PIA : Pourquoi l'ISO 29 134 ?

ISO 29134 // ISO 27 005

Amélie PAGET
Consultante Juridique
apaget@deloitte.fr

HSC by Deloitte.

Privacy Impact Assessment

Privacy Impact Assessement

DPIA

Appréciation des risques sur la vie privée

PIA

Data Privacy Impact Assessement

EIVP

Etude d'impacts sur la vie privée

Analyse d'impact relative à la protection des données

Privacy Impact Assessment

- Obligation de sécurité des données à caractère personnel
  - Art. 34 loi dite « informatique et libertés »
  - Guide CNIL : Sécurité des données personnelles
- Projet de GDPR (Règlement général sur la protection des données)
- Nouveaux Guides CNIL dédiés à l'EIVP
- GDPR du 27 avril 2016
  - Entré en vigueur le 24 mai 2016
  - Application effective le 25 mai 2018

→ Les formalités préalables disparaissent, le PIA s'impose (art. 35 GDPR)

La norme ISO 29 134

- ISO 29 100

Technologies de l'information – Techniques de sécurité – Cadre privé

- ISO 29 134

Information technology -- Security techniques -- Privacy impact assessment -- Guidelines

- *Draft* : Etape d'approbation
- Objectifs de publication : 30 mai 2017

La norme ISO 29 134

Le PIA dans la norme ISO 29134

- Définition (3.7)

Ensemble du processus d'identification, d'analyse, d'évaluation, consultation, communication et planification des traitements de impacts potentiels sur la vie privée au regard des traitements de données à caractère personnel, dans le cadre d'un système de management plus large.

- Objectifs (5.1 et 5.2)
  - Identifier et évaluer les risques sur la vie privée des personnes concernées
  - Fournir les éléments d'entrée pour construire la protection des données
  - S'assurer de la conformité d'un projet
  - Démontrer sa conformité
  - Renforcer la confiance des partenaires, clients et personnes concernées

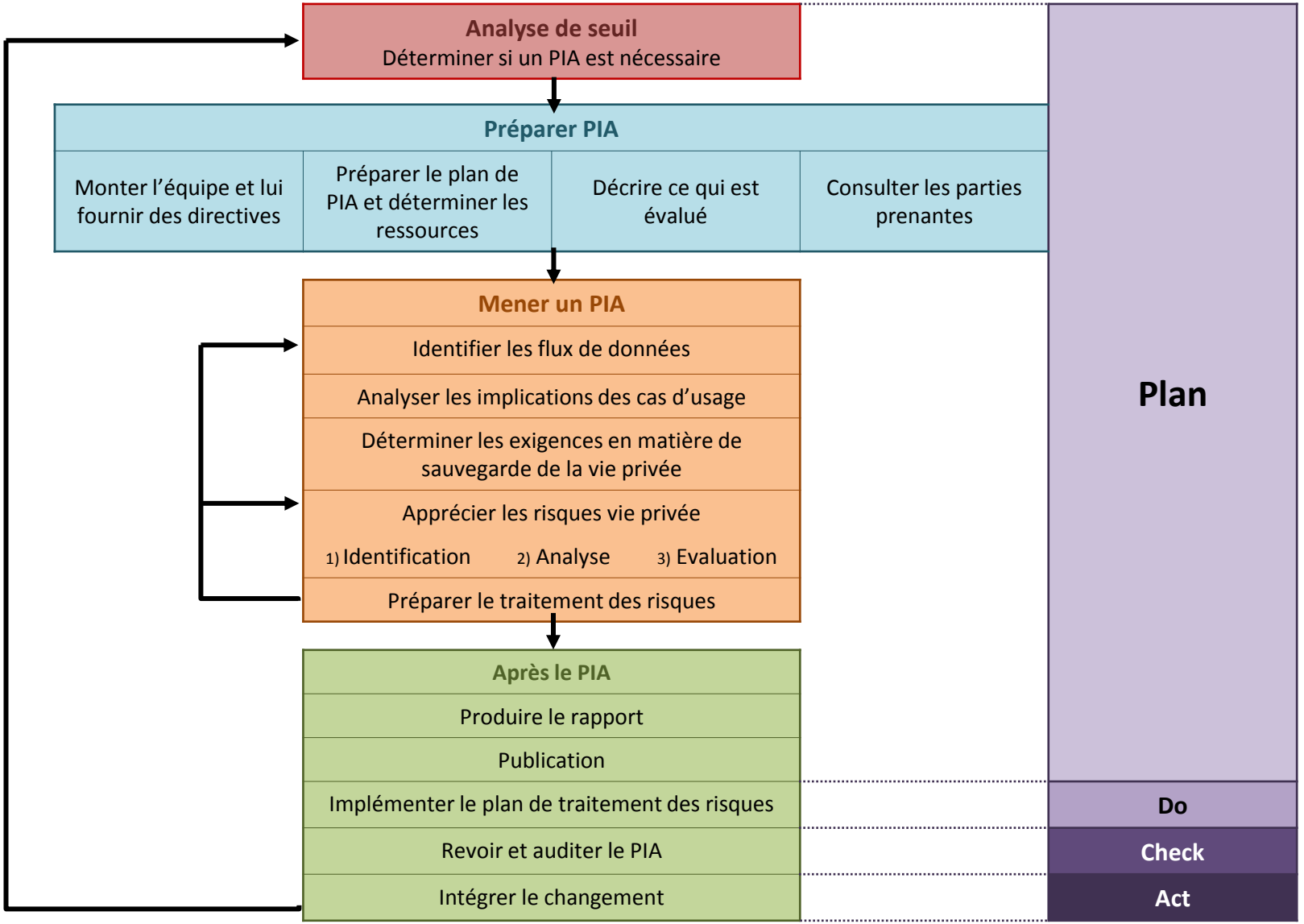
La norme ISO 29 134

Points forts	Points faibles
Inclut une phase d'étude préalable au PIA Invite à adapter le niveau de granularité du PIA Présente un processus Définit le contenu d'un rapport de PIA Reprend les grandes lignes de l'appréciation des risques ISO 27 005 S'intègre à un système de management plus global Peut s'adapter aux exigences légales	Confusions de termes Incohérences de phases Processus décousus

Structure de la norme

1. Périmètre
2. Références normatives
3. Définitions
4. Abréviations
5. **Préparer le terrain**
   - Bénéfices apportés par un PIA
   - Les objectifs du rapport de PIA
   - L'organisation du PIA
   - Le niveau de granularité du PIA
6. Recommandations pour conduire un PIA
   - Les étapes du processus
     - Objectifs
     - Eléments d'entrée
     - Eléments de sortie
     - Les actions
       - **Précise ce qui devra intégrer le rapport de PIA**
     - Les préconisations de mise en œuvre
7. **Le rapport**
8. Les annexes
   - Critères de gravité et de vraisemblance
   - Menaces génériques
   - Présentation de termes
   - Exemples d'illustration

Le processus dans la norme



Les points faibles du processus

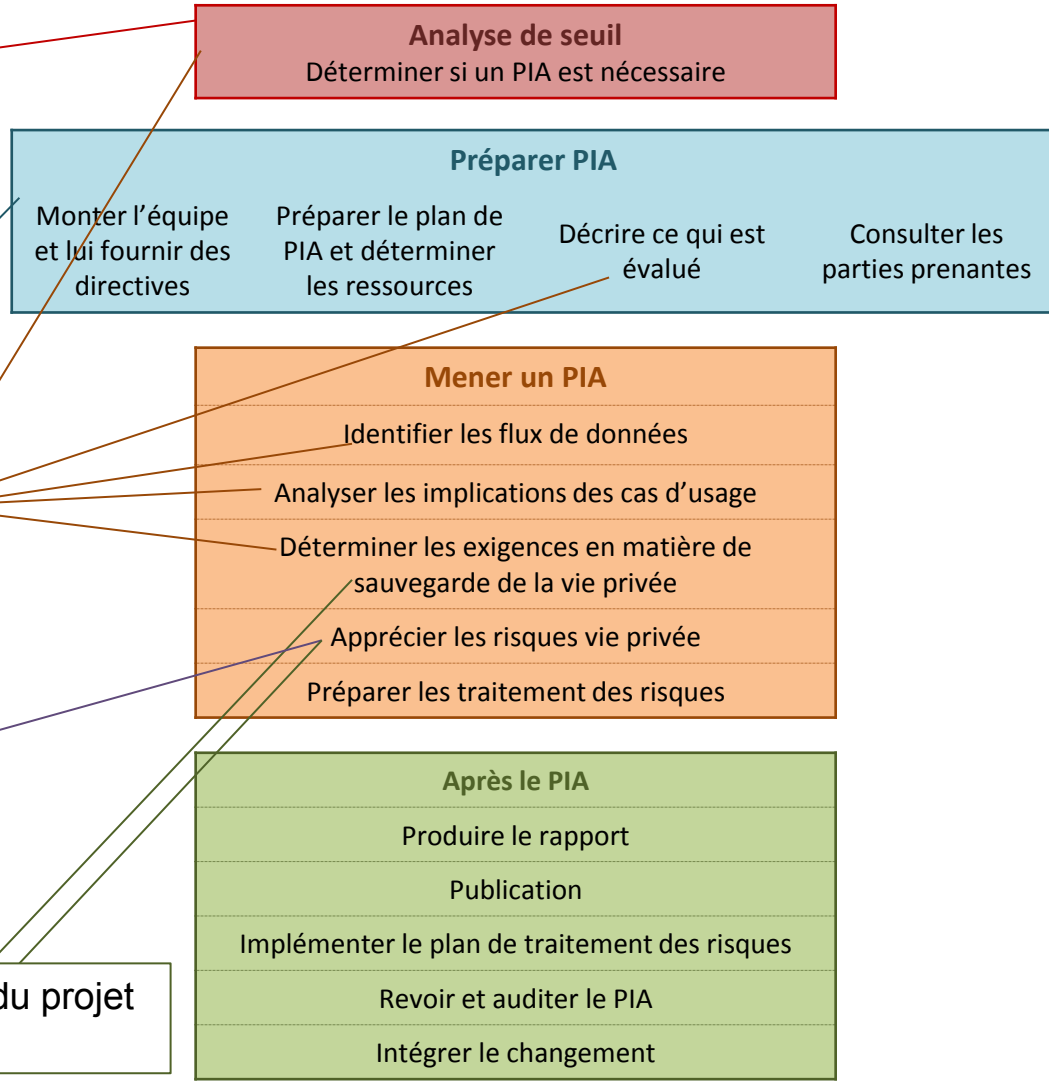
Imprécise dans son déroulement et ses critères
Inclut la définition du périmètre et des termes de référence

Le titre ne correspond pas à ce qui y est développé : les critères d'évaluation des risques
Les objectifs sont incohérents

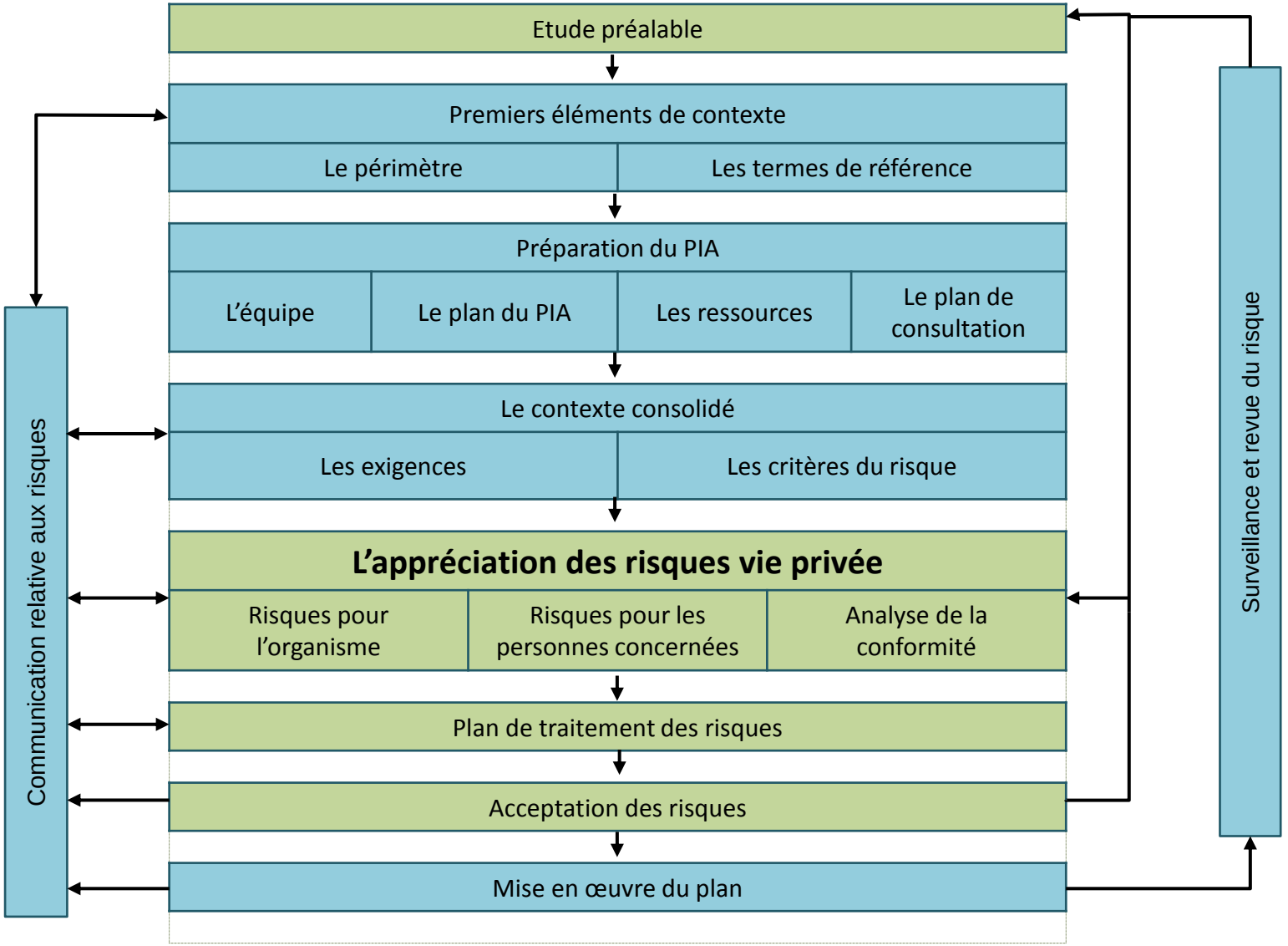
La description de l'ensemble du contexte est décousue

Confusion entre les risques supportées par les personnes concernées et ceux supportés par l'organisme
Les spécificités des critères d'acceptation du risque ne sont pas clairement présentées

Inclut également l'étude de la conformité du projet
Mais l'appréciation des risques aussi



Reconstruction du PIA



Les acteurs du PIA

L'assesseur

- Il dirige le PIA
- Il est lié à la personne en charge de la protection des données personnelles ou, à défaut, avec le chef du projet

La personne responsable de la conduite du PIA

- Elle est nommée par la Direction
- Elle conduit elle PIA

La Direction

- Elle approuve et prend les décisions
- Elle apporte son soutien au PIA

La personne qui approuve et signe le rapport

- Elle est nommée par la Direction

Les membres de l'équipe du PIA

- L'équipe peut être interne ou externe
- L'assesseur peut être soutenu par un représentant des Département métiers, IT et Juridique
- Un **expert juridique** pour mener l'analyse de conformité

Les parties prenantes

- Les prestataires externes, les partenaires et clients, les **personnes concernées**
- Elles sont consultées dans le cadre de l'appréciation des risques
- Le rapport de PIA (ou une synthèse publique) leur est communiqué

1 - Etude préalable (Analyse de seuil) (6.2)

Objectif : Déterminer si un PIA est nécessaire

Acteurs :

- Réalisé par les Direction, en coopération avec l'Assesseur
- La Direction prend la décision finale

Critères proposés par la norme

- Nouvelle technologie, nouveau service ou autre projet innovant impliquant un traitement de données personnelles ;
- Décision de traiter des données sensibles ;
- Evolution de la législation et de la réglementation en matière de vie privée, d'une politique et de standards internes, de SI, de finalités et de moyens pour traiter les données, nouveaux ou évolution de flux de données, etc.;
- Extension ou acquisitions d'activités.

Eléments de sortie : Résultats de l'étude et le mandat

Dans le GDPR

- Etude préalable
- Des critères supplémentaires : volume de données, le nombre de personnes concernées, la surveillance de zone accessible au public, le profilage, une prise de décisions produisant des effets juridiques

2 – Premiers éléments du contexte (6.2)

Actions : Si un PIA est décidé :

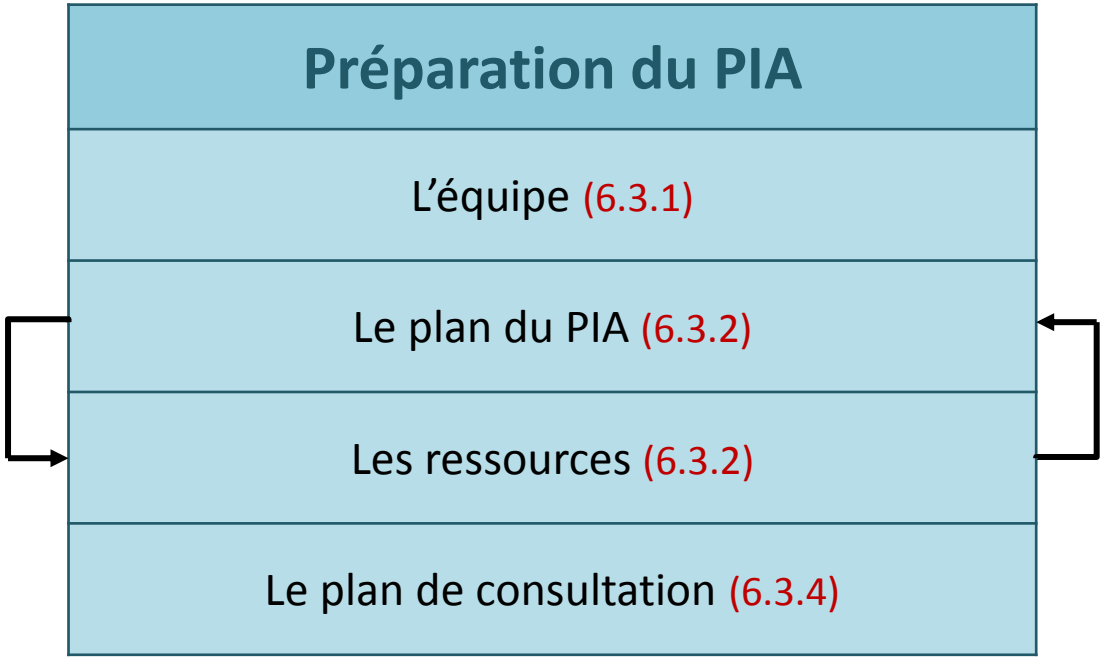
- Déterminer les limites et le domaine d'application du PIA
- Décider et documenter le niveau de granularité du PIA (5.4), les process utilisés, les cibles d'audit, la nature et le contenu du rapport de PIA

Acteurs : Réalisé par la Direction, en coopération avec l'Assesseur

Eléments de sortie

- Périmètre du PIA
- Termes de référence

3 – Préparation du PIA



4 – Contexte

1. Identifier les exigences légales en matière de protection de la vie privée (6.4.3)
   - Acteur : support de l'expert juridique
   - La notion de vie privée est plus large que celle de protection des données personnelles
     - > Droit au respect de la vie privée
     - > Droit à l'image
     - > Secret des correspondances
     - > Protection des données personnelles
     - > Obligations « sectorielles » (ex. secret médical et la protection des données de santé)
   - Projets multinationaux
   - Outils : norme ISO 29 100

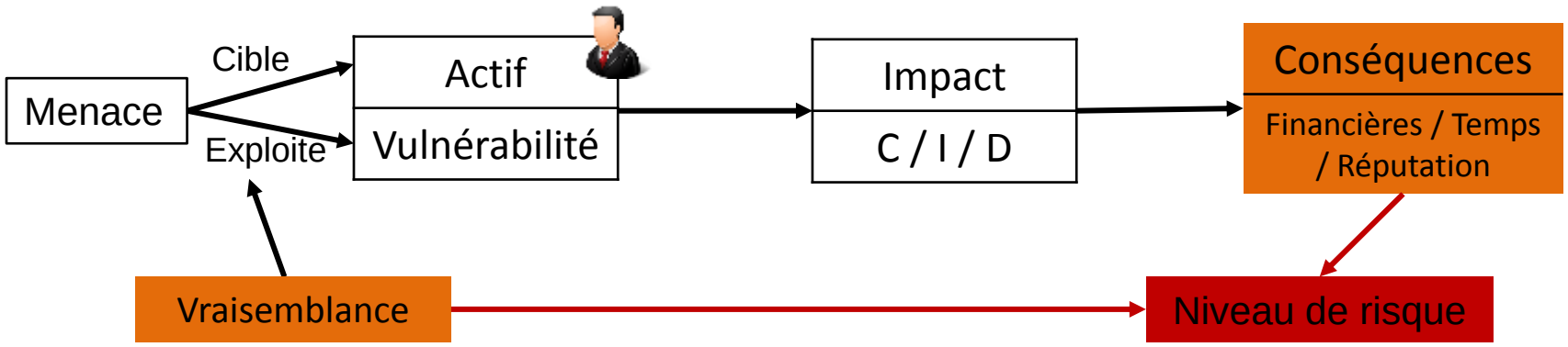
4 - Contexte

2. Définir les critères du risque

- 3 volets dans le PIA
  - Appréciation des risques pour l'organisme (6.3.1)
  - Appréciation des risques pour la personne concernée (6.3.1)
  - Analyse de la conformité (6.4.3)
- Critère du risque et d'acceptation du risque
- Définis par l'Assesseur, approuvés par la Direction

4 - Contexte

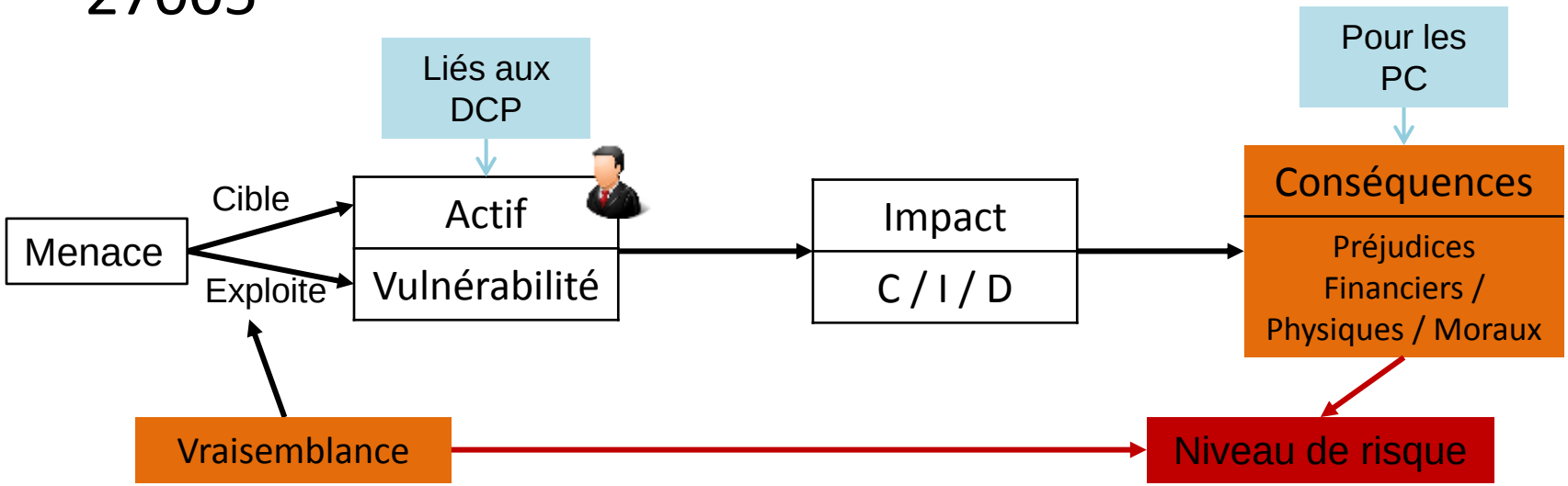
- Appréciation des risques pour l'organisme
  - Correspond à l'appréciation des risques (ISO 27 005)



- Ce volet n'est pas propre au PIA
  - Proposé par la norme ISO 29 134
  - Absent de la méthode CNIL
  - Absent du GDPR

4 - Contexte

- Risques vie privée pour les personnes concernées
- Mêmes composantes que le risque défini par l'ISO 27005



- Seule la cible change : les personnes concernées
  - Adaptation des critères et des valeurs des actifs, des impacts et des conséquences

4 - Contexte

Critères de valorisation des impacts (Annexe A)

Gravité basée sur la nature des données personnelles	Niv.
Données publiquement accessibles	1
Données dont l'accès doit être justifié par un intérêt légitime	2
Données dont la diffusion non-autorisée peut affecter la réputation des personnes concernées	3
Données dont la diffusion, la modification, la perte ou la destruction non-autorisée peut affecter l'existence ou la santé, la liberté et la vie des personnes concernées	**4**

Gravité basée sur les dommages causés	Niv.
Les personnes concernées ne seront pas affectées ou pourraient rencontrer quelques inconvénients qu'elles surmonteront sans problème	Négligeable
Les personnes concernées pourraient rencontrer des inconvénients significatifs qu'elles seraient capables de surmonter mais avec quelques difficultés	Limité
Les personnes pourraient rencontrer des conséquences significatifs qu'elles seraient capables de surmonter mais avec de sérieuses difficultés	Signifiant
Les personnes pourraient rencontrer des inconvénients significatifs, voir irréversibles, des conséquences insurmontables	**Maximum**

4 - Contexte

- Critères de valorisation de la vraisemblance (Annexe A)

Vraisemblance	Niv.
La survenance n'apparaît pas possible	Négligeable
La survenance apparaît difficile	Limité
La survenance apparaît possible	Signifiant
L'exploitation de la vulnérabilité par la menace apparaît extrêmement facile	**Maximum**

- Niveau de risque
  - Déterminer la combinaison **Gravité** et **Vraisemblance**

4 - Contexte

- Critères de valorisation des actifs
  - Absents de la norme ISO 29 134

- Nature des données (courantes, protégées, sensibles)
- Le volume des données
- Les opérations de traitement (profilage, interconnexions, etc.)
- Les effets du traitements (exclusions du bénéfice d'un droit, etc.)

4 - Contexte

- Critères de valorisation des non-conformités
  - Absent de la norme ISO 29 134
- Résultat binaire
  - Conforme
  - Non-conforme
- Volonté de prioriser les actions de mises en conformité
  - Non-conformité et non-conformité majeure
  - Critères : vraisemblance, sanctions encourues, atteinte à la réputation de l'organisme

4 - Contexte

- Critères d'acceptation du risque :
  - Pas d'information dans la norme ISO 29134

- ISO 27 005, § 7.2.4
  - Niveau cible, modulés
  - Risque / Profit
    - > Risque vie privée : profit pour les personnes concernées
  - Coûts de traitement du risque
  - Mesures envisagées
  - Typologie des risques
    - > Les risques générant une Non-conformité légale et réglementaire ne peut pas être accepté

5 – Appréciation des risques

1 - Identification des risques (6.4.4.1)
Identifier les actifs
- Données personnelles, leurs supports, les processus
- Déterminer leur propriétaire
- Valoriser les actifs
- Identifier leurs vulnérabilités

Identifier les mesures existantes
Identifier les menaces
Identifier les conséquences potentielles

2 - Analyse des risques (6.4.4.2)
- Valoriser la vraisemblance des menaces
- Valoriser la gravité des impacts
- Calculer le niveau de risque

3 - Evaluation des risques (6.4.4.3)
- Prioriser les risques et les non-conformités
- Dresser la cartographie des risques

Consultation des parties prenantes (6.3.4.3)
- Propriétaires des actifs
- Utilisateurs des actifs
- Clients et partenaires
- Personnes concernées

5 – Appréciation des risques

1 – Identification des risques

- Les actifs
  - Les actifs informationnels : données à caractère personnel (6.3.3)
  - Les supports (6.3.3)
  - Les processus : les flux de données (6.4.1) et aux processus de gestion des droits des personnes (6.3.3)

- Propose une liste de questions
  - Liste non-exhaustive
  - Croiser avec
    - les informations figurant sur le futur registre des activités de traitement (art. 30 GDPR)
    - les outils proposés par la CNIL

- Une méthode
  - Compléter une fiche du registre
  - Identifier les flux de données et les processus de gestion des droits
    - Acteurs
    - Supports

5 – Appréciation des risques

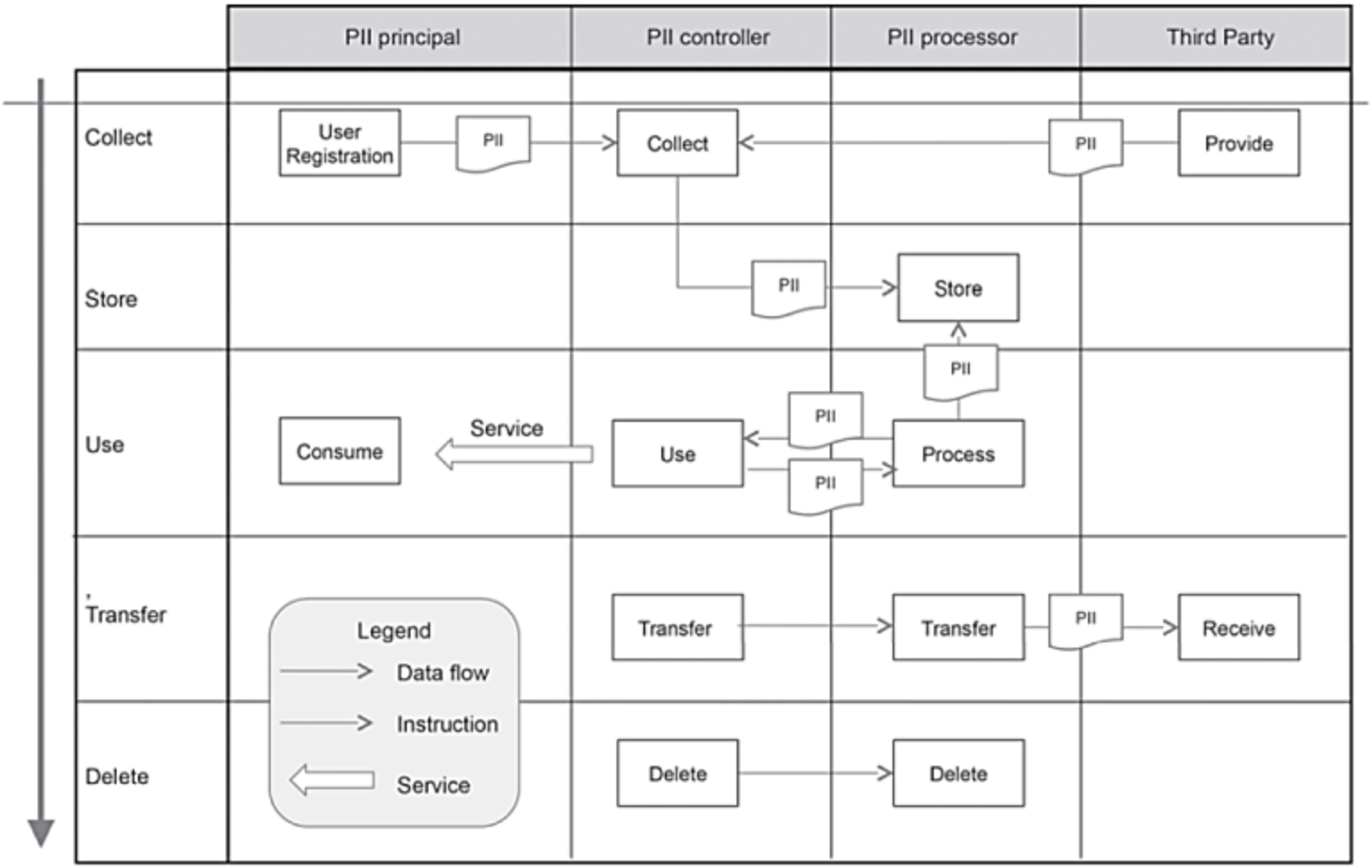
- Exemple fiche de registre

Intitulé du traitement		
Responsable de traitement Son représentant		
Service en charge du traitement Son représentant		
Finalités	Sous-finalités	
Base légale		
Catégories de données	Supports	Localisation
Volume de données		
Catégories de personnes concernées Leur nombre		
Collecte Origines Modalités Informations / Consentement		

Les usages
Les modalités de transmission
La mise à jour
Durée de conservation L'archivage L'effacement
Interconnexions
Transferts de données Destinataires et localisation Modalités juridiques
Sous-traitance Sous-traitant Données concernées Modalités juridiques

5 – Appréciation des risques

- Exemple d'illustration de flux (Annexe D)



5 – Appréciation des risques

- Les menaces
  - Implications des cas d'usage (6.4.2)
  - Menaces génériques (Annexe B)
- Les mesures existantes
  - Protection des données personnelles (sécurité)
  - Gestion de la conformité
- Les vulnérabilités
- Les conséquences
  - Impacts CID
  - Non-conformités
- Scénarios d'incident (6.4.4.1 et 6.4.4.2)

5 – Appréciation des risques

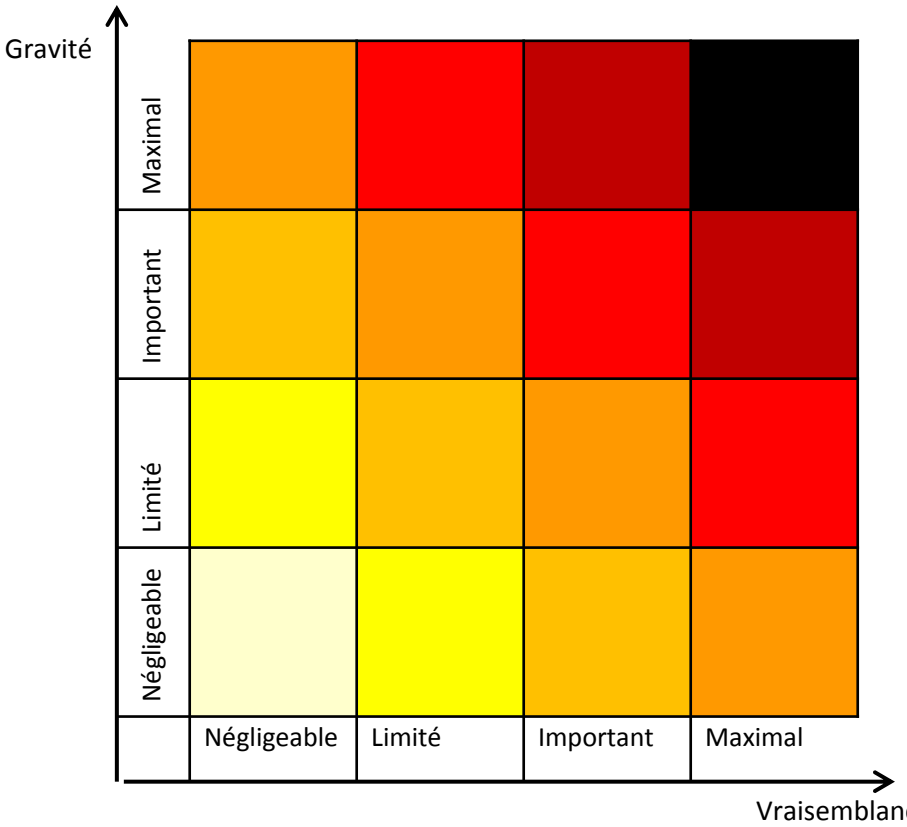
2 - Analyse des risques (6.4.4.2)

- Pour chaque risque identifié, déterminer :
  - La source de menaces la plus probable
  - La menace la plus probable
  - L'impact le plus sévère pour les personnes concernées
  - Le propriétaire du risque
  - Les mesures existantes
  - Le niveau de l'impact (conséquences potentielles)
- Estimer le risque
  - Combiner la vraisemblance de la menace et le niveau de l'impact
- Identifier les non-conformités (6.4.3)

5 – Appréciation des risques

3 - Evaluation des risques

- Priorisation des risques
- Cartographie des risques



Non-conformités
N/A
NC
NC Majeure

5 – Appréciation des risques

- Intégrer exemple de tableau excel

Actifs	Vuln et Mesures	Menace	Sc. incident	I			G	V	R	NC		Proprio	Approb.
				C	I	D				Description	Niv		
Site Internet Données du compte utilisateur	Vuln : Site vulnérable aux injections SQL	Récupération et diffusion non-autorisées des données	Un individu récupère ou modifie l'ensemble des données de compte utilisateurs							Manquement à l'obligation de sécurité des données (art. 34)		Direction	Oui

Remarque : il est aussi possible de gérer les non-conformités au travers d'une DdA (Déclaration d'Applicabilité)

6 – Le traitement des risques

1 - Choix des options de traitements (6.4.5.1)

Réduction	Maintien	Refus	Transfert

2 - Déterminer les mesures (6.4.5.2)

Mesures de protection des données	Mesures de mise en conformité

Annexe A de l'ISO 27 001
ISO 29 151 (en projet)

3 - Plan de traitement des risques (6.4.5.3)

Approbation par les propriétaires du risque

Déclaration d'acceptation par la direction

Validation du plan de traitement — Validation des risques résiduels

Calqué sur la norme ISO 27005

4 – Implémentation du plan (6.5.3)

5 – Surveillance et Evaluation (6.5.4)

6 – Amélioration et Actualisation (6.5.5)

S'intègre à un SMSI (ISO 27 001)

7 – Le rapport de PIA

1. Le périmètre du PIA
   a. Présentation du projet évalué
   b. Critères du risques
   c. Ressources et équipes
   d. Parties prenantes consultées
2. Les exigences en matière de protection des données
3. L'appréciation des risques
   a. Sources du risque
   b. Menaces et vraisemblance
   c. Conséquences potentielles et gravité de l'impact
   d. Evaluation des risques
   e. Analyse de la conformité
4. Plan de traitement des risques
5. Conclusion
   - Acceptation des risques résiduels
   - Décision de non-implémentation de recommandations issues du plan de traitement des risques
   - Modalités de communication
   - Approbation et signature par la Direction

7 – Synthèse publique

1. Bénéfices du projet
2. Les catégories de données traitées
3. Les juridictions légales
4. La synthèse de l'analyse de conformité
5. La synthèse des mesures de conformité et de traitement des risques mises en œuvre
6. Les recommandations faites aux personnes concernées
7. L'organisation responsable du PIA et du projet
8. Le point de contact pour le responsable de traitement
9. La hotline ou le service support pour le projet