseurs

5 piliers principaux

- Un enjeu de gouvernance pour un dispositif de résilience adapté et opérant
- Des obligations de reporting des incidents (connaître et réagir à la menace)
- Des obligations de tests de sécurité (s'assurer du caractère réellement opérationnel de la protection)
- Une gestion attentive des risques issus des prestataires tiers
- Un partage d'informations pertinentes

Qui doit se traduire en actions

- Une mesure des risques et incertitudes
- Une réponse adaptée à chaque situation
- Les enjeux de gouvernance
- La stratégie doit répondre aux menaces induites par les choix et évolutions
- Un plan d'actions pour se protéger efficacement

Les actions prioritaires

- Les stratégies
- les rôles
- Actions et Livrables
- Rappel du cadre d'analyse de l'ACPR

Stratégie de supervision prudentielle pour l'ACPR pour le risque informatique

- Organisation du SI (dont la SSI)
- Sécurisation du SI
- Exercice : Quiz

Gestion des risques liés aux TIC et des incidents

- Les acquis
- Les exigences de DORA
- Les précisions de DORA

Tests

- Les acquis
  - Stress Tests de place
  - Tests de résilience cyber de l'AMF
- Les exigences de DORA
- Les précisions de DORA
- Exercice : Définition d'une approche et liste des livrables

Encadrement des prestataires

- Les acquis
- Les exigences de DORA
- Les précisions de DORA
- Exercice : Définition d'une approche et liste des livrables

Partage d'information

- Les acquis
- Les exigences de DORA
- Les précisions de DORA
- Exercice : Définition d'une approche et liste des livrables

VALIDATION DES ACQUIS PAR QUIZ