# Open Source Cartouche

## Un nouveau standard pour la gouvernance et la gestion du risque

# Constat

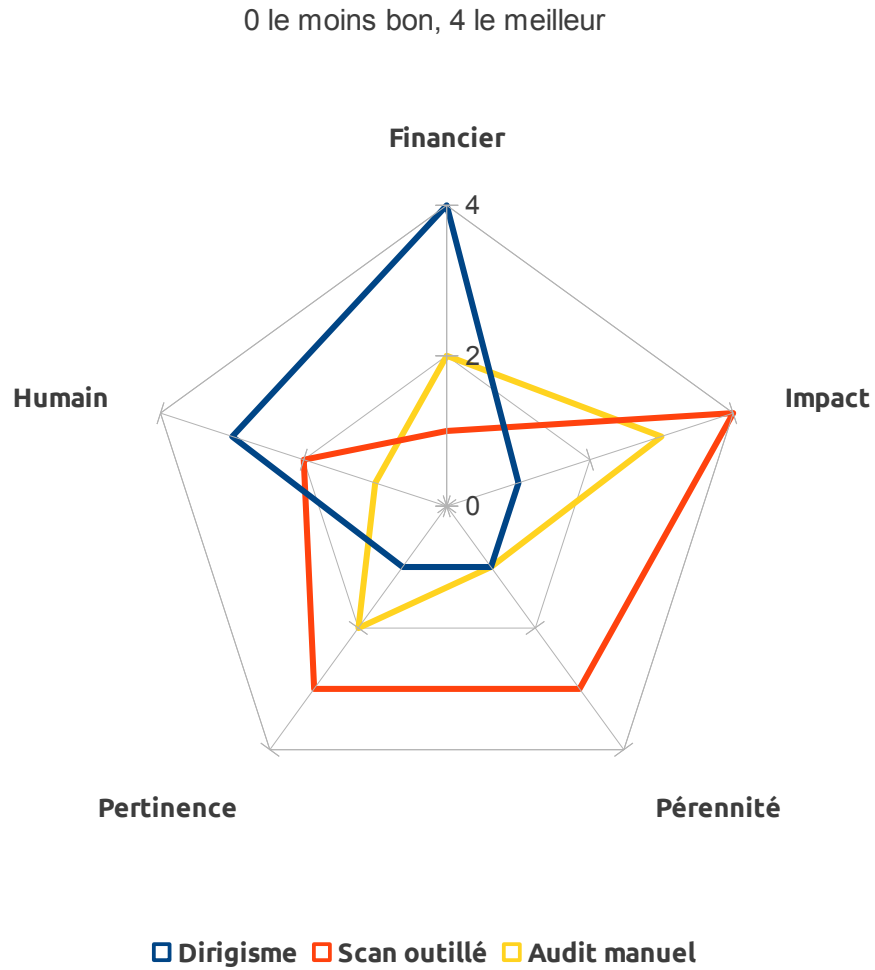
- De nombreux projets utilisent des composants Open Source distribués sous des licences incompatibles entre-elles
- Le respect des licences n'est pas une priorité pour les équipes
- Les plannings ne prévoient que rarement le contrôle de conformité des licences des composants embarqués
- La contamination du code est (presque) toujours involontaire
- Le code propriétaire est contaminé par trois vecteurs majeurs
  - Équipes de développement[1] locales
  - Outsourcing
  - TMA

1: cf. http://www.la-rache.com/

# Conséquences

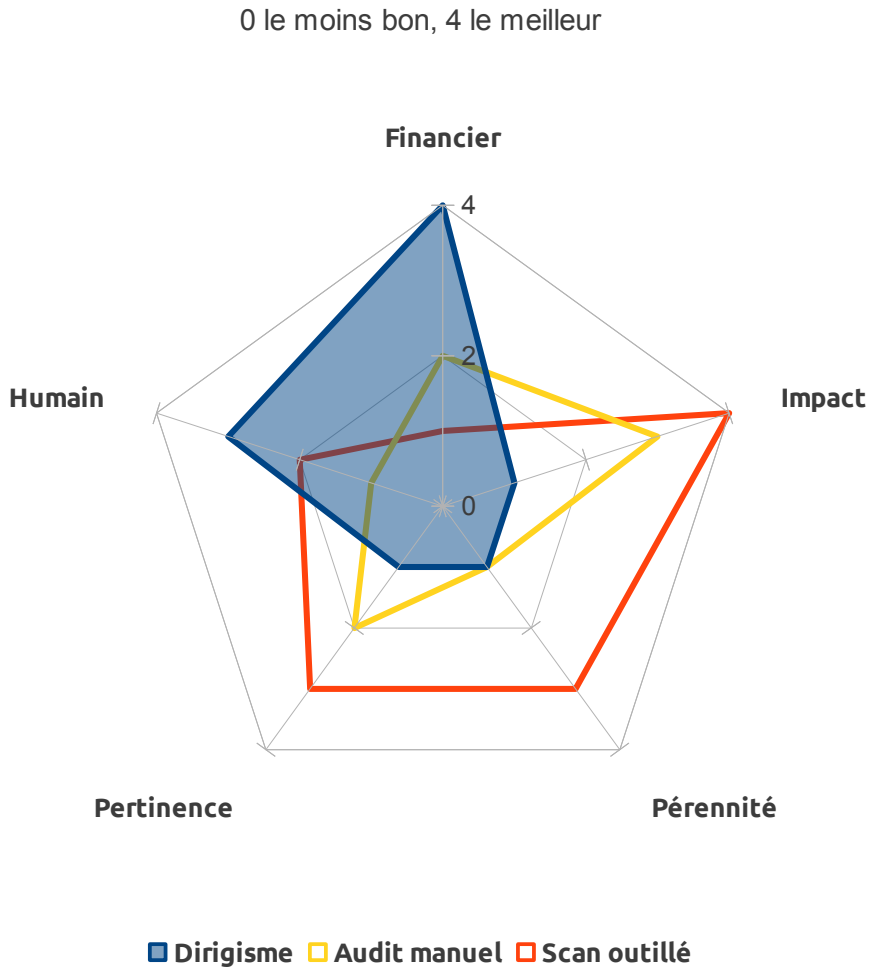
- Pour le projet
  - Code propriétaire contaminé par des licences restrictives
  - Non respect des obligations de plusieurs licences
  - Perte de la « Propriété Intellectuelle »
  - Risques sur la pérennité
- Pour l'industrie
  - Perte de crédibilité des tiers (TMA, Prestas...)
  - Perte de crédibilité de l'Open Source
- Pour la communauté
  - Perversion de la philosophie du logiciel Open Source
  - Perte de motivation et risque de démobilisation

# Solutions conjoncturelles




- Dirigisme
- Scan outillé
- Audit Manuel

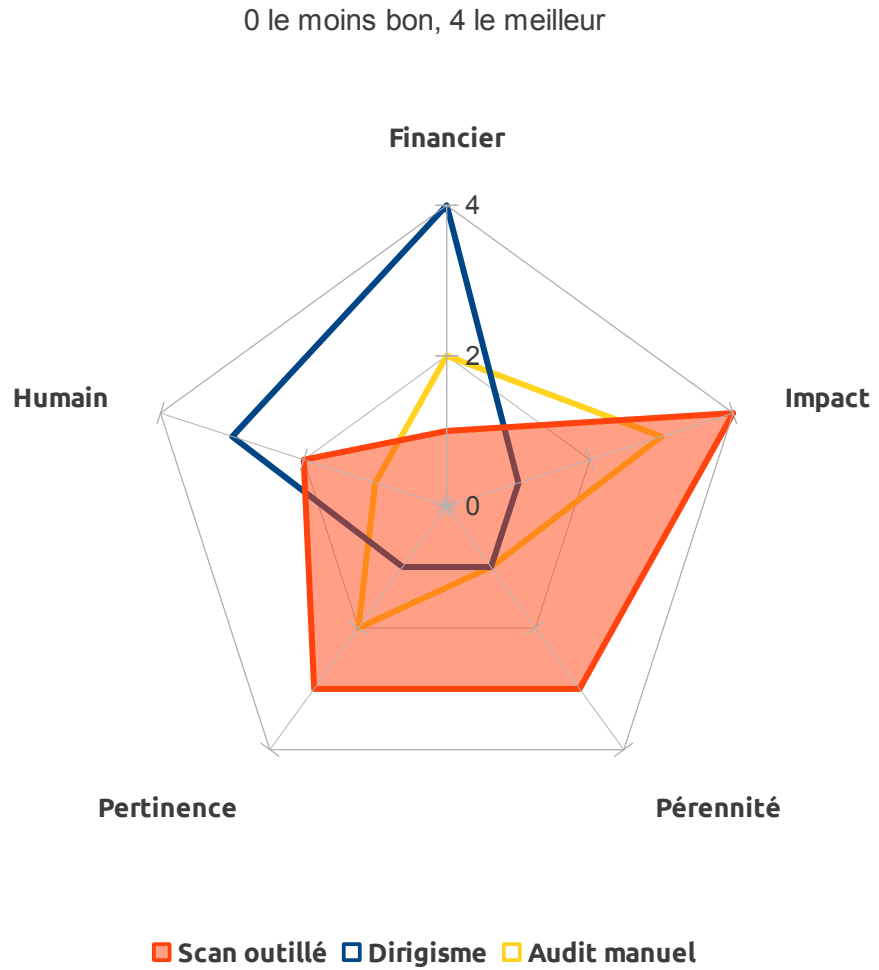
# Dirigisme




## Solution de facilité

- Peu coûteux
- Quelques ressources
- Peu pertinent
- Peu pérenne
- Très impactant

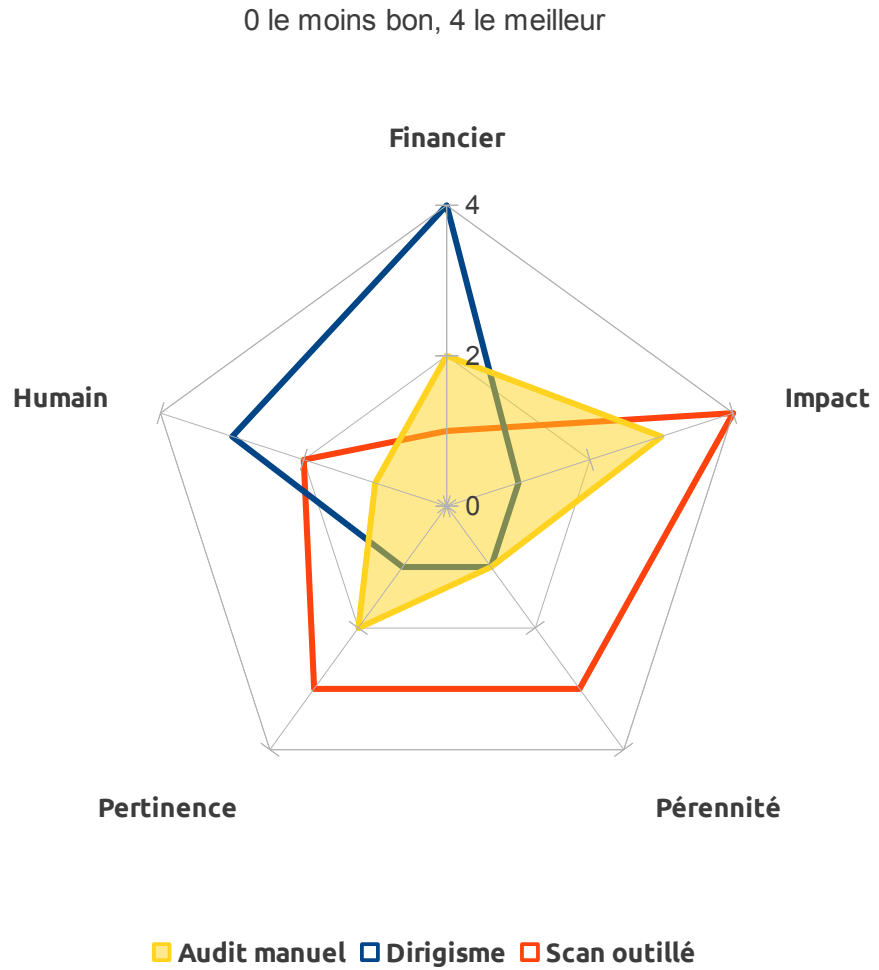
# Scan outillé




## Expertise externe

- Coûteux
- Quelques ressources
- Globalement pertinent
- Globalement pérenne
- Peu impactant

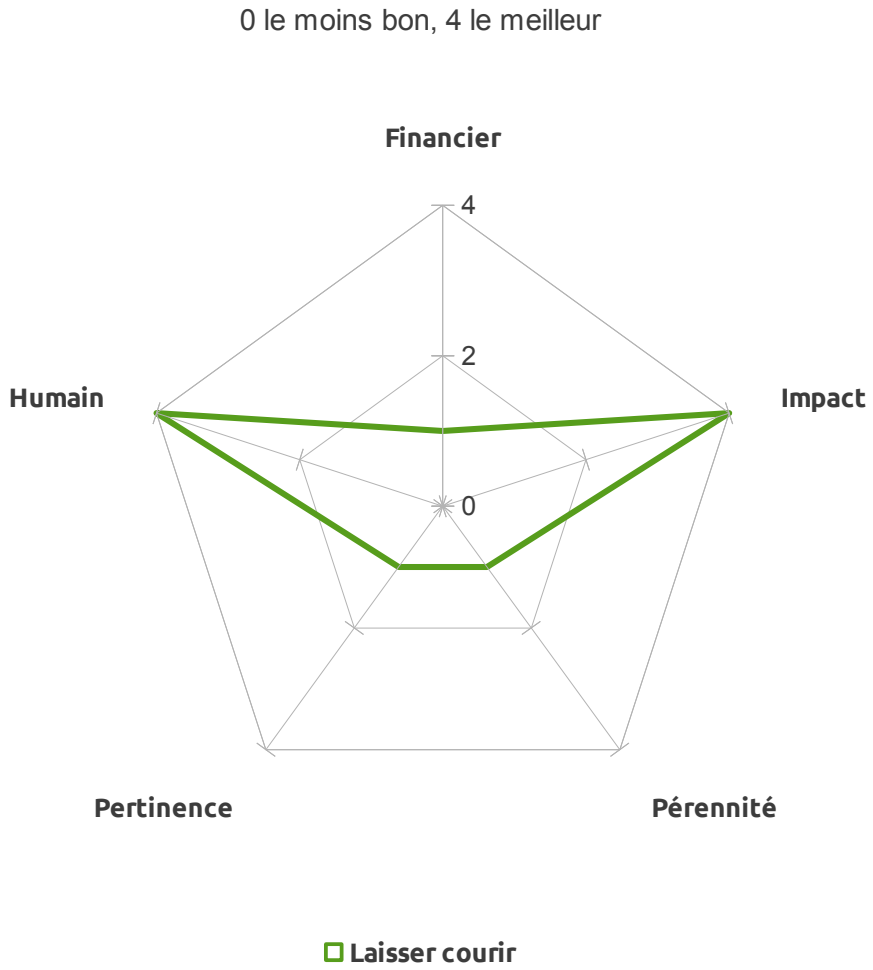
# Audit Manuel




## Travail de fourmi

- Faiblement coûteux
- Mobilise beaucoup de ressources
- Peut être pertinent
- Peu pérenne
- Moyennement impactant

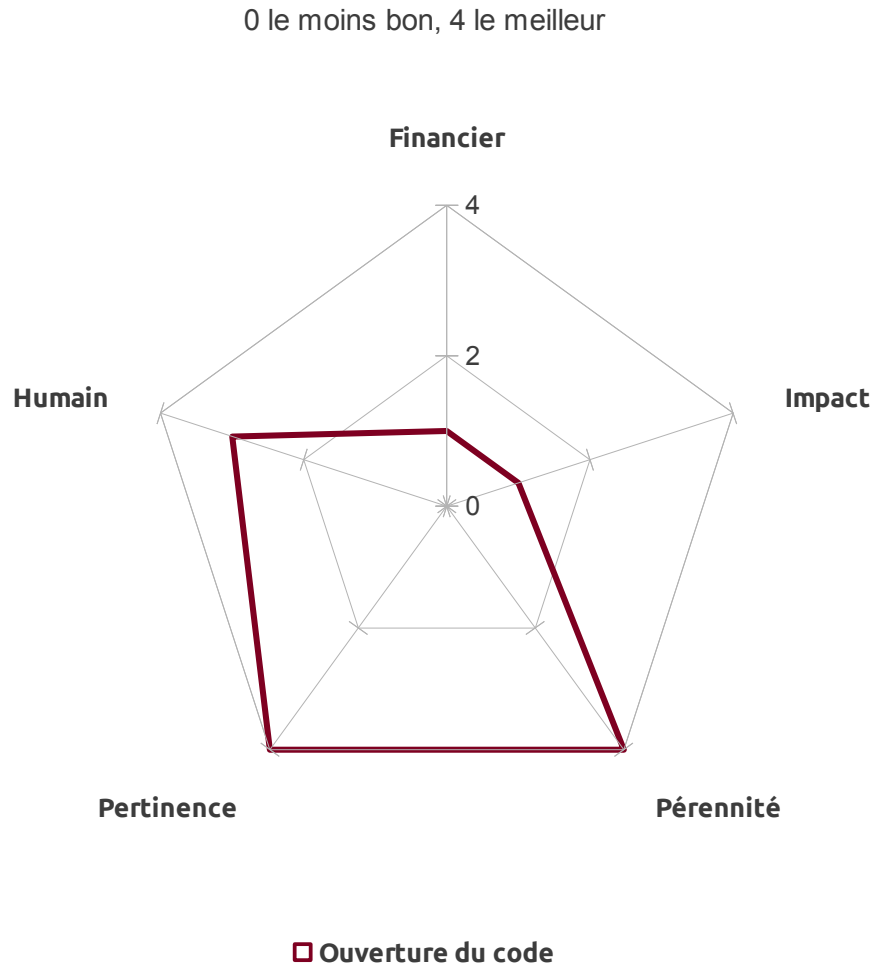
# Contre exemple 1
# « Laisser Courir »




## Prendre le risque

- Potentiellement très coûteux
- Aucune ressource
- Peu pertinent
- Peu pérenne
- Très impactant à terme

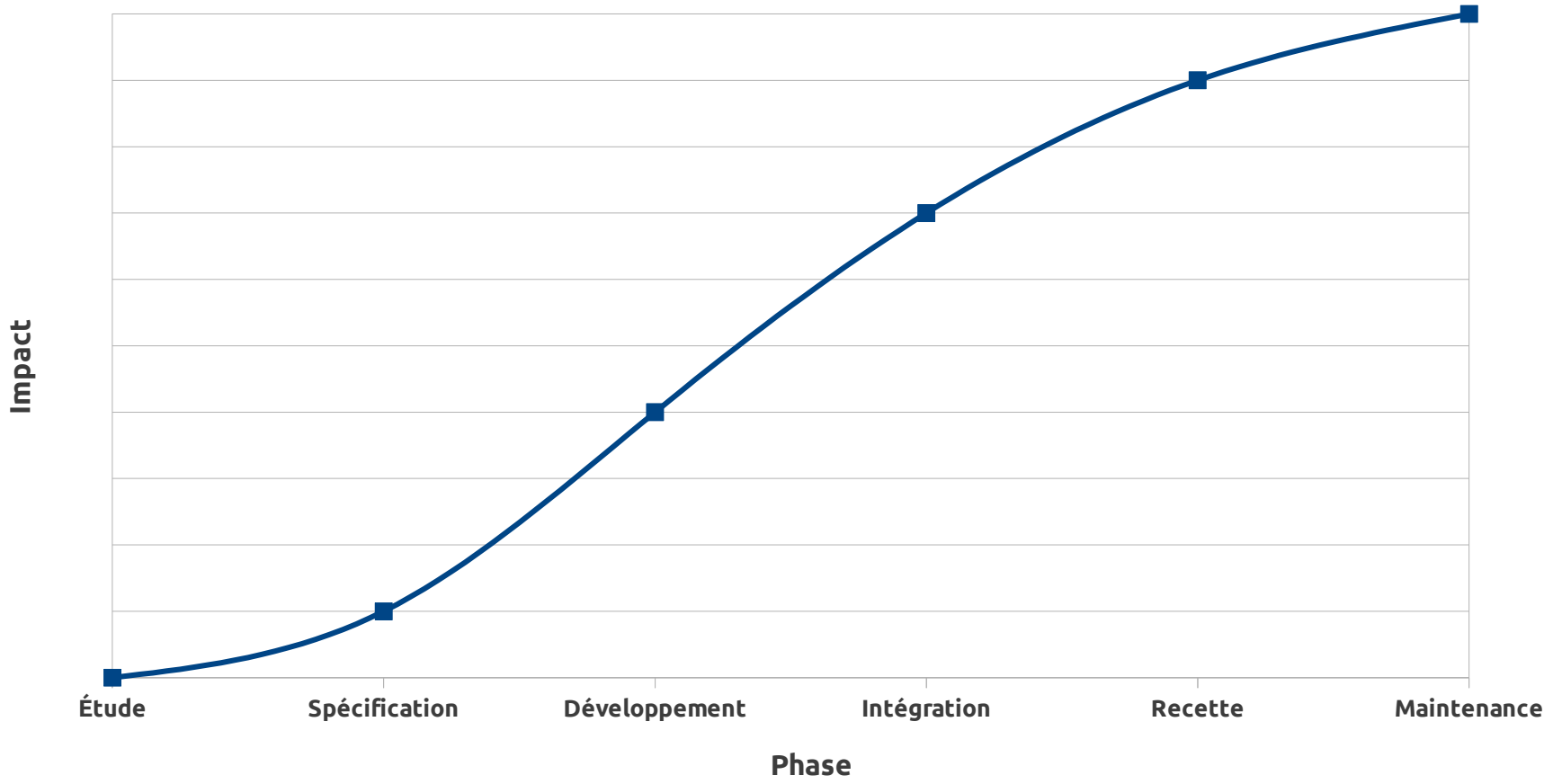
# Contre Exemple 2
# Ouverture du code




## Mise en conformité

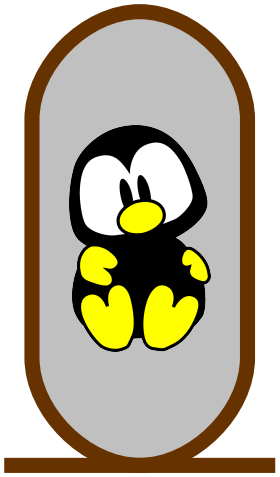
- Peu coûteux
- Nécessite d'être en conformité
- Très pertinent
- Très pérenne
- Irréversible

# Mise en conformité :
# Impacts VS Phase du projet



# Il faut appréhender le problème le plus tôt possible

# Open Source Cartouche



**Ensemble minimal d'informations permettant de qualifier un composant Open Source**

**Dérivé de la section générique de QSOS²**

2: http://www.qsos.org

# Enjeux

- Pour les projets :
  - Adresser les risques liés aux licences en amont
  - Connaître récursivement les composants embarqués dans les projets pour mieux appréhender les risques
- Pour l'industrie :
  - Proposer une solution structurelle aux problèmes de gouvernance sans remettre en cause les outils de scan
  - Tenter de mieux se prémunir contre les contaminations
  - (Re)donner confiance dans l'Open Source
- Pour les communautés :
  - Protéger le travail des communautés en arrêtant de violer les licences

# Exemple 1/3

- Composant
  - Nom
    - Open Source Cartouche
  - Version
    - 0.1
  - Page d'accueil du projet
    - http://www.opensourcecartouche.org
  - [Statut]
    - Bêta
  - [Date de publication]
    - 11/05/2011
  - [Type]
    - Identification de composant
  - [Technologie majeure]
    - Open Document

# Exemple 2/3

- Licence
  - Nom
    - GNU Free Documentation License
  - Version
    - 1.3
  - Texte complet
    - http://www.gnu.org/licenses/fdl.html
- Développeurs
  - Nom
    - Philippe-Arnaud HARANGER
  - Email
    - philippe-arnaud.haranger@atosorigin.com
  - Société
    - Atos Origin

# Exemple 3/3

- Restrictions
  - Propriétaire du Droit d'Auteur
    - Atos Origin
  - [Brevets logiciels connus]
    - Aucun
  - [Algorithmes de chiffrement utilisés]
    - Aucun
- [Misc]
  - Commentaires libres
  - Nombre de Fichiers
  - Volume de Données
  - Dépendances

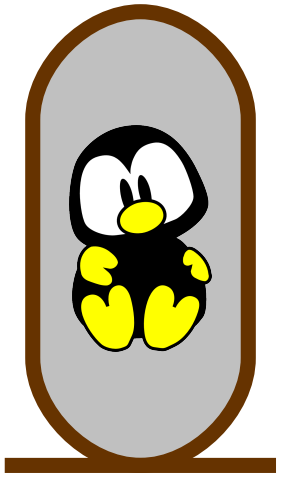
```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE Cartouche SYSTEM "http://www.opensourcecartouche.org/dtd/0.1.dtd">
<Cartouche Version="0.1">
    <Component>
        <ComponentName>Open Source Cartouche</ComponentName>
        <ComponentVersion>0.1</ComponentVersion>
        <ComponentHomepage>http://www.opensourcecartouche.org</ComponentHomepage>
        <Status>Beta</Status>
        <ReleaseDate>11/05/2011</ReleaseDate>
        <Type>Methodology</Type>
        <MainTech>Open Document</MainTech>
    </Component>
    <License>
        <LicenseName>GNU Free Documentation License</LicenseName>
        <LicenseVersion>1.3</LicenseVersion>
        <LicenseHomepage>http://www.gnu.org/licenses/fdl.html</LicenseHomepage>
    </License>
    <Team>
        <Developer>
            <DeveloperName>Philippe-Arnaud HARANGER</DeveloperName>
            <DeveloperEmail>philippe-arnaud.haranger@atosorigin.com</DeveloperEmail>
            <DeveloperCompany>Atos Origin</DeveloperCompany>
        </Developer>
    </Team>
    <Legal>
        <Copyright>Atos Origin</Copyright>
    </Legal>
    <Misc>
        <FileNumber>2</FileNumber>
        <Data>
            <Volume>1.2</Volume>
            <Unit>Mo</Unit>
        </Data>
        <Dependencies>
            <Component>
                <ComponentName>Libre Office</ComponentName>
                <ComponentVersion>3.2</ComponentVersion>
                <ComponentHomepage>http://www.libreoffice.org</ComponentHomepage>
            </Component>
        </Dependencies>
    </Misc>
</Cartouche>
```

# Utilisations Envisageables

- Gouvernance
  - Vérifier la conformité des composants (ping @Fossology)
  - Lister l'ensemble des composants embarqués dans une application (récursivement)
- Sécurité
  - Corréler les composants et la liste de leurs vulnérabilités connues et alerter en temps réel
- Développement
  - Juger les composants sur des critères objectifs non techniques
- Tiers (Prestataires, TMA...)
  - Rassurer les clients sur les composants intégrés
- Communautés
  - Informer de l'état et du devenir du projet pour rassurer les utilisateurs

# Et maintenant ?

- S'accorder sur le contenu du standard
- Publier le Cartouche des projets sur lesquels VOUS travaillez
- Promouvoir le standard en privilégiant les projets diffusant leur Cartouche
- Créer l'écosystème permettant d'élargir les possibilités
  - Générateur de Cartouche en ligne
  - Générateur de badge pour publication en ligne
  - Vérificateur de cohérence des licences
  - Outil de demande de composant pour un projet
  - Vérificateur des failles de sécurité connues



# JOIN US !

http://www.opensourcecartouche.org

@OSCartouche