@ : Christine.andreck@gmail.com
Thomas.arino@hotmail.fr

MISE EN ROUTE D'UNE CONFORMITÉ CNIL DANS UN ÉTABLISSEMENT PUBLIC

Conférence présentée le 20 octobre 2015 à :
L'Observatoire de la Sécurité des Systèmes d'Information et des Réseaux de Toulouse

CHRISTINE ANDRECK & THOMAS ARINO / PARTENAIRE : RÉMY BLANCHARD

SOMMAIRE

INTRODUCTION : Rappel des textes applicables

INTRODUCTION : Contexte

- TDCP* de 21.300 étudiants /1.000 personnes (ens/personnel)
- Gestion 140 applications et 63 Bases de données
- 45.000 mails reçus/jour
- 700 postes de travail (hors salles de TP informatiques)
- 160 serveurs

*Traitement de Données à Caractère Personnel

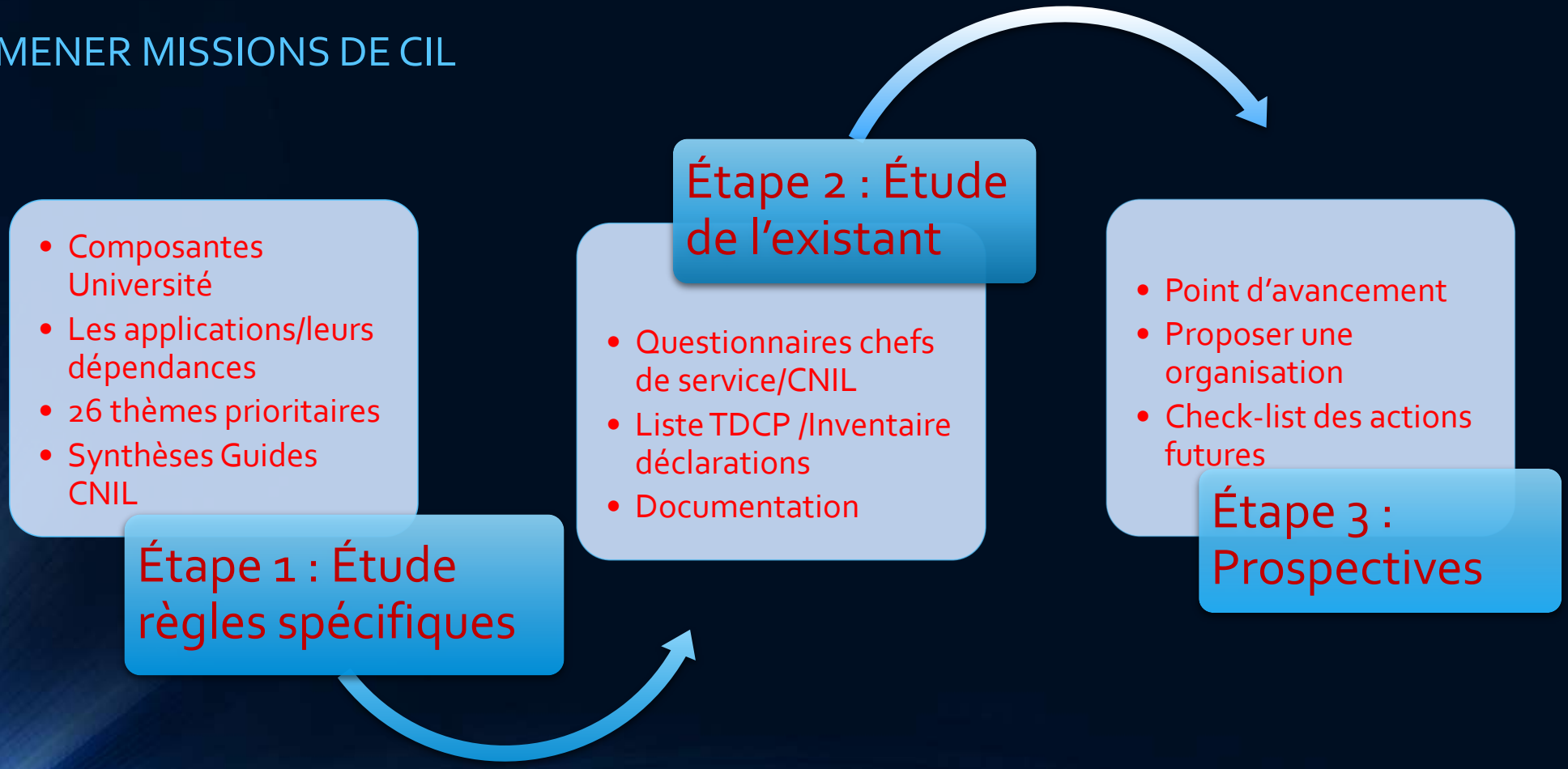
INTRODUCTION : Contexte (Suite)

LA DSI

- Missions : infrastructure / matériels / logiciels / services numériques
- Structure :
    1. Système
    2. Support
    3. Ingénierie

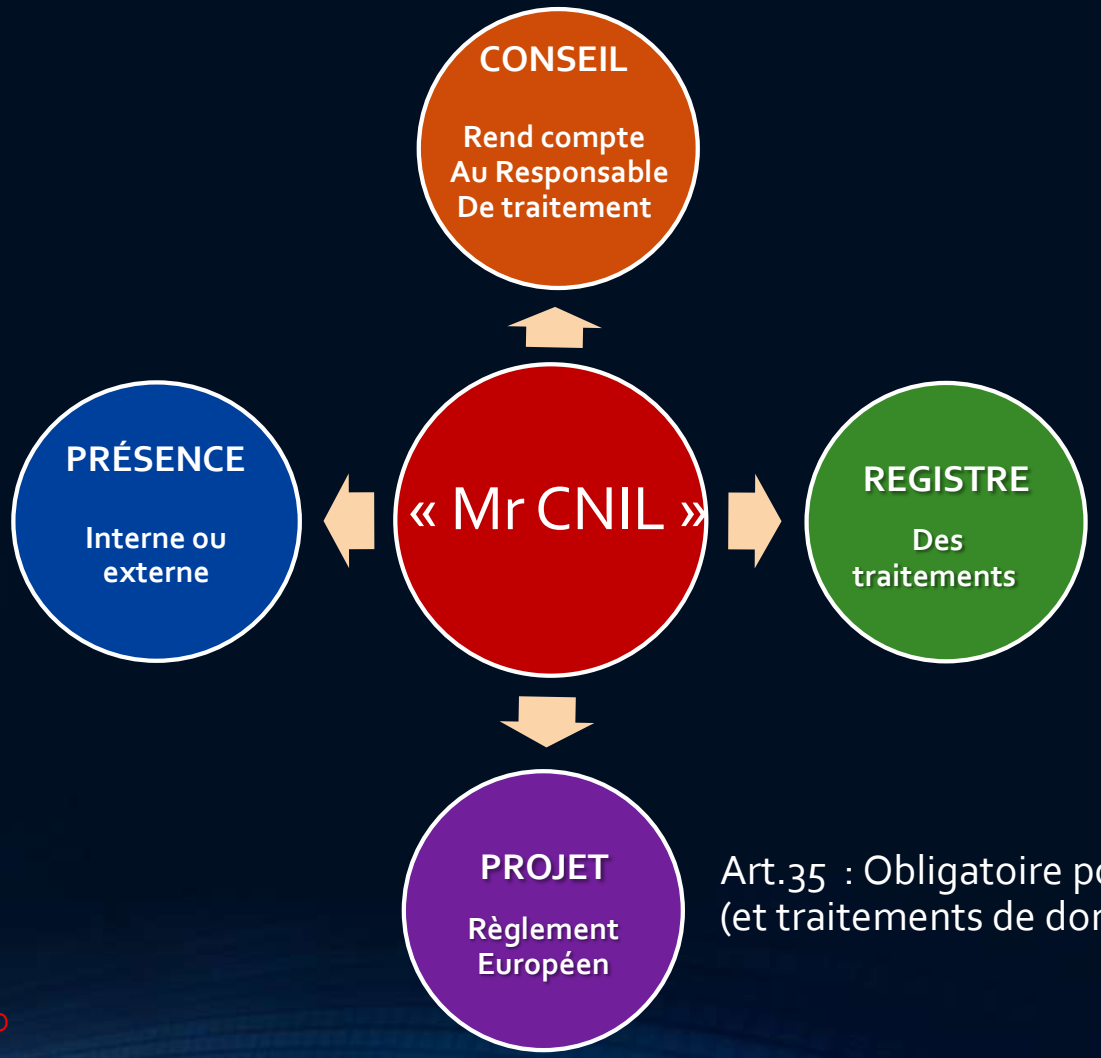
INTRODUCTION : Initialisation démarche

MENER MISSIONS DE CIL



INTRODUCTION : Le CIL

CORRESPONDANT INFORMATIQUE ET LIBERTES



Au-delà 50 personnes
Forcément interne à la structure

Il se substitue aux déclarations normales et simplifiées

Art.35 : Obligatoire pour organismes publics
(et traitements de données de + 5.000 Personnes)

INTRODUCTION :Risques de non-conformité

Sanctions CNIL

Avertissements

Sanctions pécuniaires (150K€ max ; x2 si récidive) ; limite : 5 % CA

Injonctions

Retrait de l'autorisation

Sanctions pénales

Art 226-16 -> 226-24 Code pénal

3 ans de prison + 100K€ (divulgation par imprudence/négligence…)

5 ans de prison + 300K€ (Non-respect principe de sécurité, communication tiers non-autorisés…)

Discrédit dans l'opinion

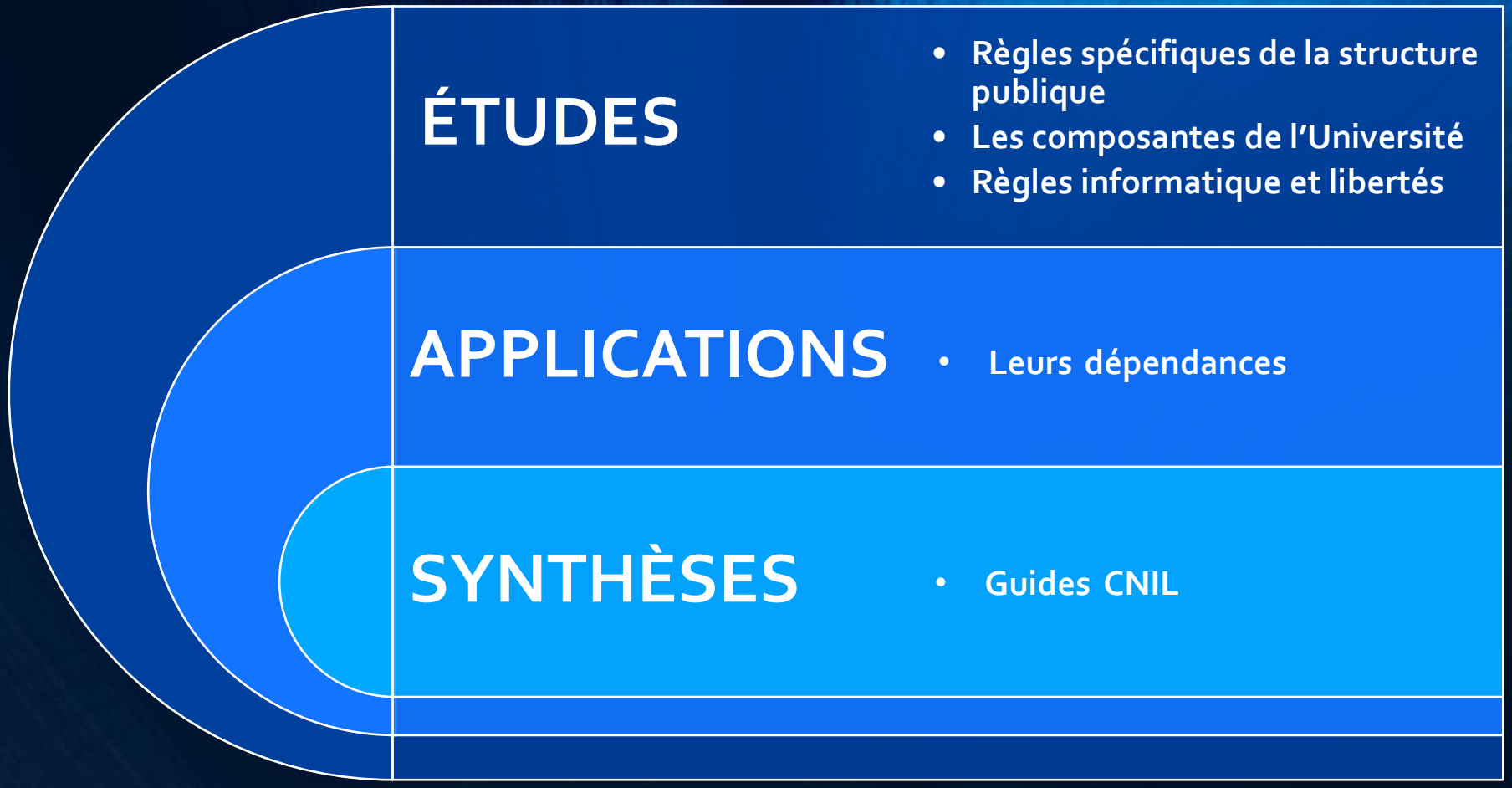
Publicité possible des sanctions

Image de marque impactée

Ex : sites de rencontre

DÉROULEMENT : Règles spécifiques à la structure

ÉTAPE PRELIMINAIRE



DÉROULEMENT : Étude de l'existant

2ème Étape

- Délimitation périmètre de travail
- Analyse de documentation juridique
- Questionnaires des différents acteurs
- Cartographie des TDCP
- Inventaire des déclarations

DÉROULEMENT : Exemple des données dématérialisées

ÉTAT DES LIEUX

- Archivage numérique
- Sauvegarde numérique
- Protection à distance des données

RECOMMANDATIONS

- MDP
- Mise à jour
- Code NAS BU
- Alarmes
- Réduire les personnes autorisées
- Historique

DÉROULEMENT : Exemple de la Charte Informatique

ÉTAT DES LIEUX

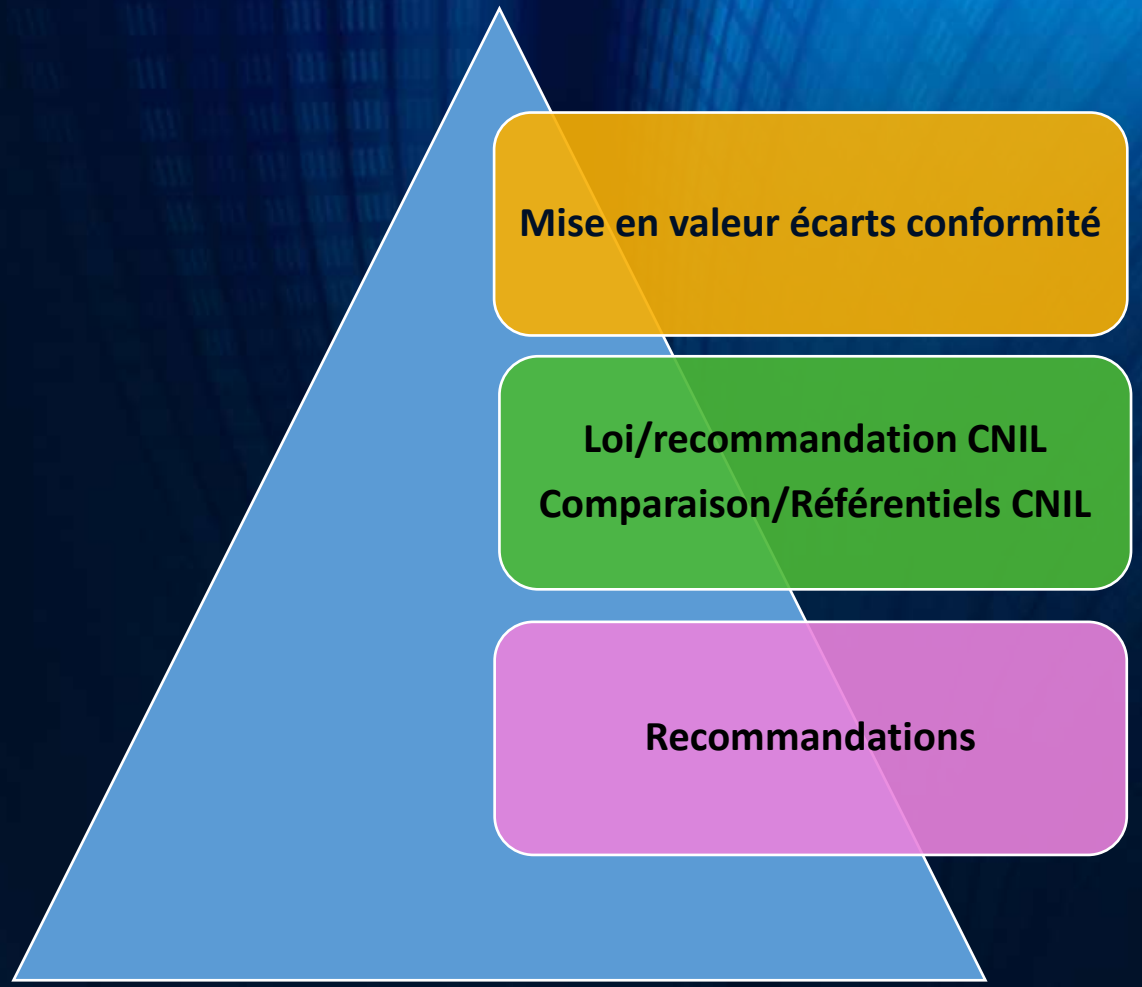
- Information indiv/collective utilisateurs :
  - Des traitements de leurs données
  - Du contrôle & Utilisation outils informatiques
- Charte OBLIGATOIRE si collecte données par le SI

RECOMMANDATIONS

- Opposabilité : Si annexée au Règlement intérieur
- Définition usage professionnel/privé résiduel
- Ne peut interdire usage raisonnable d'internet
- Rappel principe confidentialité Administrateur réseau
- Livret procédures (bonnes pratiques)

DÉROULEMENT : Bilan

3ème Étape



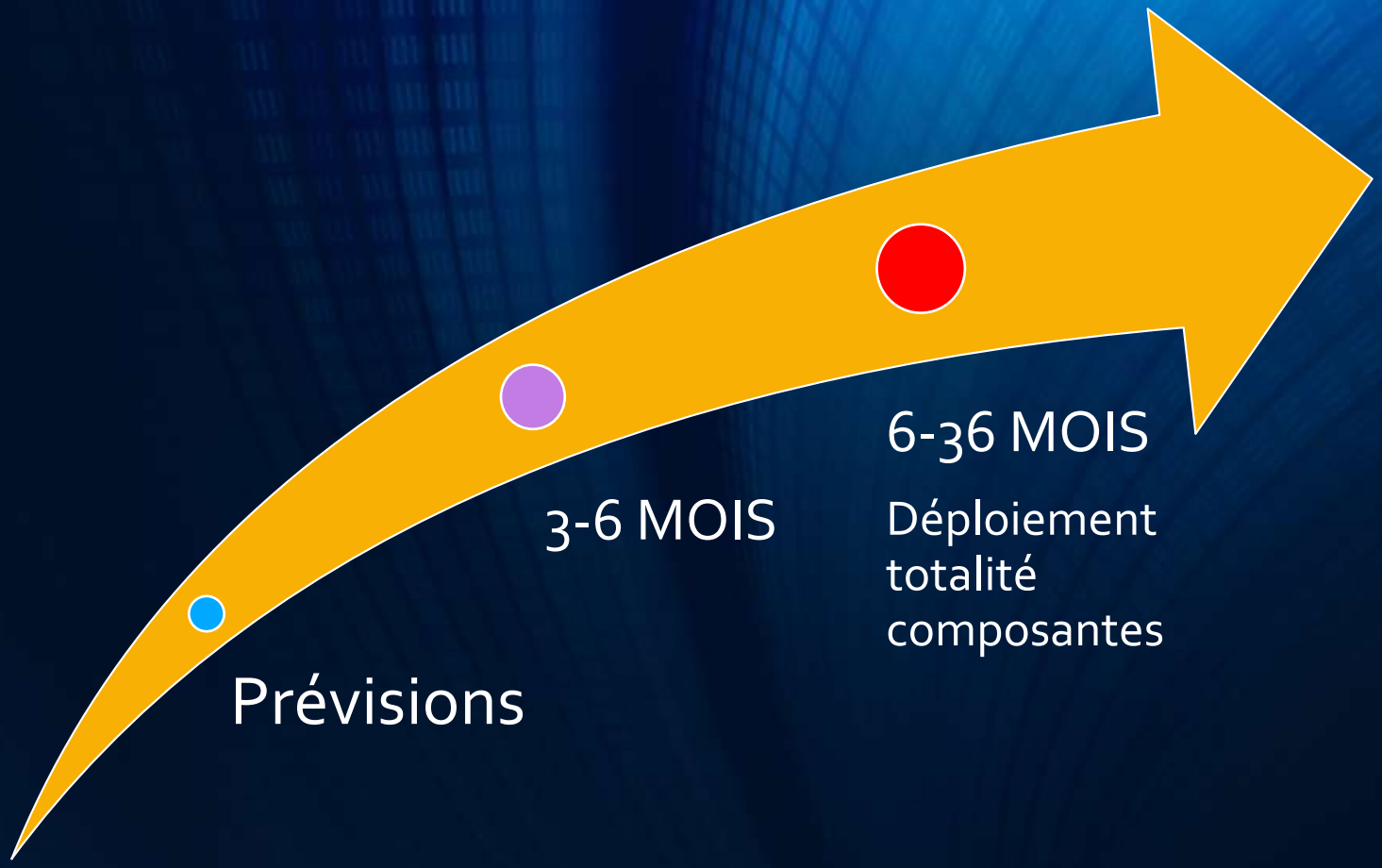
DÉROULEMENT : Bilan (Suite)

4ème Étape

- Conformité relative aux déclarations CNIL les plus structurantes pour l'Université
- Initialisation :
  - d'une architecture de documentation juridique
  - d'une organisation

PRIORITÉS PRÉVISIONNELLES

RECOMMANDATIONS



PRIORITÉS PRÉVISIONNELLES

RECOMMANDATIONS

Délai	
3-6 mois	Préparer la nomination d'un CIL
	Compléter la liste des Traitements de Données à caractère personnel (TDCP) + Formalités correspondantes
	Audits particuliers (Sécurité, sous-traitance, transferts DCP en dehors UE, hébergement externe)
	Création d'une page Web « Ma-CNIL »

PRIORITÉS PRÉVISIONNELLES

RECOMMANDATIONS

Délai	Bâtir une organisation interne
6-36 mois	Déploiement sur la totalité des composantes de l'Université
	Permettant la centralisation effective des procédures

CONCLUSION

URGENT

Anticipation du projet de Règlement européen pour les Responsables de traitement

PREPARER

Une organisation interne Informatique et Libertés

Nomination d'un CIL bientôt obligatoire pour tous les organismes publics

CONCLUSION

MERCI DE VOTRE ATTENTION

DES QUESTIONS ?