jres
Montpellier 2015

Mise en place d'une Gouvernance Informatique et Libertés

Un retour d'expérience

amue
MUTUALISATION + SOLUTIONS

LA GOUVERNANCE

I. Contexte

II. Promesses du référentiel de la CNIL

III. Expérimentation

IV. Résultats

V. L'essentiel

I. LE CONTEXTE GÉNÉRAL DE LA GOUVERNANCE

« Les grandes personnes sont décidément très très bizarres »

I. LE CONTEXTE GÉNÉRAL DE LA GOUVERNANCE

+ Gestion de l'urgence et pas assez de recul pour la gouvernance
+ Formalités déclaratives de façade, contrôle a priori inefficace voire inexistant
+ Législation hésitante et changeante
+ Prochain règlement européen (adoption début 2016 et délai d'application 2 ans) :
  - Plus de contraintes, plus de preuves à fournir, sanctions plus lourdes…
+ Nécessité de préparer la transition
+ Pas de socle solide pour la gouvernance *Informatique et Libertés*
+ Pas de fil conducteur (malgré beaucoup de textes de loi et de paramètres à prendre en compte)
+ Pas de méthodologie
+ Pas d'appui au sommet de la hiérarchie

II. LES PROMESSES DU RÉFÉRENTIEL

« Mais si tu viens n'importe quand, je ne saurai jamais à quelle heure m'habiller le cœur… Il faut des rites »

LE RÉFÉRENTIEL, PRODUIT FINI OU MATIÈRE PREMIÈRE ?

+ Le référentiel de la CNIL compte vingt-cinq exigences
+ Il couvre trois thématiques :
  - Organisation
  - Mise en conformité
  - Réclamations et incidents.
+ C'est une réponse anticipée à l'imminence du prochain règlement européen
  - Oui… mais trop compliquée (en l'état) : Trop dense et livré sans mode d'emploi
+ Nécessité de compléments méthodologiques…

LES INTERROGATIONS LIÉES À LA GOUVERNANCE

Le RT

+ Garantie juridique ?
+ Objectifs abordables ?
+ Gains bancables ?
+ « Où en sommes-nous ? »

Le CIL

+ Organisation à conseiller ?
+ Méthodologie de mise en conformité ?
+ Circuit d'exercice des droits ?

Autres interrogations (en résumé)

+ Où allons-nous ?
+ Qu'est-ce qu'on peut faire ?

III. L'EXPÉRIMENTATION

« Si tu veux un ami, apprivoise-moi ! »

III. EXPÉRIMENTATION – LE CAHIER DES CHARGES

+ Vision globale
+ Indicateurs simples et pertinents
+ Traçabilité et adhésion à la démarche
+ Efficience
+ Couverture totale de la problématique

III. EXPÉRIMENTATION – RECHERCHE D'UNE RÉPONSE

+ Démarche basée sur l'identification et le décompte des conditions et résultats élémentaires à cumuler pour remplir les exigences du référentiel (les items)

+ En quoi cette démarche répond-t-elle à notre cahier des charges ?

AU COMMENCEMENT ÉTAIENT LES EXIGENCES DU LABEL…

+ Choix d'opérabilité : subdiviser les exigences en items

Exigence	Items	Nb
EOR01	Politique de protection interne formalisée	1
	Politique interne	
EOR02	Politique de protection externe formalisée	2
	Politique externe – Qualité Information	
EOR03	Politiques de protection validées par le CIL et diffusées	3
	A décliner en interne et à l'externe : Validation – Diffusion – Révision/Périodicité (au minimum tous les 3 ans)	
		6

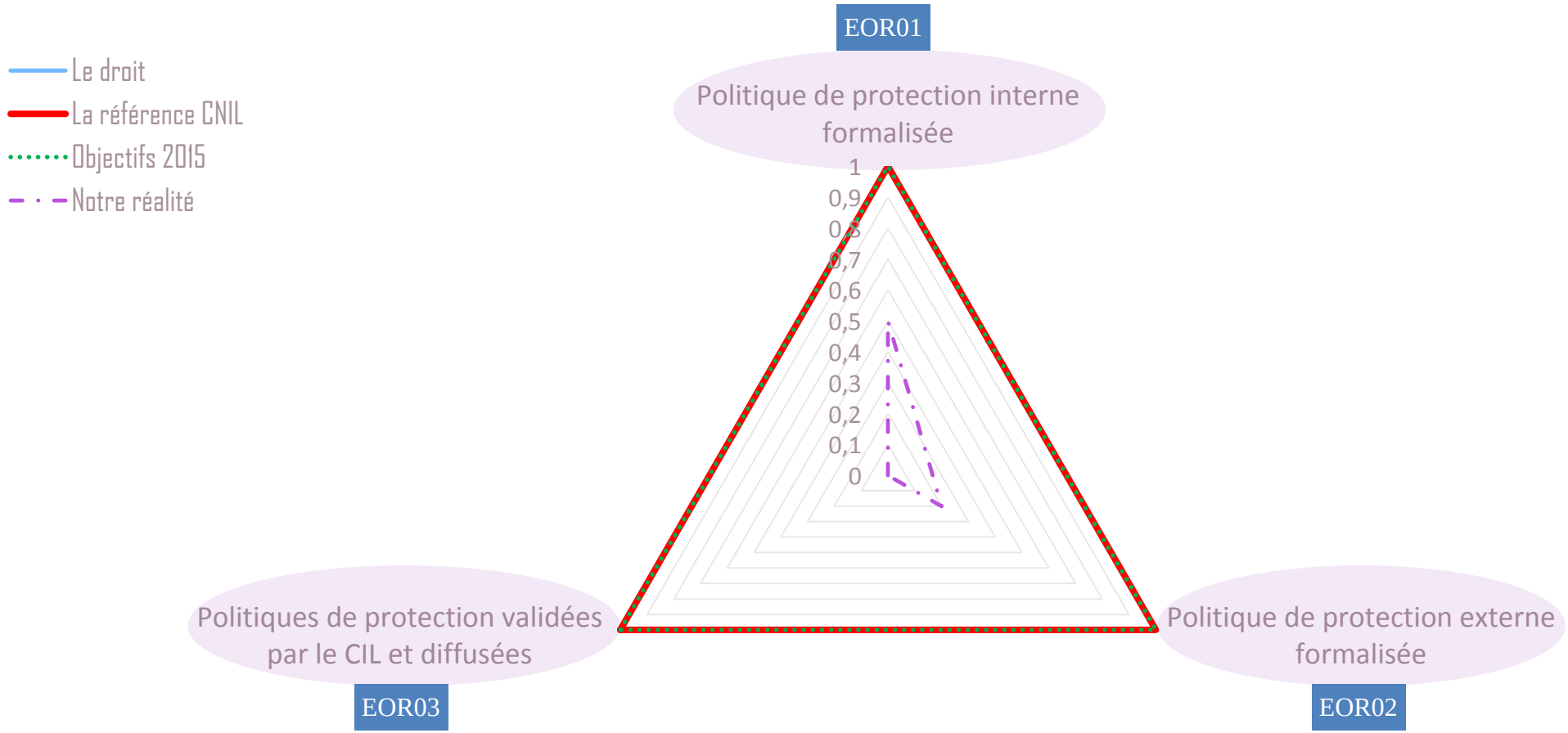
AUTRE EXEMPLE DE DÉCOMPTE D'ITEMS

Exigence	Items	Nb
EM01	Analyse de conformité juridique effectuée par le CIL	10
	A décliner par traitement (à l'amont) Finalité du traitement – Proportionnalité du traitement – Accès aux données – Pertinence des données (au regard de la finalité) – Durée de conservation – Nombre de destinataires – Encadrement sous-traitance – Information claire et préalable – Transfert hors UE – Auteur de l'analyse	
EM02	Plan d'actions préventives et correctives proposé par le CIL	3
	A décliner par traitement (à l'amont) Recommandations – Plan d'actions préventives – Plan d'actions correctives	
		13

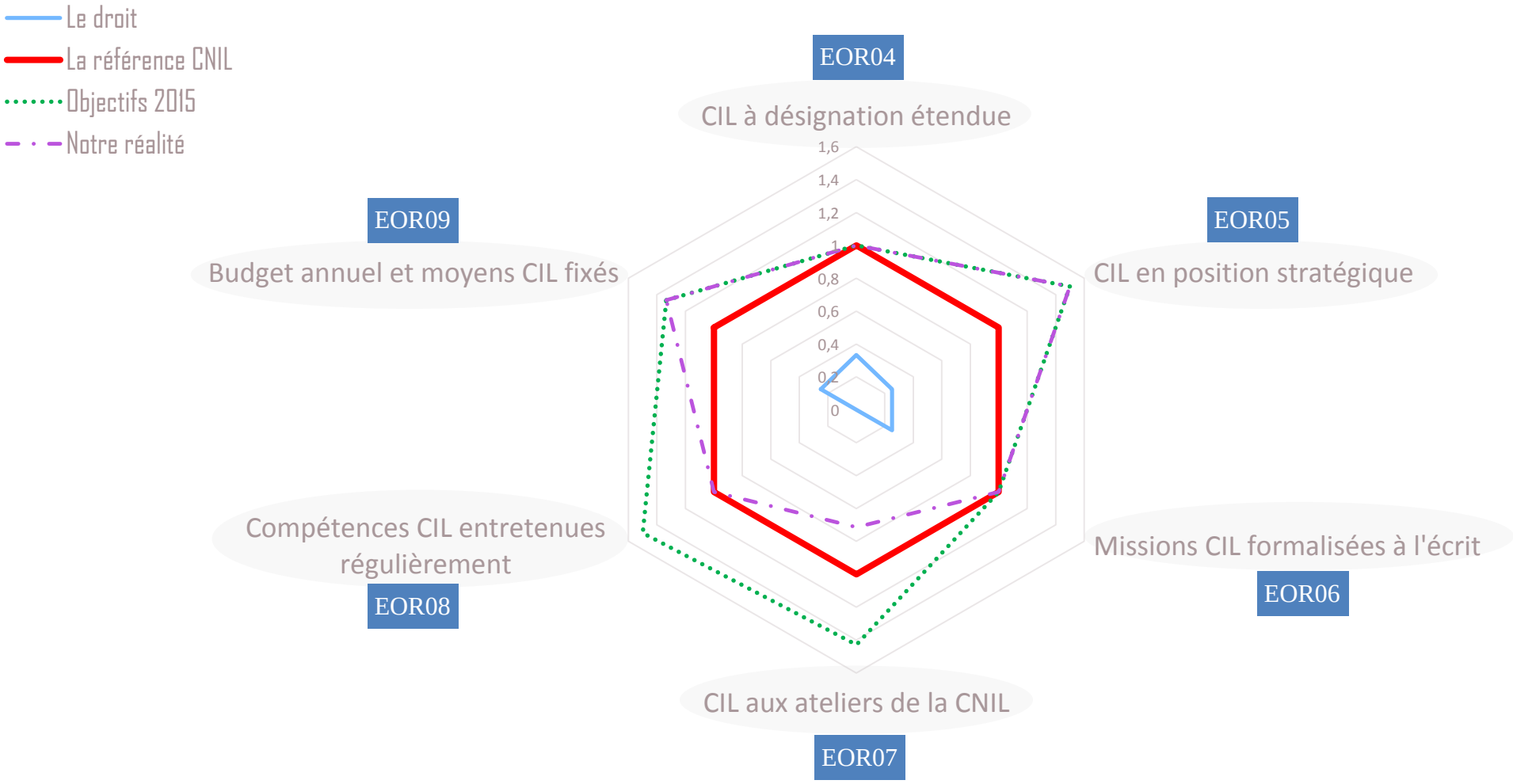
III. EXPÉRIMENTATION – A QUOI SERVENT LES ITEMS ?

- Base de comparaison (contraintes légales *vs* exigences du label)
- Guides au plan opérationnel
- Représentation graphique des exigences et des objectifs
- Représentation de l'avancement des procédures et processus « Informatique et Libertés »

III. EXPÉRIMENTATION - POLITIQUES



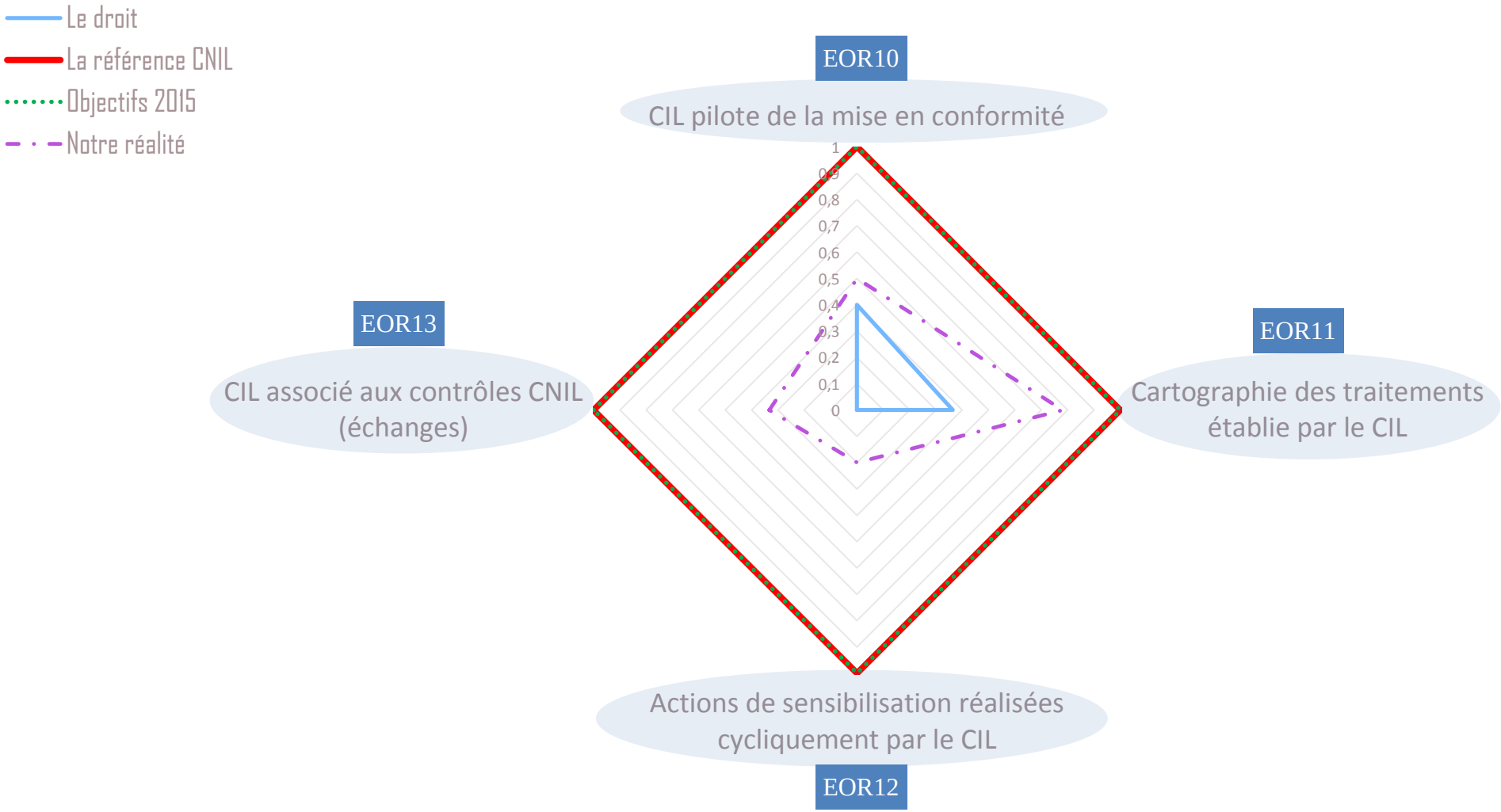
III. EXPÉRIMENTATION - LE CIL



III. EXPÉRIMENTATION – LA GESTION DES ITEMS

- Saisie des items du référentiel
- Saisie des abscisses sommitales *du radar du droit*
- Radar des objectifs : définition à partir des items du référentiel en cochant ceux que l'on souhaite soi-même s'imposer
- Validation des items
- Calcul des nouvelles valeurs des abscisses du radar de réalité

III. EXPÉRIMENTATION – PILOTAGE



UNE VIDÉO DE SENSIBILISATION…

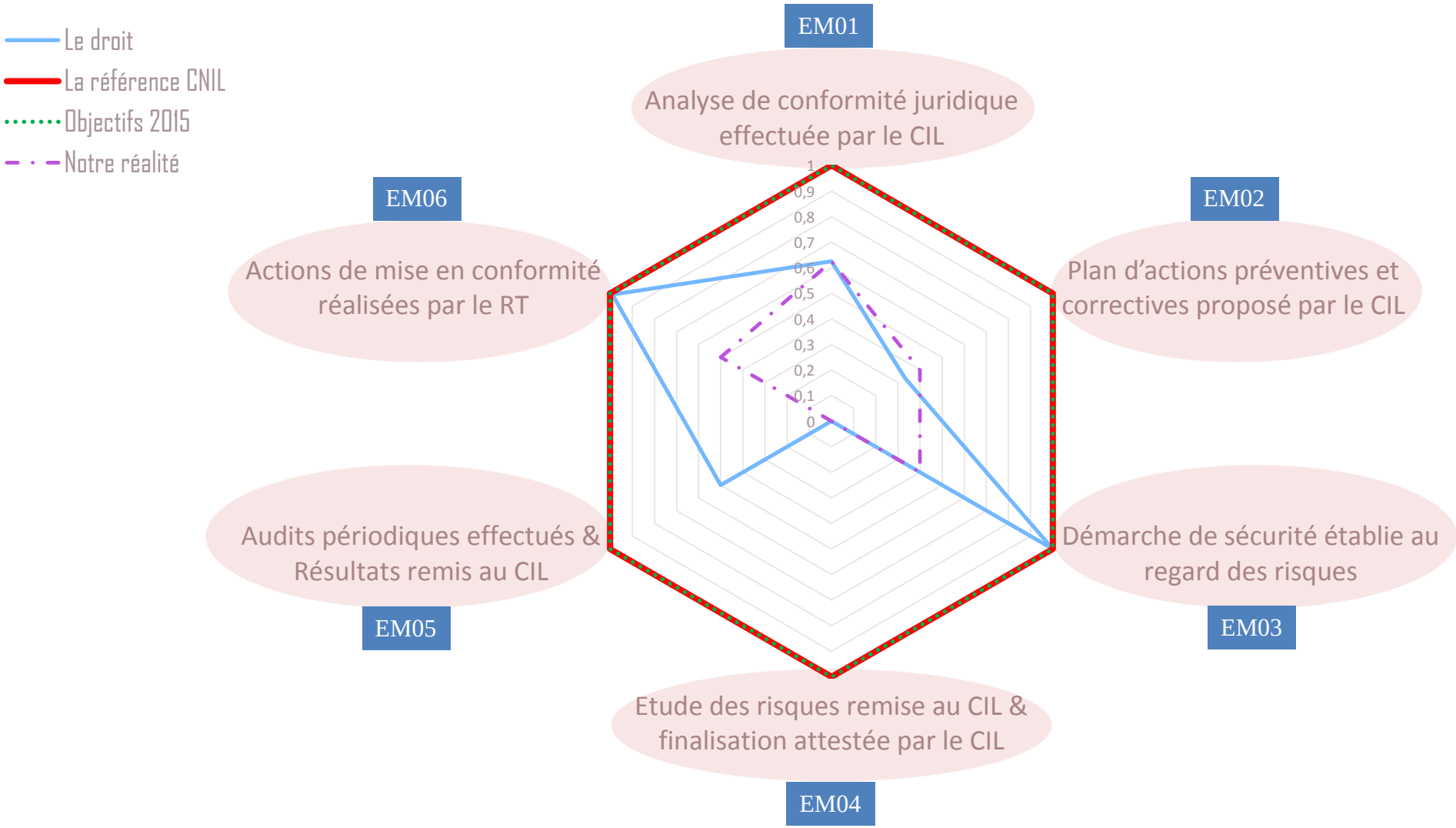
MAIS NE DEVRAIT-ON PAS TENDRE À RENDRE CETTE SITUATION IMPOSSIBLE ?

- Dans nos établissements, il pourrait se poser bien des questions. Par exemple, y a t-il :
  - Garantie de gestion des protocoles « sécurisés » ?
  - Effectivité de la restriction des accès ?

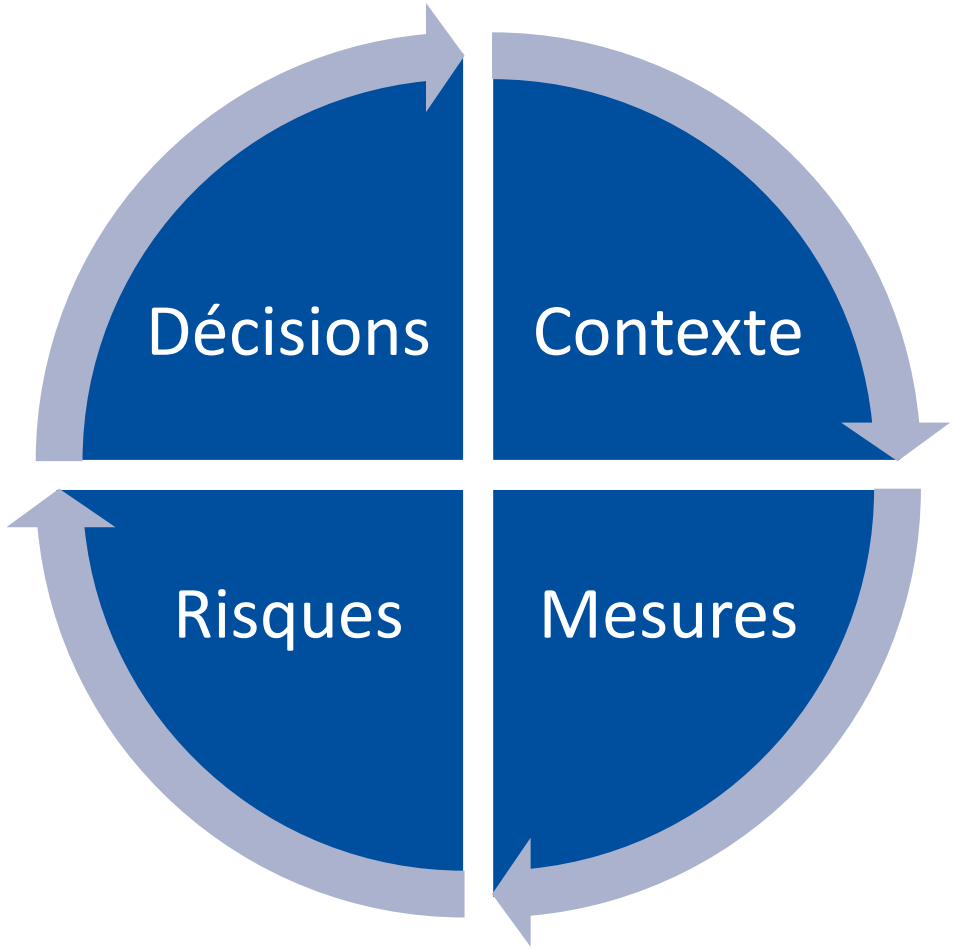
- Les administrateurs systèmes ont-ils vraiment besoin d'accéder à toutes les données à caractère personnel pour gérer leurs systèmes ?

- CIL et RSSI, même combat…

III. EXPÉRIMENTATION – CONFORMITÉ



III. EXPÉRIMENTATION – UNE EIVP/PIA ?



III. EXPÉRIMENTATION – PIA ET *PRIVACY BY DESIGN*

PIA vs Privacy by design :

+ Logiciels conformes à la livraison ;
+ Pas de rupture de la « chaîne de conformité » en phase d'exploitation
+ Respect du principe de Privacy by default/design tout au long du cycle de vie des logiciels

PIA ET *PRIVACY BY DESIGN* – RETOMBÉES DU LABEL POUR LES ADHÉRENTS

Respect du principe de Privacy by default/design par exemple :

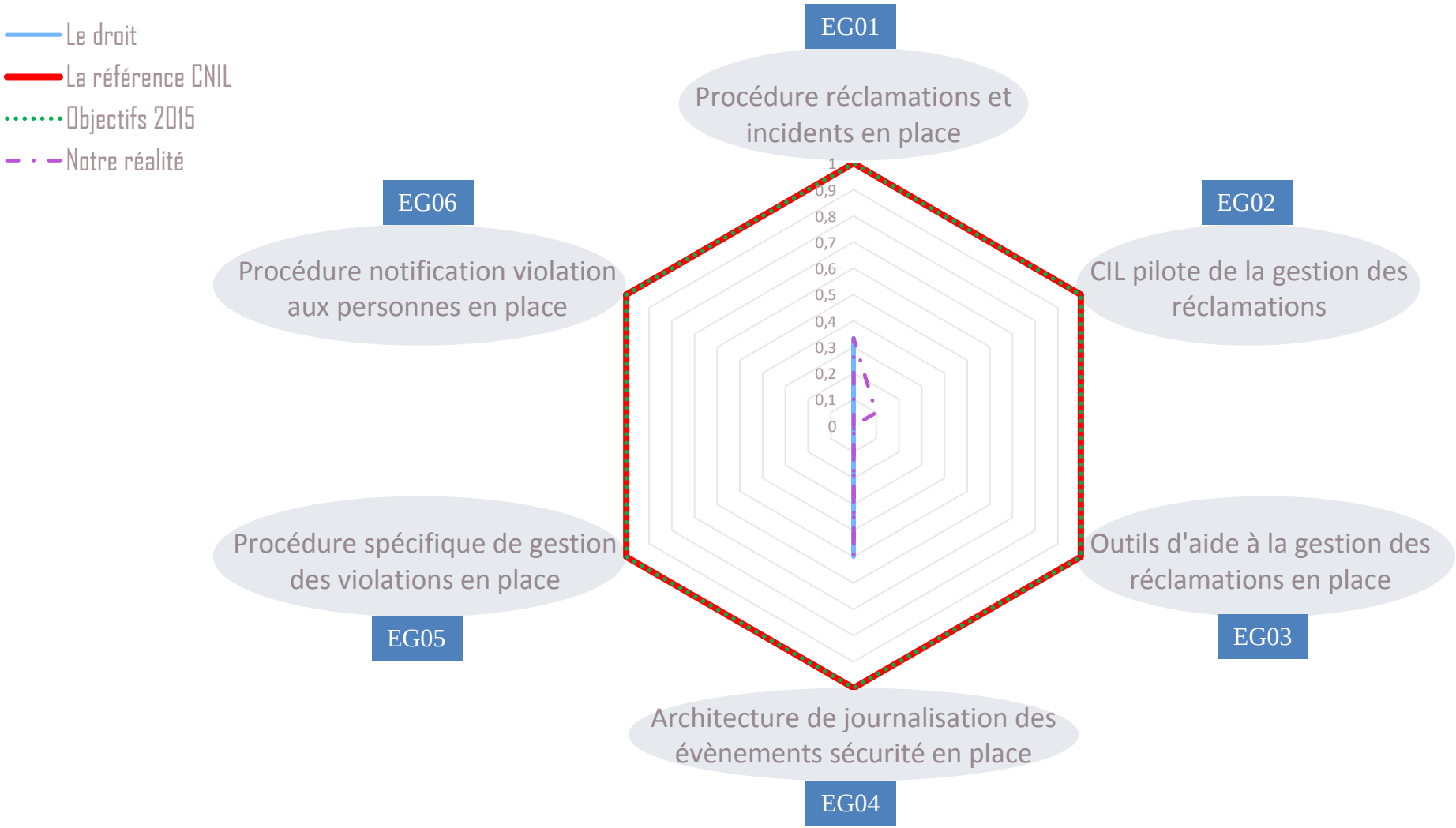
+ pour gérer la problématique des durées de conservation
+ pour mieux prendre en compte l'exercice des droits des personnes :
  - dispositifs de création de liens vers les politiques de protection
  - Droit d'accès
+ avec paramétrage par défaut déjà conforme au droit
+ en protégeant les « contenus » aussi bien que les contenants.

III. EXPÉRIMENTATION – PIA ET *PRIVACY BY DESIGN* – RETOMBÉES DU LABEL POUR LES ADHÉRENTS

Retombées positives planifiées via :

+ Dispositif d'assurance qualité de l'Amue
+ Capitalisation de l'analyse des régimes juridiques applicables et partage sur l'extranet de l'Amue
+ Accompagnement des établissements dans leur démarche de gouvernance Informatique et Libertés (en lien avec la CPU)
+ Mise à jour régulière du Guide I&L ESR (Amue, CNIL, CPU).

III. EXPÉRIMENTATION – RÉCLAMATIONS ET INCIDENTS



IV. LES RÉSULTATS – LA VISION GLOBALE

« Vu d’un peu loin ça faisait un effet splendide »

IV. LES RÉSULTATS – A QUOI SERT L'INDICATEUR ?

+ Roadmap complète
+ Politique de protection de l'établissement par rapport au référentiel
+ Actions obligatoires réalisées ou à réaliser
+ Chemin parcouru
+ Reste à faire par rapport aux objectifs fixés
+ Rehaussements d'objectifs
+ Amélioration continue

+ EIVP/PIA à effectuer
+ Prochains cycles

IV. LES RÉSULTATS – CARACTÉRISTIQUES DE L'INDICATEUR

+ Sensible :
  - aux variations du référentiel
  - aux changements de cadre normatif, législatif ou règlementaire
+ *Zoomable*
+ Modulable
+ Protéiforme
  - Graphique ou tableau
  - Topologique ou pondéré
+ Généralisable

CONCLUSION

+ Nécessité de préparer la transition vers le règlement européen :
  - Exigences du label - Réponse anticipée
  - Opportunité de mutualiser
  - Possibilité d'outiller la démarche en mode SaaS
  - Exploration d'autres démarches, d'autres outils…

CONCLUSION

Quatre vecteurs suffisent à répondre aux interrogations sur :

+ la situation d'un établissement vis-à-vis du droit et par rapport à ses objectifs I&L;
+ sa capacité à anticiper les changements s'annonçant au niveau européen.

Quatre vecteurs suffisent... Il reste à les décliner en :

+ politiques de protection
+ compétences et moyens de pilotage
+ conformité et respect des principes et droits fondamentaux des personnes.

CONCLUSION

+ **Pour la constitution du dossier de demande de label :**

  Meilleure structuration de l'affectation de moyens et du recueil des preuves

+ **Au plan opérationnel :**

  Transformation du référentiel en fil conducteur et véritable levier opérationnel

  Démarche mesurable

  Couverture totale de la problématique

+ **Pour la communication et la sensibilisation des acteurs :**

  Vision permanente et globale de l'essentiel de la gouvernance.

V. L’ESSENTIEL

« L’essentiel est invisible pour les yeux… »

VI. L'ESSENTIEL

+Le temps

+Les liens

+La confiance

+Le bien-être numérique

Merci de votre attention

Contact

frantz.gourdet@amue.fr