Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF
Transformation numérique et gouvernance de l'informatique TNI

14.09.2026

Em002-2.2 Liste de contrôle Analyse et préparation OSS

Version 2.0-cc435f3

Table des matières

1. Objet 2
1.1. Nom et brève description du logiciel 2
1.2. Personne de contact et examen 2
2. Liste de contrôle 2
3. Remarques finales 4

Cette liste de contrôle fait partie du document *Em002-2 Instructions pour la publication de logiciels open source* et s'adresse aux spécialistes TIC.
Elle sert à examiner la documentation et le code source d'un projet. Elle contribue ainsi à garantir que le niveau de qualité de la documentation est suffisant pour publier une application en open source. Elle permet également de vérifier que le code source et tous les composants tiers utilisés par le projet ne présentent aucun risque juridique. Ces mesures réduisent les risques de sécurité.
Les informations relatives à cette liste de contrôle figurent dans *[Em002-2]*, chapitre 4.

Cette liste de contrôle garantit en outre que la documentation du projet s'adresse aussi bien aux utilisateurs finaux qu'aux spécialistes techniques.

1. Objet

1.1. Nom et brève description du logiciel

Indiquez le nom du logiciel.

1.2. Personne de contact et examen

Indiquez l'organisation, la personne de contact du service spécialisé ainsi que les personnes responsables (p. ex. ISBO/DSBO) qui ont vérifié le respect des exigences de publication.

2. Liste de contrôle

☐ La *liste de contrôle Em002-2.1 Évaluation préalable OSS* a été remplie et aucun point problématique n'a été constaté.

☐ Le code source à publier a été analysé.

- Vérifier comment la qualité du code existante et les directives ont été mises en œuvre.
- S'assurer qu'aucune donnée (de test) sensible n'est incluse, p. ex. des données fondées sur des personnes ou des cas réels.
- Documentation à jour (voir [Em002-2] annexes D.1. et D.2.)
- Supprimer les fichiers inutiles ou les documents obsolètes.
- Vérifier le code à la recherche de secrets ou d'identifiants.[1]
- Effectuer des tests de sécurité ciblés et mettre ensuite en place un programme de bug bounty (public).[2]

1. https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2022/git.html
2. https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-it-spezialisten/themen/bug-bounty-programme.html

- Examiner toutes les bibliothèques utilisées afin de s'assurer que les licences sont disponibles et que les listes correspondantes (attributions) ont été établies.
- Description du déploiement (pipeline CI/CD[3]) et, le cas échéant, mise en place d'une instance de démonstration.

☐ Choix de la licence

- Vérifier les éventuelles dépendances à des licences existantes.
- Pour le code de tiers, vérifier la compatibilité des conditions d'utilisation avec la licence prévue et remplacer le code si nécessaire.
- Choisir la licence appropriée à l'aide du guide « Em002-3 Guide de licences OSS » (les recommandations principales sont l'AGPL pour le copyleft et la MIT pour les licences permissives).

Licence choisie et justification

☐ La documentation est conservée avec le code source (voir [Em002-2] annexe D.1.)

Justification / lieu de conservation

☐ La documentation s'adresse aussi bien aux utilisateurs finaux qu'aux spécialistes techniques.

Liste de la documentation centrale

☐ Documentation détaillée du code source (spécifique à l'OSS)

La documentation standard importante (README, LICENSE, CONTRIBUTING, etc.) est disponible.

☐ Le code source, historique compris, ne contient aucune donnée personnelle sensible, protégée ou confidentielle. Ou l'historique a été entièrement supprimé. (voir [Em002-2] annexe E.2.)

Explication de l'examen (s'il n'est pas classé comme document distinct)

3. https://fr.wikipedia.org/wiki/CI/CD

☐ Il a été clarifié avec le fournisseur et tous les développeurs concernés au sein de l’administration fédérale si les informations sur les auteurs (noms, adresses électroniques) peuvent être publiées. À défaut, le code source, historique compris, a été nettoyé ou anonymisé.

☐ Les bibliothèques utilisées par le projet sont compatibles avec la licence du projet.

Explication de l’examen (s’il n’est pas classé comme document distinct)

☐ Le projet utilise un gestionnaire de paquets pour gérer ses dépendances.

☐ Le projet déclare sa licence dans le descripteur correspondant du gestionnaire de paquets. Établissement d’une Software Bill of Materials (SBOM) recensant tous les composants open source utilisés.

☐ Le code source contient un fichier *THIRD-PARTY-LICENSES.md* indiquant pour chaque bibliothèque utilisée : le nom du projet de la bibliothèque, sa page d’accueil, l’identifiant SPDX de sa licence et un lien vers celle-ci.

☐ Pour les applications, une boîte de dialogue « À propos » renvoyant au fichier *THIRD-PARTY-LICENSES.md* est disponible.

☐ Dans le cadre du processus de revue de code, il est garanti que le fichier *THIRD-PARTY-LICENSES.md* est mis à jour à chaque modification des bibliothèques.

3. Remarques finales

Remarques et renvois à d’autres documents pertinents

Classement du formulaire

Veuillez classer ce formulaire avec la documentation de projet et/ou conformément aux prescriptions de votre autorité (unité d’organisation).

Licence du modèle de liste de contrôle : CC0 1.0 Universal

Ce document est publié sous la *licence CC0*. Il peut être librement utilisé, modifié et diffusé, y compris à des fins commerciales et dans tout format.