Les Webinars du CT2M

LE PARTENAIRE À VOTRE MESURE

Réunion n°28 du Club des Laboratoires Accrédités

Partage d'expériences, évolutions dans le domaine de l'accréditation, évolutions normatives…

Comment auditer le système d'information d'un laboratoire accrédité en s'appuyant sur le GEN GTA 02 ?

PROGRAMME

I. Présentation du CT2M

II. Déroulement du webinar

III. Thématique : Comment auditer le système d'information d'un laboratoire accrédité en s'appuyant sur le GEN GTA 02 ?

IV. Questions / réponses

V. Conclusion

Le CT2M, Centre Technologique Méditerranéen de Métrologie

Le CT2M :

- ✓ Créé en 1993
- ✓ Laboratoire d'étalonnage de masses accrédité COFRAC selon l'ISO 17025 depuis 1994
  (N° accréditation 2-1292, Portée disponible sur www.cofrac.fr)
- ✓ Statut SCOP depuis le 1er avril 2016

Une équipe de 8 formateurs / consultants :

David BENHAMOU…….	dbenhamou@ct2m.fr
Laure DOMENECH……..	ldomenech@ct2m.fr
Boris GEYNET……..	bgeynet@ct2m.fr
Lise HEGRON……..	lhegron@ct2m.fr
Nicolas GARTNER…….	ngartner@ct2m.fr
Cécilia BOYON……..	cboyon@ct2m.fr
Margaux VITELA…….	mvitela@ct2m.fr
Océane ANTOINE…….	oantoine@ct2m.fr

Centre des Creusets
Route de Lançon
13250 SAINT CHAMAS
04 90 50 90 14
www.ct2m.fr

Le CT2M, Centre Technologique Méditerranéen de Métrologie

Formation / Conseil / Audit

→ Formations sur votre site, sur-mesure, à distance

« Accompagner les laboratoires dans leurs projets Qualité et Métrologie »

Contact : David BENHAMOU dbenhamou@ct2m.fr 06.78.00.10.26

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE
La certification qualité a été délivrée au titre de la catégorie d'action suivante : ACTIONS DE FORMATION

Organisation de comparaisons interlaboratoires (CIL)

« Organiser des CIL conformément à l'ISO 17043 et sous accréditation COFRAC pour les CIL sur l'étalonnage de masses de 1 mg à 20 kg »

Contact : Boris GEYNET bgeynet@ct2m.fr 06.83.94.60.87

cofrac COMPARAISONS INTERLABORATOIRES
N° accréditation 1-7127
Portée disponible sur www.cofrac.fr

Etalonnage de masses pour toutes les classes jusqu'au E2

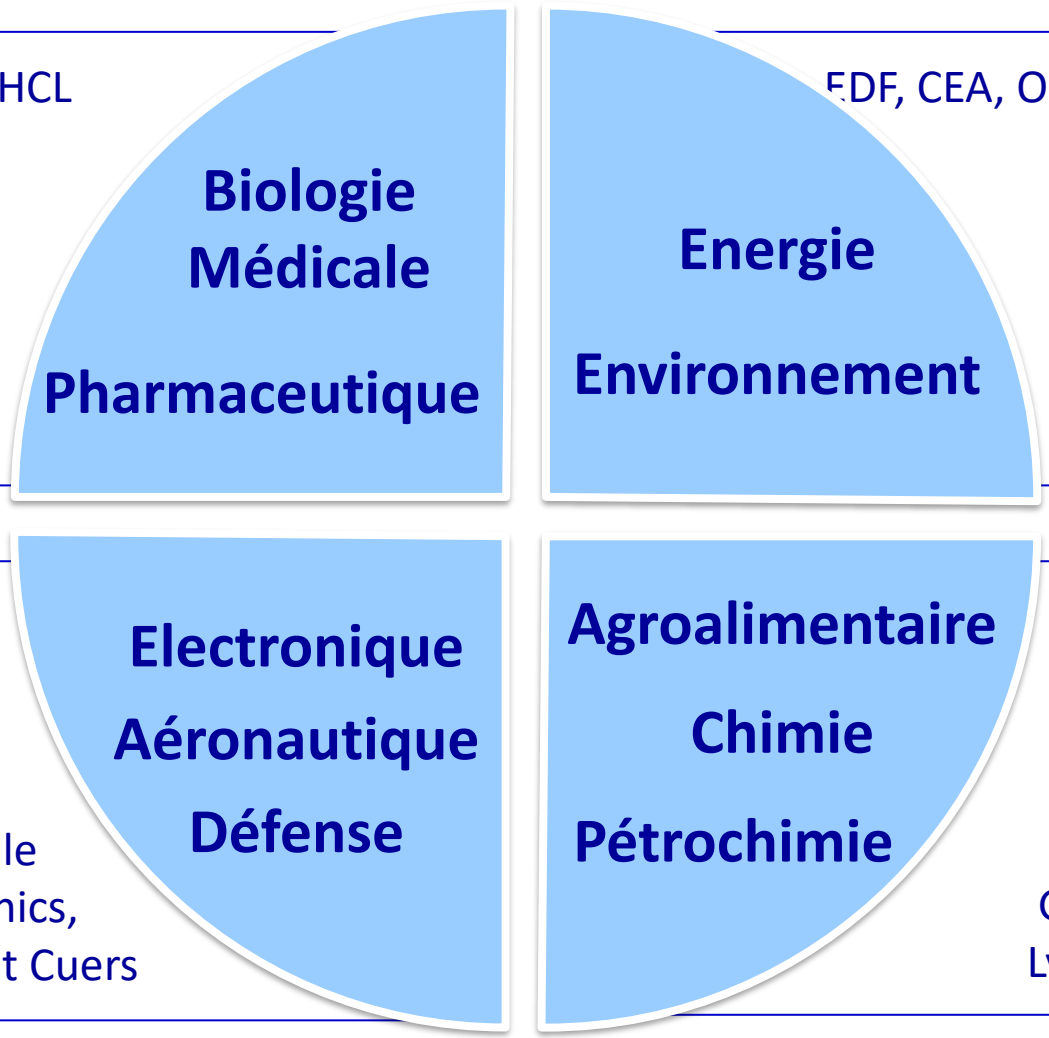
« Etalonner et vérifier des masses de 1 mg à 5 tonnes sous accréditation COFRAC »

Contact : Anaïs LAMOUR alamour@ct2m.fr 04.90.50.90.14

cofrac ÉTALONNAGE
N° accréditation 2-1292
Portée disponible sur www.cofrac.fr

Le CT2M, Centre Technologique Méditerranéen de Métrologie

Ils nous font confiance…



AP-HM, AP-HP, HCL
CHU, LABM
EFS, Bioqualité,
Biosanté,
SANOFI, EDQM
ARKOPHARMA
BIOMERIEUX

EDF, CEA, ORANO, ASNR
EICHROM
MIRION
CARSO
PROTEC
PRONETEC
LDA, SCL

DGA
Airbus
Naval Group
Aviation civile
Marine Nationale
STMicroelectronics,
AIA Ambérieu et Cuers

Total
Nestlé
Arcelor
Coca Cola
Royal Canin
Geogaz, SEPR
Lyondellbasell

- ✓ Les échanges se font par écrit dans le **fil de conversation**
- ✓ Les questions sont abordées **au fil de la présentation**
- ✓ Les **réponses aux questions** sont apportées :
  - Lorsqu'elles concernent le sujet qui est abordé
  - Si elles peuvent intéresser les autres participants
  - En fin de webinar si elles n'ont pas pu l'être avant

La **présentation** sera disponible sur notre site internet :

https://ct2m.fr/communication/petits-dejeuners/

La **vidéo du webinar** vous sera transmise avec un lien disponible 1 semaine uniquement.

II. Déroulement du webinar

Formation ▾ Audit / Conseil ▾ Essais inter-laboratoires ▾ Etalonnage ▾ CT2M

Nos webinars

Les webinars (anciennement « Petits Déjeuners ») du CT2M sont l'occasion de discuter de vos préoccupations présentes et futures sur un thème particulier, en lien avec la métrologie et/ou la qualité.
Ils ont lieu 2 fois par an, courant juin et décembre, et se déroulent toujours un vendredi matin.

Ils sont totalement gratuits et ouverts à tous.

En savoir plus

Les thématiques des webinars passés

Métrologie des enceintes selon le FD X 15140 et évolutions du LAB GTA 24
Décembre 2023

Métrologie des AVAP selon l'ISO 8655 et LAB GTA 90
Juin 2024

Comparaison Inter-laboratoires (CIL)
Décembre 2022

CT2M

LE PARTENAIRE À VOTRE MESURE

Thématique : Comment auditer le système d'information d'un laboratoire accrédité en s'appuyant sur le GEN GTA 02 ?

Webinar du 20/06/25

1. **Les exigences des référentiels d'accréditation**
2. Les généralités du GEN GTA 02
3. Qu'est-ce que l'audit ?
4. Quelques exemples de questions d'audit

- §7.11.1 / §7..2.1 - Le laboratoire / OCIL doit avoir accès aux données et aux informations nécessaires pour réaliser ses activités
- §7.11.2 / §7.5.2.2 – Le laboratoire / OCIL doit **valider** ses systèmes de gestion de l'information (**les fonctionnalités** et le **bon fonctionnement des interfaces)** à la **mise en service** et **après chaque modification** (des configurations ou d'un logiciel) pour :
  - ✓ la collecte,
  - ✓ le traitement,
  - ✓ l'enregistrement,
  - ✓ la transmission,
  - ✓ le stockage,
  - ✓ la récupération de données.

Conserver des preuves des validations

- §7.11.3 / §7.5.2.3 - Les systèmes de gestion de l'information doivent :
  - **Être protégés**:
    - ✓ contre tout accès non autorisé
    - ✓ de **la falsification** et de la perte de données
  - Être utilisés dans un environnement conforme aux spécifications du fournisseur - cas des systèmes non informatisés : conditions protégeant l'exactitude de l'enregistrement manuel et la transcription
  - Être entretenu afin de **garantir l'intégrité des données**
  - **Inclure l'enregistrement des défaillances du système** et les actions associées

    Sauvegardes des serveurs, accès limités par mot de passe ou droit

- §7.11.4 / 7.5.2.4 - Si la gestion est faite **par un prestataire externe**, le laboratoire / OCIL doit s'assurer qu'il respecte les exigences de la norme

- §7.11.5 / §7.5.2.5 – Les documents sur les systèmes de gestion doivent être facilement **accessibles au personnel**

- §7.11.6 / §7.5.2.6 - Les **calculs et le transfert de données doivent être vérifiés** de façon appropriée et systématique

Validation du système (LAB REF 02 / LAB CIL REF 02) :

Action de **confirmer par l'examen de preuves objectives** que les **spécifications** d'un système informatisé :

- **sont conformes aux besoins et attentes des utilisateurs,**
- que toutes les **exigences de la norme** ont été prises en compte.

- §7.6.3 Le ou les systèmes utilisés pour :
  - le prélèvement,
  - le traitement,
  - l'enregistrement,
  - le compte rendu,
  - le stockage,
  - la récupération des données et informations relatives aux examens effectués,

doivent être :

a) - **validés par le fournisseur**

- **vérifiés par le laboratoire** en matière de **fonctionnalité** avant leur mise en service.

Tout changement apporté au système, y compris les modifications concernant la configuration logicielle du laboratoire ou celles concernant un logiciel commercial de série, doit être **autorisé, documenté et validé** avant sa mise en œuvre;

b) être **documentés**, la documentation devant être facilement accessible aux utilisateurs autorisés, y compris celle relative au fonctionnement au jour le jour du système;

c) être mis en œuvre en tenant compte de la **cybersécurité** afin de protéger le système contre tout accès non autorisé et protéger les données contre l'altération ou la perte;

d) être utilisés dans un **environnement conforme aux spécifications** du fournisseur ou, dans le cas de systèmes non informatisés, susceptible de préserver l'exactitude de l'enregistrement manuel et de la transcription;

e) faire l'objet d'une **maintenance** de manière à assurer l'intégrité des données et informations et à inclure **l'enregistrement des défaillances** du système et des actions immédiates et correctives appropriées.

Les calculs et transferts de données doivent être contrôlés de manière systématique et appropriée.

§7.6.4 Plans en cas de panne

Le laboratoire doit avoir des **processus planifiés** pour maintenir l'activité en cas de défaillance ou pendant une panne des systèmes d'information qui affecte les activités du laboratoire. Cela couvre la sélection et l'édition de comptes rendus automatiques des résultats.

7.6.5 Gestion hors site

Si le ou les systèmes d'information du laboratoire font l'objet d'une gestion et d'une maintenance **hors site** ou si celles-ci sont **sous-traitées à un prestataire externe**, le laboratoire doit s'assurer que le prestataire ou l'opérateur du système satisfait à toutes les exigences applicables du présent document.

1. Les exigences des référentiels d'accréditation
2. **Les généralités du GEN GTA 02**
3. Qu'est-ce que l'audit ?
4. Quelques exemples de questions d'audit

2. Les généralités GEN GTA 02
2.1 Définition du système d'information

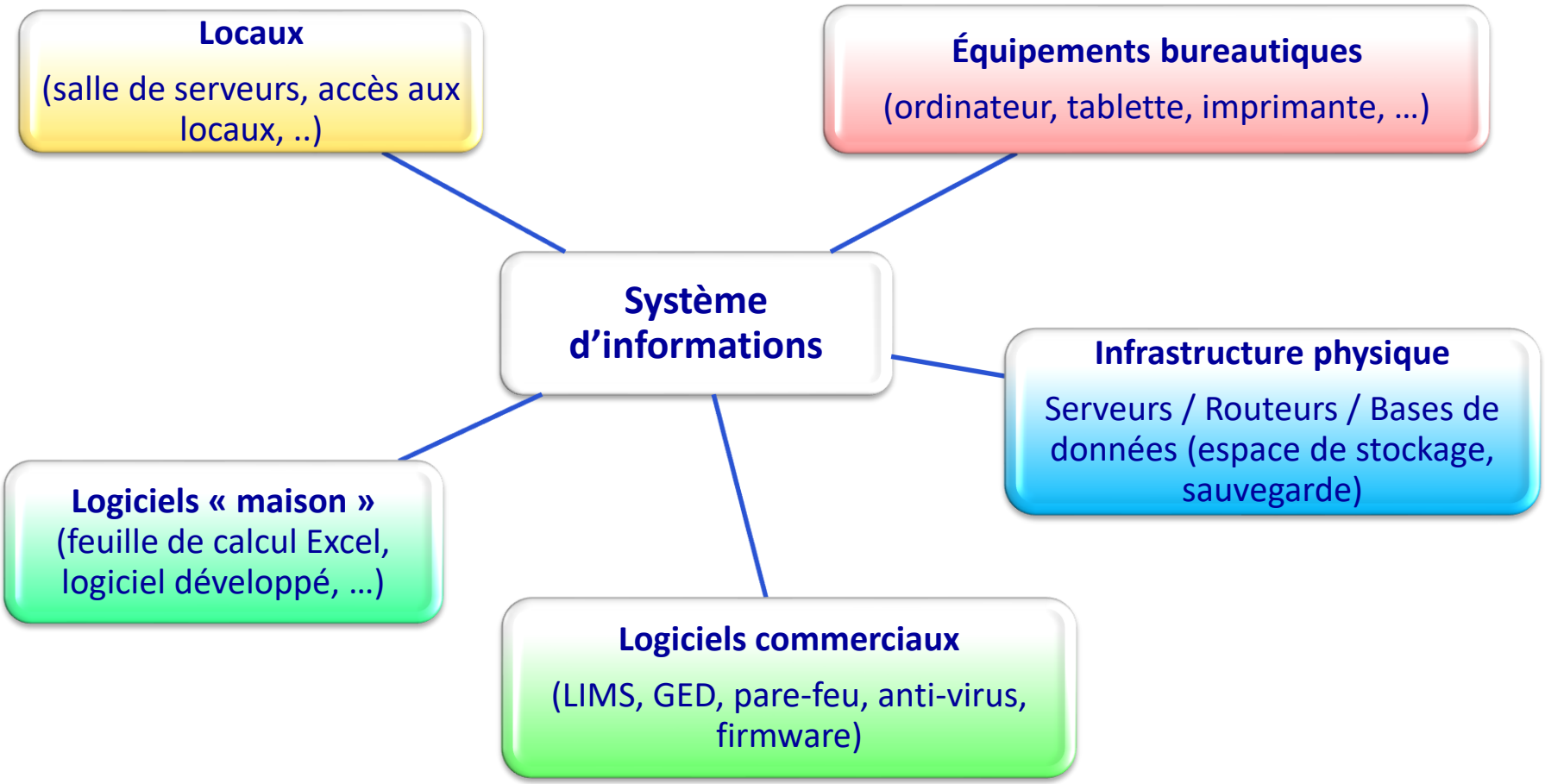
Guide Technique d'Accréditation – Systèmes d'information dématérialisés

Actuellement en révision 01

Ce guide est applicable à compter du 01/06/2024

Ce document s'adresse aux organismes utilisant un ou des systèmes d'information dématérialisés dans le cadre des prestations de leur portée d'accréditation (actuelle ou demandée)

Système d'information : Ensemble des ressources (moyens matériels et humains) destinées à collecter, classifier, traiter, stocker, gérer et diffuser les informations



Cartographie : Représente le système d'information ainsi que ses connexions avec l'extérieur.

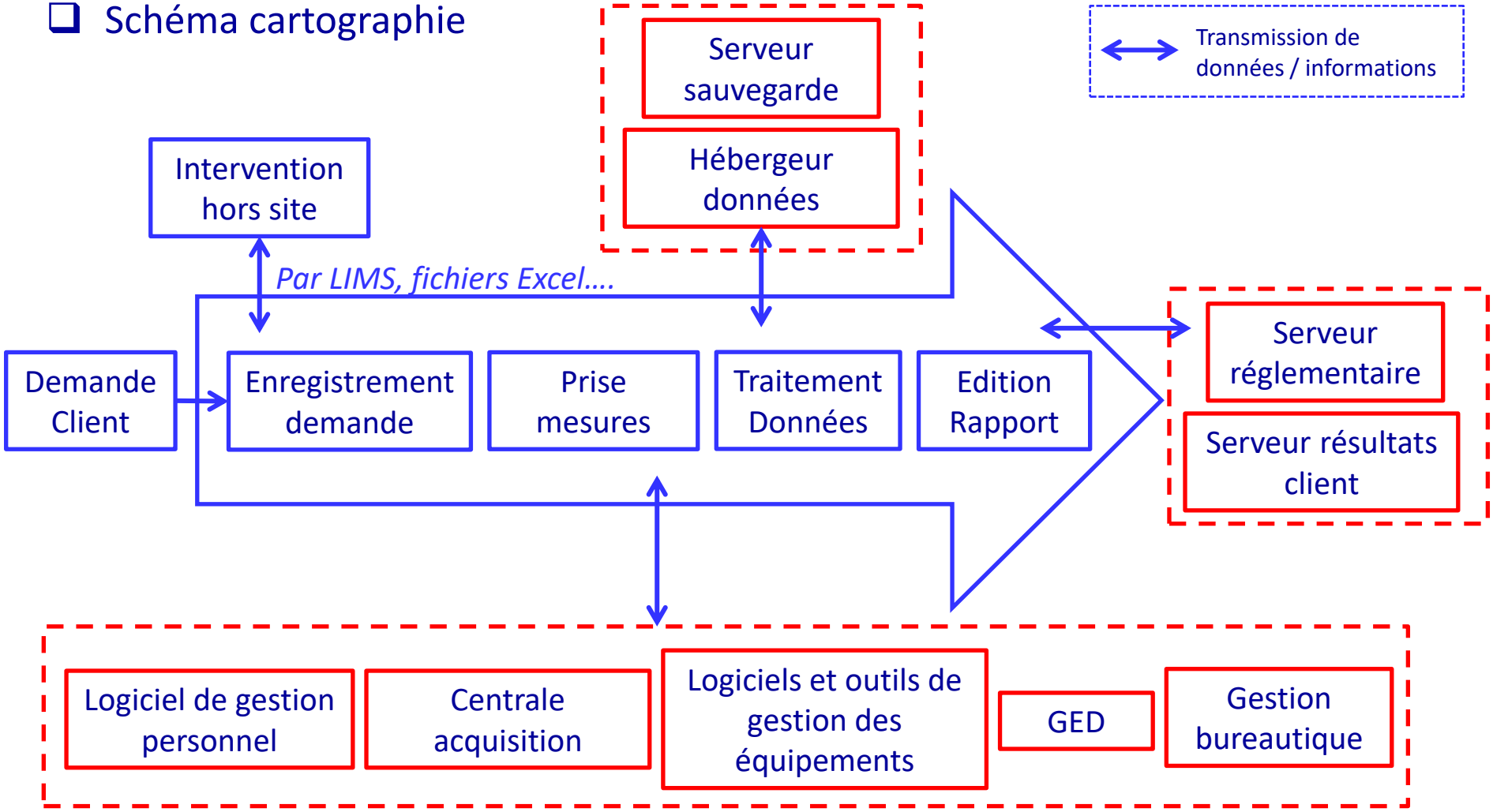
Elle peut inclure : le matériel, les logiciels, les réseaux de connexion, les informations, les activités impactées et les processus concernés…

Objectifs pour le laboratoire :

- ❑ Avoir un outil de pilotage de l'évolution du système d'information
- ❑ Avoir un outil d'identification des systèmes les plus critiques et les plus exposés
  - ➢ Permet d'avoir des mesures adéquates pour traiter ces risques
  - ➢ Permet éventuellement de réagir plus efficacement dans la recherche de cause d'incident

- ❑ Outil pour l'auditeur :
  - ➢ Permet d'identifier les interfaces ou les logiciels les plus critiques que l'on pourra par la suite auditer.

❑ Schéma cartographie



Comment identifier les failles relatives à la sécurité ?

→ Analyse de la sécurité du SI selon 4 critères **DICP** :

- **D**isponibilité : Garantir le bon fonctionnement des outils informatiques pour assurer l'accès aux informations.
- **I**ntégrité : Assurer la qualité des données, dans les temps et espaces prévus.
- **C**onfidentialité : Seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées
- **P**reuve : Garantir la traçabilité suffisante pour tout contrôle et administration de la preuve (traçabilité des actions menées, authentification des utilisateurs, imputabilité du responsable de l'action effectuée).

1. Les exigences des référentiels d'accréditation
2. Les généralités du GEN GTA 02
3. **Qu'est-ce que l'audit ?**
4. Quelques exemples de questions d'audit

L'audit, c'est quoi??

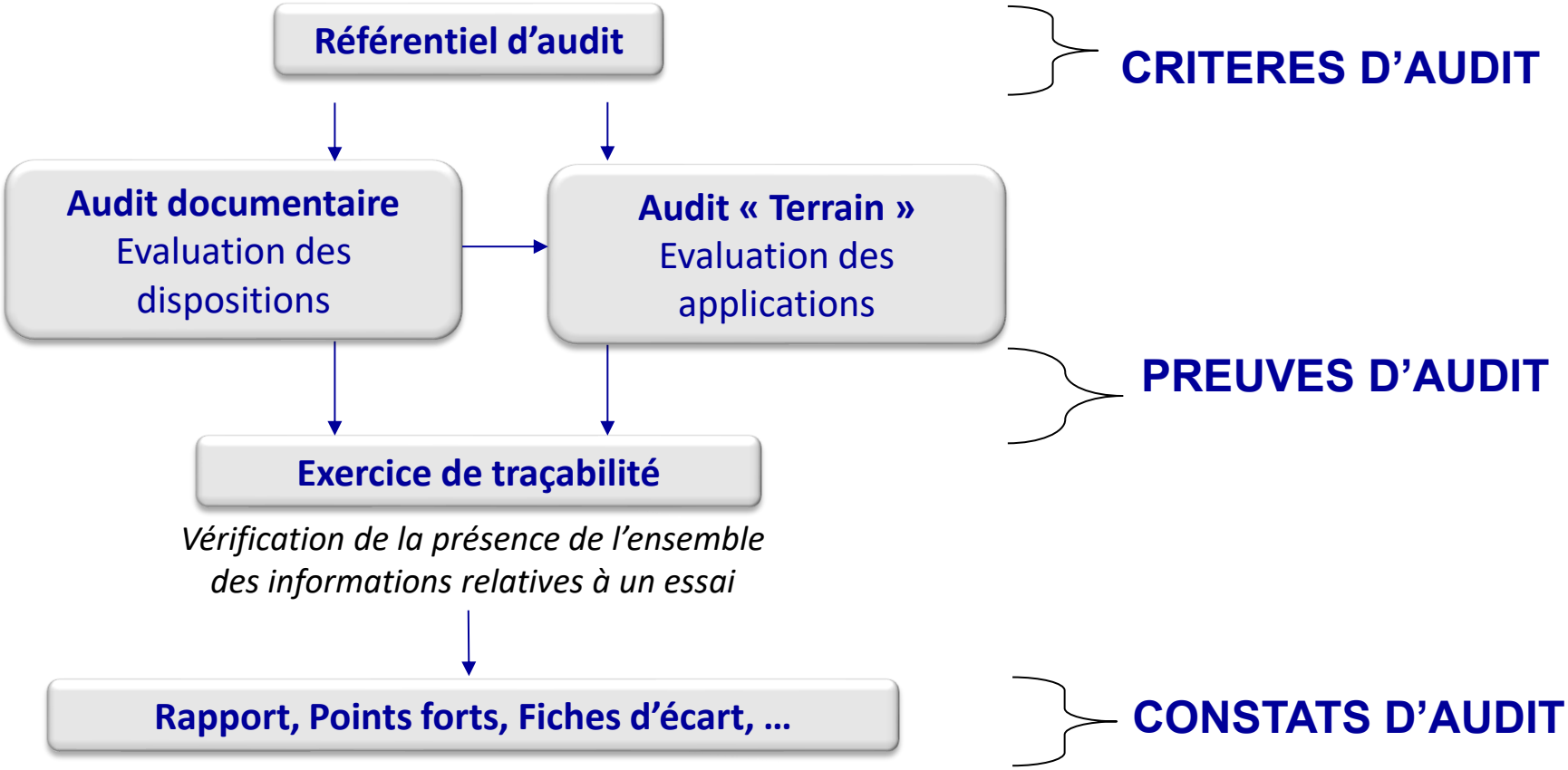
En définition …

AUDIT (*ISO 19011 : lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental*)

Processus systématique, indépendant et documenté en vue d'obtenir des **preuves objectives (preuves d'audit)** et de les évaluer de manière objective pour déterminer dans quelle mesure les **critères d'audit** sont satisfaits.

Référentiels d'accréditation

3. Qu’est-ce que l’audit ?



L’auditeur :

1) Examine la pertinence des **dispositions** par rapport aux exigences du référentiel.

2) Vérifie **l’application** de ces dispositions sur le terrain :

- ✓ en interrogeant le personnel
- ✓ en examinant les enregistrements (= preuves)
- ✓ **en vérifiant que les systèmes mis en place sont fonctionnels**

PREUVES D'AUDIT

- Seules les informations vérifiables constituent des preuves d'audit

  → **Notez les références** de tous les documents présentés !

  … de manière détaillée et systématique lorsque vous avez les documents sous les yeux : ne pas craindre de prendre le temps d'enregistrer les informations utiles

1. Les exigences des référentiels d'accréditation
2. Les généralités du GEN GTA 02
3. Qu'est-ce que l'audit ?
4. **Quelques exemples de questions d'audit**

❑ Question :

- ➢ Comment assurez-vous que seules les **personnes autorisées** ont accès aux infos qui leur sont destinées ?

❑ Exemples de moyens

- ➢ Mise en place d'un système de **protection du réseau**
- ➢ Mise en place d'une politique de **gestion des mots de passe**
- ➢ Pour le personnel de l'organisme :
  - Définition des **droits d'accès**
  - **Engagement** au respect de la confidentialité et de la stratégie de sécurité informatique
  - **Sécurisation des accès distant** (VPN…)
- ➢ Pour les prestataires :
  - **Cryptage / anonymisation** des données accessibles par les fournisseurs
  - Mise en place d'un système de **traçabilité** permettant de formaliser les opérations réalisées
- ➢ Pour les clients :
  - Mise en place de **clauses de confidentialité** dans les contrats, les CGV, les conventions de preuves

❑ Question

- Comment s'assurer de l'intégrité des données (exactes, lisibles, contemporaines…) ?

❑ Exemples de moyens

- **Formation** des utilisateurs concernant la sécurité/intégrité des données
- Définition des **droits informatiques** en lien avec le niveau de responsabilité/qualification des personnel
- Mise en place d'historiques dans les logiciels pour le **suivi des modifications**
- Mise en place de **protections** contre les logiciels malveillants
- Mise en place de systèmes de **chiffrement des données**
- Réalisation de **tests d'intégrité des données**
- Réalisation de **tests de récupération de données**

❑Question

- ➢Comment gérez-vous la **sauvegarde** du système d'information de l'organisme ?

❑Exemples de moyens

- ➢ Mise en place d'une **stratégie de sauvegarde**
- ➢ Suivi du **planning de sauvegarde**
- ➢ Mise en place de moyen pour **éviter que les données sauvegardées soient inexploitables**
- ➢ Mise en place de conduites à tenir en **cas de panne**
- ➢ Détermination de **Plan de Reprise d'Activité (PRA)** ou de **Plans de Continuité d'Activité (PCA)**

❑ Question

- ➢ Comment faites vous pour que les données numériques sont **conservées durant les durées définies ?**

❑ Exemples de moyens

- ➢ Définition des **supports d'archivage** en fonction de leur pérennité dans le temps
- ➢ Définition et **sécurisation des supports** (incendie, inondation, rongeurs…)
- ➢ Mise en place de modalités pour s'assurer que les données archivées vont **rester lisibles** même après l'arrêt d'un logiciel
- ➢ Définition des **durées d'archivage**
- ➢ Définition des **droits d'accès**
- ➢ Vérification de l'**intégrité** des archives

❑ Question

- ➢ Comment s'assurer que les prestataires externes répondent aux besoins identifiés ?

❑ Exemples de moyens

- ➢ Définition des **besoins** de l'organisme et des **exigences** applicables au prestataire externe dans contrat, convention, CdC… (confidentialité, tâches, outils de communication, modalité de connexion, traçage des tâches…)
- ➢ Réalisation d'une **évaluation**

NB : Les services informatiques internes à l'organisme sont à considérer comme des prestataires externes selon l'ISO 17025.

❑ Question

- ➢ Comment avez-vous validé votre système d'information ?

❑ Exemples de moyens

- ➢ La validation peut consister à vérifier la **qualité** des données primaires, secondaires, métadonnées, l'**intégrité** et **confidentialité** des données
- ➢ La vérification que les exigences sont atteintes en réalisant un **dossier test** avec des résultats attendus, de **tests de connexions**, une **validation des calculs** par comparaison à des résultats attendus, une vérification des **droits d'accès par profil**
- ➢ La vérification que les exigences sont maintenues en réalisant un **dossier tests** avec des résultats attendus, des **tests de connexions**, une **vérification des calculs par échantillon**nage, des **droits d'accès par profil**, des **tests de restauration** des données

Etude de cas n°1

- Les incidents liés aux outils du Système d'Information (SI) du laboratoire sont enregistrés et traités via un outil dédié géré par la Direction Informatique (prestataire externe)
- Le laboratoire peut déclarer des incidents sur cet outil et consulter l'état d'avancement du traitement.
- Il n'a pas les droits d'accès pour faire une extraction des incidents qu'il a déclaré
- De ce fait, aucun bilan des incidents liés au SI n'est présenté lors de la Revue de Direction

Cette situation est-elle acceptable ?

Etude de cas n°2

- Le laboratoire gère les accès à son Système d'Information (SI) et les droits associés à chaque profil.
- Des prestataires externes ont également accès à ce système d'information et pour chaque personne intervenant chez ses prestataires externes, un accès est créé avec un mot de passe unique par personne.
- Cependant, le laboratoire ne tient pas à jour une matrice des profils et des droits pour chaque fonction définie dans son organisation. L'information est disponible dans le profil numérique de chaque personne. Il préfère gérer les accès au cas par cas, car seule une dizaine de personnes ont un profil dans le SI.

Cette situation est-elle acceptable ?

LE PARTENAIRE À VOTRE MESURE

Nos formations sur le sujet :

Inscriptions : *ct2m@ct2m.fr*

Formation	Dates en INTER
Q2 – Devenir auditeur interne selon l'ISO 17025	Du 6 au 10 octobre 2025 (4 j)
Q15 – Gestion du système d'information selon le GEN GTA 02 et validation des fichiers de calculs	30 septembre 2025 (1 j)
Q18 – Savoir auditer le système d'information d'un laboratoire accrédité	Du 1er au 2 octobre 2025 (1,5 j)