Homologation de sécurité du SI Lyon 2

Présentation de la démarche
CA du 17/11/2023

CONTEXTE REGLEMENTAIRE (1/2)

https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045537693

Décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics

fixe les règles de gouvernance de la sécurité numérique au sein des administrations de l'Etat et **des établissements publics** sous sa tutelle

introduit en outre une **homologation de sécurité** des infrastructures et services logiciels informatiques du système d'information et de communication de l'Etat.

UNIVERSITÉ LUMIÈRE LYON 2

CONTEXTE REGLEMENTAIRE (2/2)

Décret n° 2022-513 du 8 avril 2022

Art 3 .- Les infrastructures et services logiciels informatiques qui, à la date d'entrée en vigueur du présent décret, composent le système d'information et de communication de l'Etat font l'objet de **l'homologation de sécurité dans un délai de deux ans** à compter de cette date.

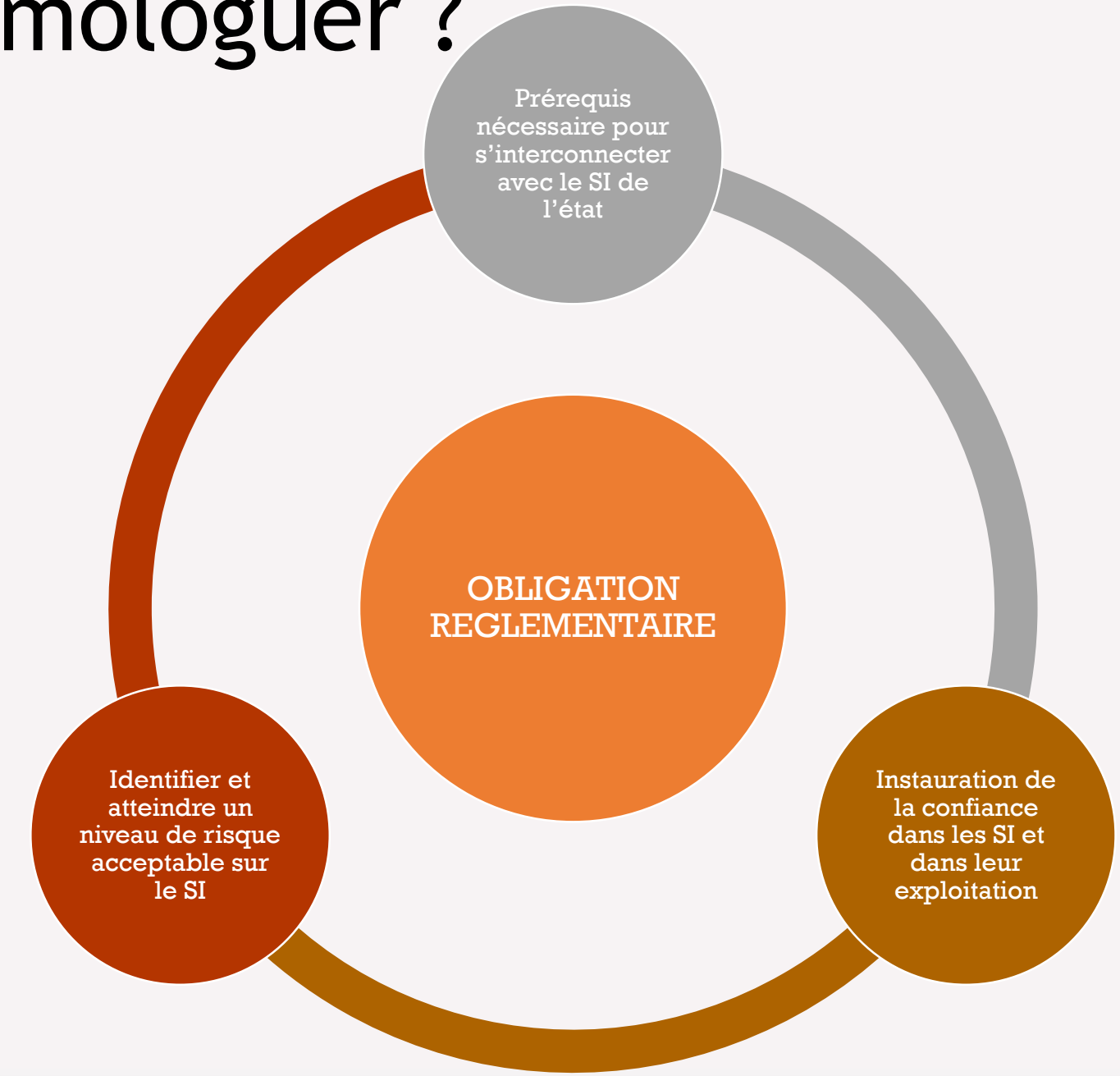
Art. 4-3.- Les infrastructures et services logiciels informatiques qui composent le système d'information et de communication de l'Etat font l'objet, **préalablement à leur mise en œuvre**, d'une homologation de sécurité.

Décision formelle prise par l'AQSSI* (ou par toute personne à qui elle délègue cette fonction) qui atteste que :
- les risques pesant sur la sécurité ont été identifiés et que les mesures nécessaires pour maîtriser ces risques sont mises en œuvre;
- les éventuels risques résiduels ont été identifiés et acceptés par l'AQSSI.

UNIVERSITÉ LUMIÈRE LYON 2

**AQSSI = Autorité Qualifiée pour la Sécurité des Systèmes d'Information / interne à l établissement*

Pourquoi homologuer ?



UNIVERSITÉ LUMIÈRE LYON 2

Comment homologuer ?

- Démarche recommandée par le Ministère
  - Classer les Systèmes d'Information par ordre d'importance pour l'établissement

    SI critiques
    SI sensibles
    SI standards
  - Traiter les homologations par vagues, et par ordre d'importance décroissant

- Méthode « type » proposée par l'ANSSI: 4 temps et 9 étapes

UNIVERSITÉ LUMIÈRE LYON 2

Démarche ANSSI

Définition de la stratégie d'homologation

- **Étape no 1 : Quel système d'information dois-je homologuer et pourquoi ?**
  - Définir le référentiel réglementaire applicable et délimiter le périmètre du système à homologuer.
- **Étape no 2 : Quel type de démarche dois-je mettre en œuvre ?**
  - Estimer les enjeux de sécurité du système et en déduire la profondeur nécessaire de la démarche à mettre en œuvre.
- **Étape no 3 : Qui contribue à la démarche ?**
  - Identifier les acteurs de l'homologation et leur rôle (décisionnaire, assistance, expertise technique, etc.).
- **Étape no 4 : Comment s'organise-t-on pour recueillir et présenter les informations ?**
  - Détailler le contenu du dossier d'homologation et définir le planning.

Maîtrise des risques

- **Étape no 5 : Quels sont les risques pesant sur le système ?**
  - Analyser les risques pesant sur le système en fonction du contexte et de la nature de l'organisme et fixer les objectifs de sécurité.
- **Étape no 6 : La réalité correspond-elle à l'analyse ?**
  - Mesurer l'écart entre les objectifs et la réalité.
- **Étape no 7 : Quelles sont les mesures de sécurité supplémentaires à mettre en œuvre pour couvrir ces risques ?**
  - Analyser et mettre en œuvre les mesures nécessaires à la réduction des risques pesant sur le système d'information. Identifier les risques résiduels.

Prise de décision

- **Étape no 8 : Comment réaliser la décision d'homologation ?**
  - Accepter les risques résiduels : l'autorité d'homologation signe une attestation formelle autorisant la mise en service du système d'information, du point de vue de la sécurité.

Suivi a posteriori

- **Étape no 9 : Qu'est-il prévu pour maintenir la sécurité et continuer de l'améliorer ?**
  - Mettre en place une procédure de révision périodique de l'homologation et un plan d'action pour traiter les risques résiduels et les nouveaux risques qui apparaîtraient.

Déclinaison Etablissement

Pragmatisme et opportunité

- Première homologation sur le SI financier imposée par notre raccordement au service INFINOÉ (INformation FINancière des Organismes de l'État)
- Homologations suivantes des nouvelles briques du SI avant mise en production (imposé par le décret)
- En tâche de fond, homologations des SI préexistants par ordre de criticité

Accompagnement externe

- Méthodologique (process, documents, instances…)
- Accompagnement dans la première homologation…
  - … pour nous aider à acquérir l'autonomie nécessaire
- Recours au marché CAIH avec 2 prestataires (comparatif en cours)

UNIVERSITÉ LUMIÈRE LYON 2

Questions / Réponses

UNIVERSITÉ LUMIÈRE LYON 2