# Licences de dépendances : la checklist SPDX pour un inventaire fiable

Transformez la gestion des licences de vos composants tiers en un contrôle reproductible. Cette fiche vous aide à relier chaque dépendance à une version, une preuve et un identifiant SPDX exact.

### Au sommaire



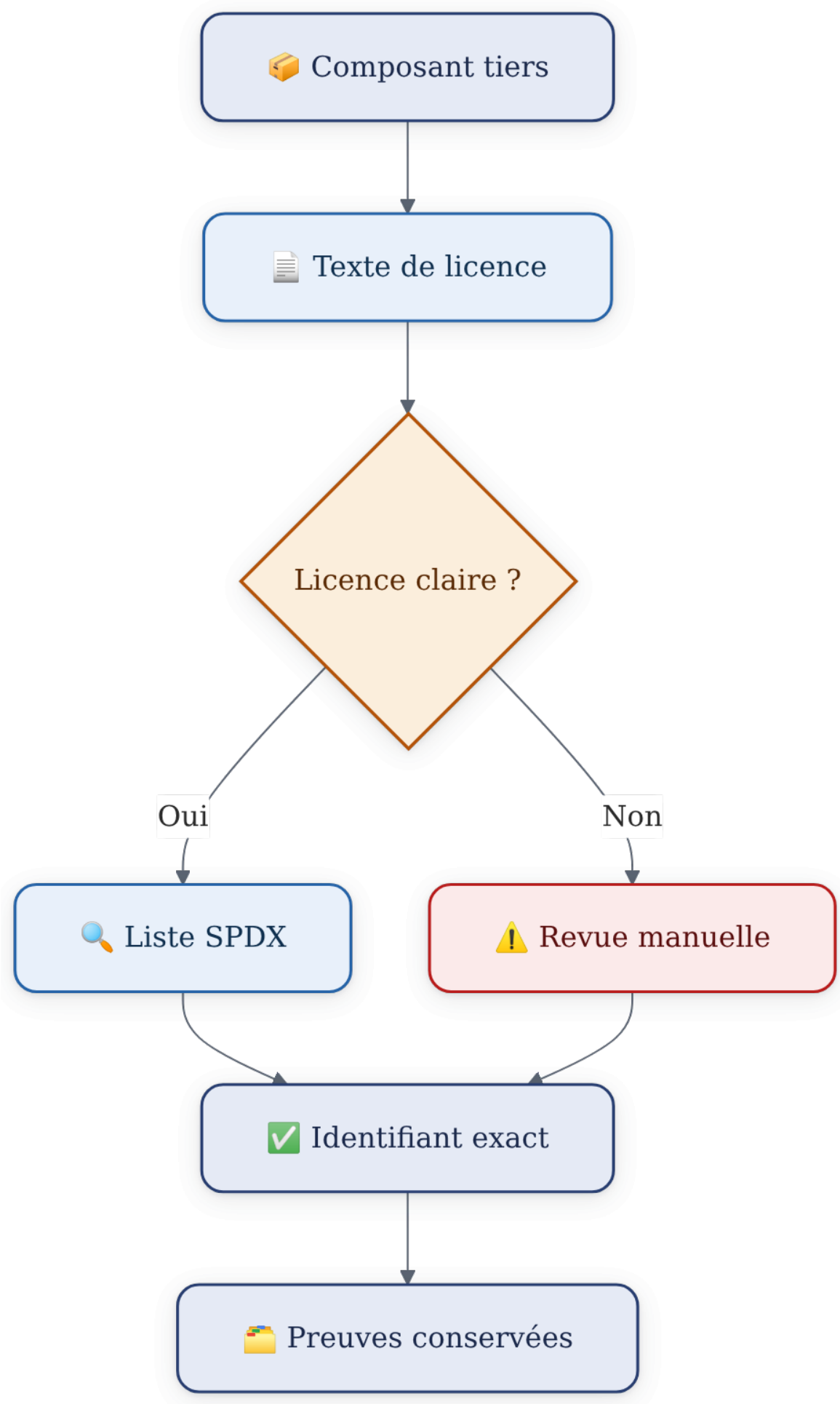
## Le repère essentiel

SPDX normalise la façon de nommer les licences afin de limiter les libellés ambigus.

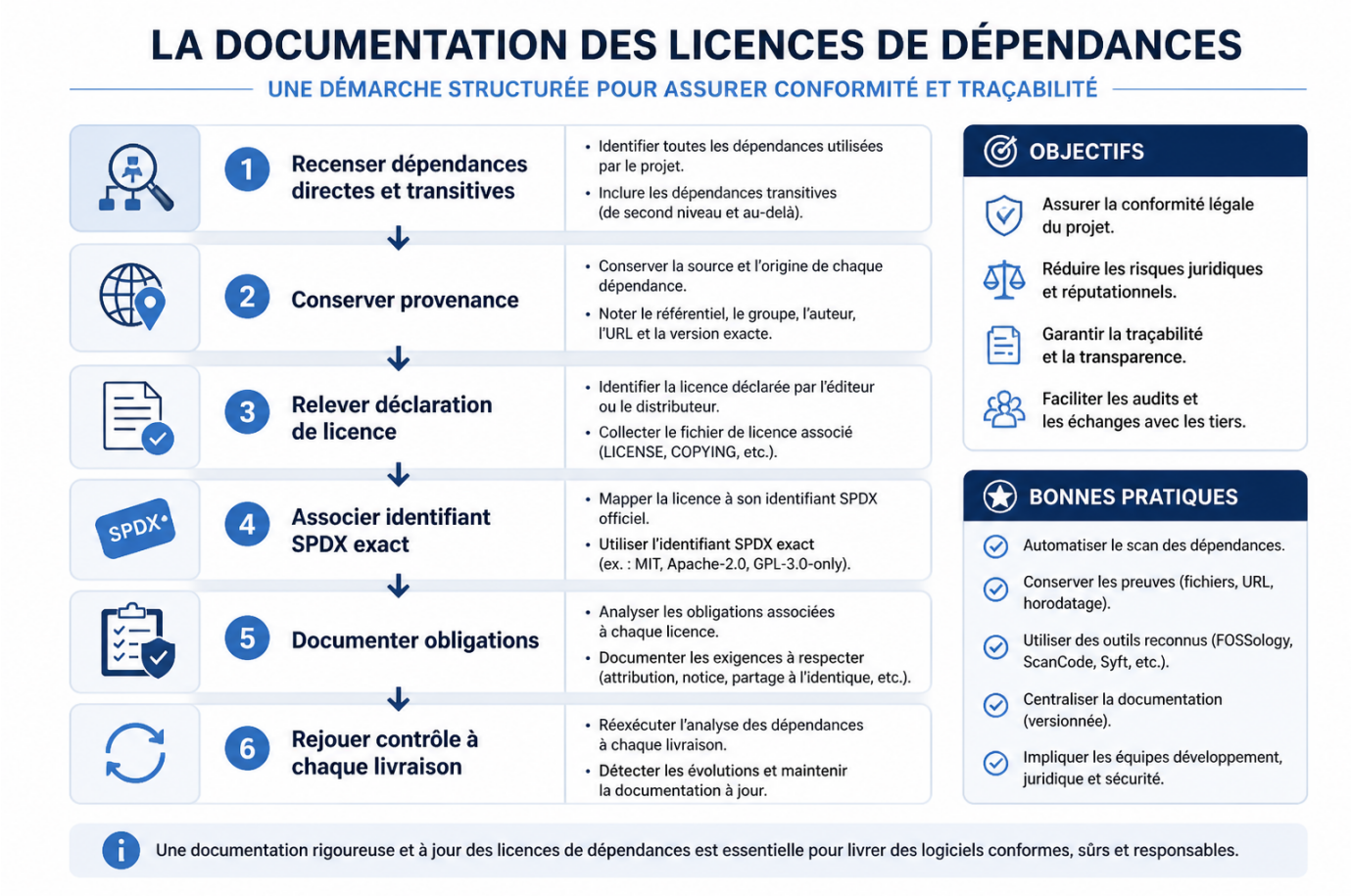
Un identifiant SPDX facilite l'inventaire et l'automatisation, mais ne remplace ni le texte de licence ni les avis de copyright.

Le périmètre doit inclure les dépendances directes et transitives.

Une expression SPDX décrit une licence ou un choix de licences ; elle ne constitue pas, à elle seule, une décision de conformité.


📦 Composant tiers
📄 Texte de licence
Licence claire ?
Oui
Non
🔍 Liste SPDX
⚠️ Revue manuelle
✅ Identifiant exact
🗂️ Preuves conservées

**INFOGRAPHIE** *Schéma du processus d'identification SPDX pour les licences de dépendances logicielles*




**INFOGRAPHIE** *Étapes de documentation des licences de dépendances avec identifiants SPDX.*

## 1. Construire un inventaire exploitable

- **Exporter le graphe des dépendances directes et transitives**
  Utiliser le gestionnaire de paquets ou l'outil de build.
- **Figer la version analysée de chaque composant**
  L'inventaire doit correspondre à un état précis du projet.
- **Identifier les composants réellement embarqués ou distribués**
  Inclure notamment les livrables, conteneurs et bibliothèques distribuées.
- **Noter la provenance de chaque composant**
  Registre, dépôt source, archive ou image de conteneur.
- **Prévoir un format de suivi durable**
  Manifeste, SBOM ou registre interne plutôt qu'un relevé ponctuel.

## 2. Vérifier l'attribution de licence

- **Consulter les métadonnées du paquet**
  Elles constituent un signal, pas une preuve suffisante à elles seules.
- **Lire le fichier LICENSE ou le texte de licence fourni**
  Partir de la déclaration du composant concerné.

**Contrôler les en-têtes de code et les notices incluses**
Relever les avis de copyright et les fichiers NOTICE éventuels.

**Conserver la source de l'attribution**
Associer la preuve à la version exacte du composant.

**Marquer les résultats ambigus ou contradictoires**
Ils nécessitent une investigation manuelle.

## 3. Choisir la notation SPDX adaptée

| Information constatée | Notation SPDX | Contrôle à conserver |
|---|---|---|
| Licence MIT clairement déclarée | MIT | Texte de licence et avis de copyright fournis |
| Apache License, Version 2.0 | Apache-2.0 | Notices, fichier NOTICE éventuel et périmètre de distribution |
| GNU GPL version 3 uniquement | GPL-3.0-only | Absence de formulation autorisant les versions ultérieures |
| Licence spécifique à un fournisseur | LicenseRef-Interne | Texte complet, origine et validation adaptée au contexte |

! **Ne pas approximer les identifiants**
Copiez l'identifiant exactement tel qu'il figure dans la SPDX License List, y compris les traits d'union et les suffixes comme « -only » ou « -or-later ». Évitez d'introduire un identifiant déprécié lorsqu'une expression recommandée existe.

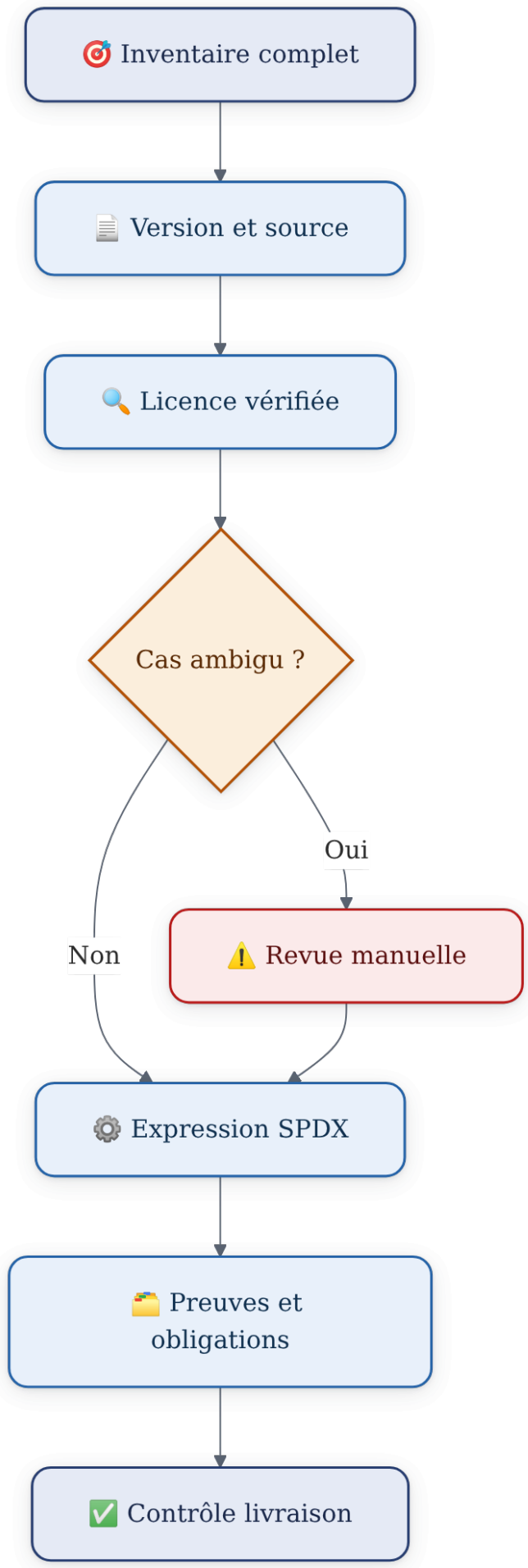

🎯 Inventaire complet
📄 Version et source
🔍 Licence vérifiée
Cas ambigu ?
Oui
Non
⚠️ Revue manuelle
⚙️ Expression SPDX
🗂️ Preuves et obligations
✅ Contrôle livraison

**SCHÉMA** *Parcours de documentation et de contrôle des licences SPDX des dépendances.*

## 4. Finaliser le contrôle avant chaque livraison

- **Associer chaque dépendance à son identifiant SPDX vérifié**
  Ne pas déduire la licence d'un simple libellé approximatif.
- **Documenter les obligations identifiées**
  Conserver textes, avis, exceptions et décisions internes nécessaires à la redistribution.
- **Traiter manuellement les licences absentes, personnalisées ou contradictoires**
  Un outil de scan est un point de départ, non une conclusion.
- **Mettre à jour l'inventaire à chaque livraison**
  Une nouvelle version peut modifier la licence, les notices ou la chaîne transitive.
- **Prévoir une revue adaptée lorsque le cas est sensible ou incertain**
  La normalisation SPDX ne remplace pas l'analyse des obligations applicables.

*Cette fiche aide à structurer la documentation des licences ; elle ne remplace pas l'analyse des obligations de redistribution ni un avis juridique lorsque nécessaire.*