



Il existe un certain nombre d'initiatives permettant de vérifier la qualité et le sérieux d'un site d'archivage pérenne.

Certaines sont basées sur une auto-évaluation par le site lui-même, d'autres sont basées sur un audit plus complexe effectué par des spécialistes extérieurs.

On peut citer :

- La checklist TRAC (Trustworthy Repositories Audit & Certification) proposée par l'OCLC (Online Computer Library Center), qui est issue de travaux entre le Research Library Group et les Archives nationales américaines.
- Drambora qui est une méthodologie d'autoévaluation en ligne des archives numériques, développée par le Digital Curation Centre (DCC) et le Digital Preservation Europe (DPE).
- le Core Trust Seal, émanation du DSA (Data Seal of Approval) et de l'ICSU WDS (the International Council for Science's World Data System).
- La norme ISO 16-363 qui permet d'auditer un site d'archivage pérenne. Elle est issue d'un guide de bonnes pratiques pour auditer un système numérique ; ce guide a été rédigé par le CCSDS, l'auteur de la norme OAIS. Il s'agit ici d'un processus formel assez lourd, mais qui offre une certification de haut niveau.



TRAC :

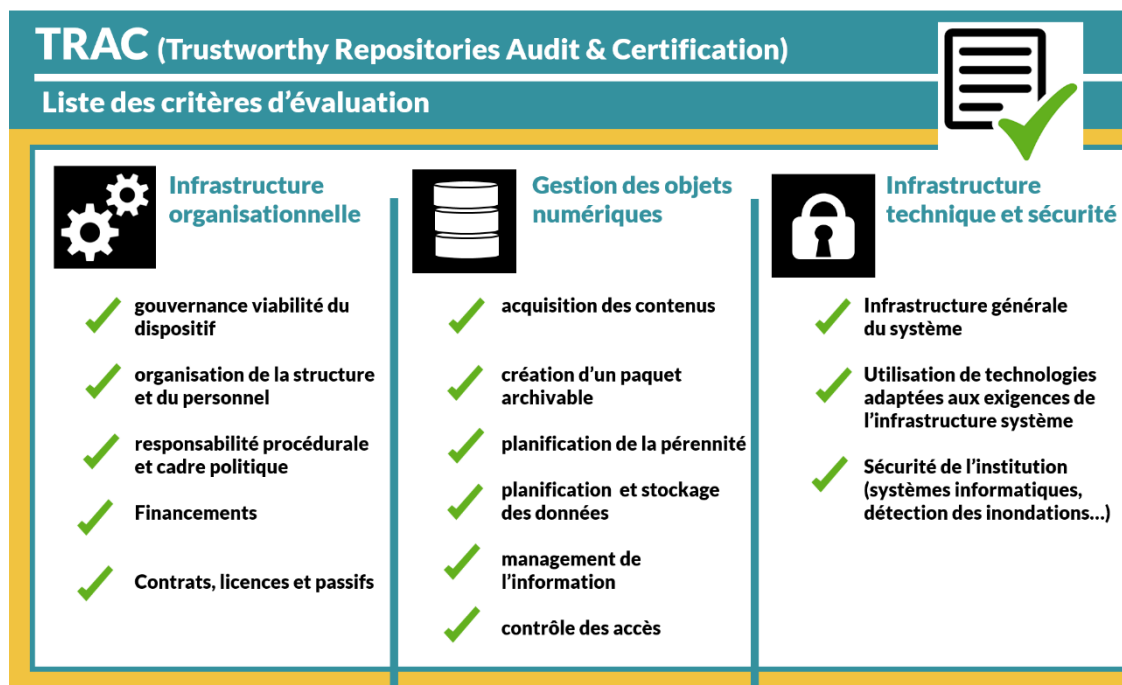
Le document [TRAC](#) (Trustworthy Repositories Audit & Certification = Audit et certification d'entrepôts fiables : Critères et liste de contrôle) est issu des réflexions d'un groupe de travail composé de la NARA (National Archives and Records Administration) et le RLG (Research Library group), et poursuivi sous l'égide de l'OCLC (Online Computer Library Center).

Son objectif est de fournir une liste de critères classés par domaines, permettant à une archive d'évaluer sa fiabilité et sa pérennité, et de démontrer que le personnel a les compétences requises (formation archivistique, compétences techniques ou expertise juridique).

Le vocabulaire et les concepts utilisés dans ce document sont définis dans [le modèle OAIS](#).

Les critères TRAC sont divisés en trois groupes de sujets. Chaque critère proposé fait l'objet d'une formulation précise, d'un texte explicatif et d'un ensemble d'exemples sur les moyens permettant de justifier que le critère est rempli.





Les auditeurs du TRAC examinent cette auto-vérification, puis effectuent une visite sur place pour recueillir les preuves fournies, et évoquer les problématiques soulevées. Les auditeurs classent ensuite le dépôt sur une échelle de 1 à 5 pour chacun des trois groupes de sujets.

Pour conserver la certification, les institutions doivent rencontrer les auditeurs dans les 18 à 24 mois pour une consultation. Après 4 ans, la certification expire et l'institution doit commencer une nouvelle vérification.

Cette liste de contrôle permet aux archives d'évaluer l'aptitude de leur institution à assurer la gestion d'une collection numérique, ou bien encore d'identifier les points faibles de la stratégie de conservation adoptée.



DRAMBORA :

Drambora a été développé en 2007 par le Digital Curation Center (DCC) britannique et le Digital Preservation Europe (DPE). Il s'agit d'une méthodologie **d'audit interne** des archives numériques, basée sur une **auto-évaluation** des risques. Elle peut être appliquée à des archives de différents types : bibliothèques, archives de données scientifiques, archives institutionnelles.

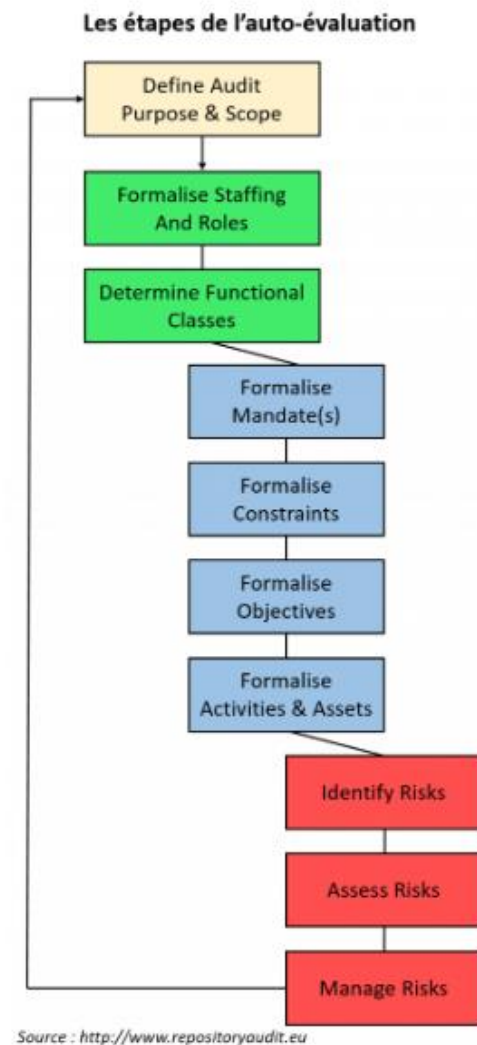
Cette méthode consiste à analyser au préalable le contexte dans lequel évolue l'organisme concerné (politique générale, objectifs, organisation, ressources etc...) afin de mettre en évidence les risques pouvant menacer le service, et de mettre en place les solutions nécessaires pour améliorer la sécurité et la stabilité d'une archive numérique.

La méthode fournit un outil en ligne ([DRAMBORA Interactive](#)) pour définir les caractéristiques d'une archive, guider les utilisateurs lors des différentes étapes du processus d'audit et ainsi faciliter l'évaluation.



La méthode est divisée en plusieurs étapes, construites sur la base des 10 exigences auxquelles doit répondre l'archive :

- obtention d'un mandat et engagement de l'archive
- organisation adaptée
- respect des lois et des réglementations
- politique efficace et effective
- infrastructure technique adaptée
- acquisition et versement des objets
- préservation de l'intégrité, de l'authenticité et de la possibilité de lecture des objets
- gestion des métadonnées et réalisation d'audits
- diffusion des objets
- actions et plans de préservation des données



Renouvelé régulièrement, ce processus d'évaluation permet de maintenir la qualité et la sécurité d'une archive, tout en préparant un audit externe pouvant mener à une certification.



CoreTrustSeal :

Le [CoreTrustSeal](#) est une organisation de certification mise en place conjointement par le **DSA** (Data Seal of Approval) et le **ICSU WDS** (the International Council for Science's World Data System).

Cette certification garantit aux déposants que leur données seront protégées et gérées de manière optimale.

Le CoreTrustSeal remplace depuis juillet 2017 les certifications DSA et WDS.

Le Data Seal of Approval (DSA) est une accréditation élaborée en 2007 par le DANS (Data Archiving and Networked Service) aux Pays-Bas.

N'importe quelle institution publique ou privée destinée à entreposer / stocker / archiver des données peut faire acte de candidature pour le Data Seal of Approval.

Le World Data System (WDS) certifie des organisations de gestion de données scientifiques tout en les regroupant dans des « communautés d'excellence ». Il aide ces communautés à améliorer leurs pratiques et procédures.

Norme ISO16363:2012 :

[La norme ISO16363:2012](#) donne des recommandations pour effectuer **un audit**. Afin d'aider les auditeurs, la norme a été conçue de manière hiérarchique.

Cette norme focalise l'attention des auditeurs sur **trois points principaux** :

- **L'infrastructure organisationnelle**, qui s'intéresse à l'organisation de l'archive, à son engagement en faveur notamment de la pérennisation, de la viabilité financière et des aspects légaux.
- **La gestion des objets numériques**, qui traite des fondamentaux de l'archivage numérique, en suivant les concepts OAIS
- **La gestion des risques** pour l'infrastructure et la sécurité, pour laquelle les auditeurs peuvent s'appuyer sur la certification ISO 27000.

L'objectif de cet audit est d'identifier les points de conformité aux critères et ceux qui nécessitent une amélioration.

