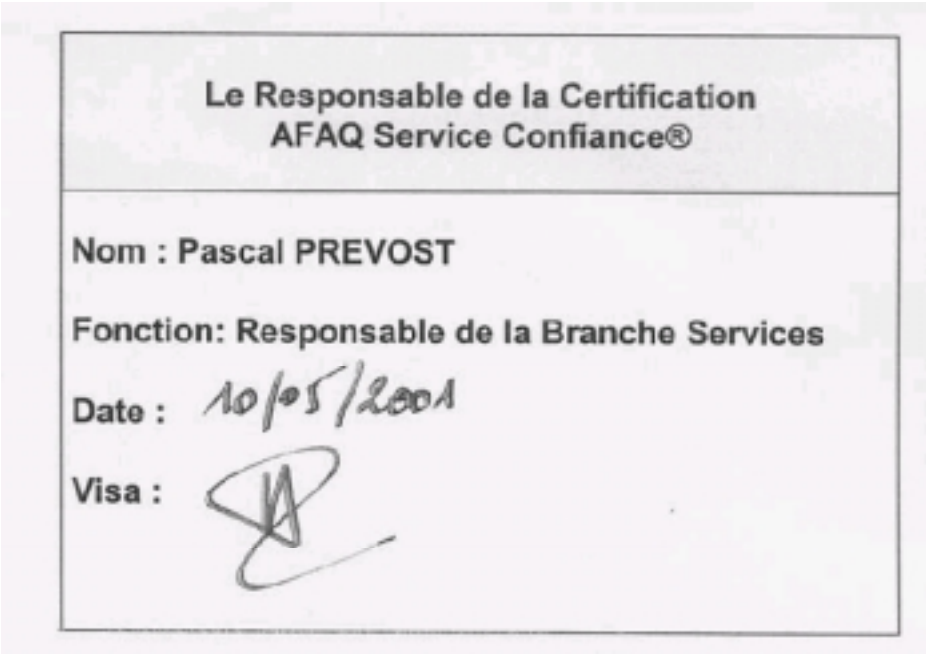
PLAN DE CONTROLE EXTERNE DU REFERENTIEL AFAQ Service Confiance

REF –118 – 01

Sauvegarde à distance de données numériques

REFERENCE : PCE-118-01
30/03/2001



1. Définition et objectif du plan de contrôle externe

Le présent plan de contrôle externe s'inscrit dans le cadre de la certification de service définie par les articles L. 115-27 à L. 115-33 et R. 115-1 à R. 115-12 du Code de la Consommation.

L'objet du plan de contrôle externe est de définir les modalités d'attribution et de maintien du certificat AFAQ Service Confiance® par l'organisme certificateur pour l'activité de **sauvegarde à distance de données numériques** définie dans le référentiel **REF-118-01*.***

Le plan de contrôle externe décrit :

- les étapes de certification
- les méthodes de contrôle utilisées par AFAQ pour la réalisation des audits.

L'audit initial de certification et les audits de suivi permettent de contrôler le respect de l'ensemble des engagements de service et dispositions définis dans le référentiel.

2. Attribution et maintien du certificat AFAQ Service Confiance®

2.1 - Etude de la candidature

Personnel Permanent AFAQ

Toute entreprise candidate à la certification de service dépose une demande de certification auprès de l'organisme certificateur.
Le dossier de candidature comporte :

- Un engagement de l'entreprise à prendre connaissance et à respecter les modalités de certification, portant notamment sur le fait, à la date de l'audit :
  - D'être en mesure d'apporter la preuve de l'application des engagements de service sur une période de **3 mois minimum** avant l'audit initial. Cette disposition ne concerne pas les engagements dont la fréquence d'application est supérieure à la durée minimum définie. Toutefois, l'entreprise doit apporter la preuve que leur mise en œuvre est définie et planifiée.
  - D'avoir réalisé un audit interne portant sur l'ensemble du référentiel (engagements et dispositions d'organisation).

- Une « fiche contact » reprenant des informations sur l'entreprise et son organisation.

- La liste récapitulative des sites concernés reprenant les interlocuteurs, leurs coordonnées et les conditions d'accès dans le cas d'une certification multisite)

- La liste des documents et des enregistrements relatifs à chaque engagement.

Une analyse de la recevabilité de la demande de certification de l'organisme est effectuée sur la base de son dossier de candidature.

2.2 - Audit initial de certification

L'audit est réalisé par un **auditeur ICA** qualifié par **AFAQ**, choisi en fonction de son expérience du secteur d'activité et formé spécifiquement à l'audit AFAQ Service Confiance® .

Auditeurs formés et qualifiés par AFAQ

La durée d'audit est liée à la taille de l'organisme et des sites concernés.

L'audit initial porte sur les points suivants :

- Respect des engagements de service,
- Mise en œuvre des dispositions d'organisation, de suivi et de pilotage garantissant le respect des engagements,
- Examen des résultats des enquêtes de satisfaction clients

Les critères de contrôle sont repris pour chaque engagement et disposition de suivi et pilotage dans les tableaux pages 5 à 17.
S'il le juge utile pour réaliser sa mission, l'auditeur peut compléter les critères de contrôle définis dans le présent plan de contrôle externe.

Les méthodes de contrôle sont définies par l'auditeur pour chacun des critères des contrôles parmi les méthodes suivantes:

- Entretien avec le personnel afin de s'assurer que les engagements et les dispositions sont connues et comprises par le personnel concerné.
- Contrôle visuel, constat attestant de la présentation de documents ou d'éléments définis dans le référentiel
- Examen des indicateurs qualité afin de s'assurer de la régularité dans le respect des engagements.
- Examen documentaire des documents de référence et des enregistrements correspondants.

A l'issue de l'audit, le *responsable d'audit* élabore le rapport d'audit et remet à l'entreprise, s'il y a lieu, des fiches de remarques et/ou non-conformités appelant une réponse de l'entreprise.

2.3 - Prise de décision

Le responsable d'audit soumet son rapport d'audit à un groupe d'Experts Service.

Auditeurs formés et qualifiés par AFAQ

Les Experts Service sont issus des Comités de Certification d'AFAQ. Ils sont formés à la certification de service et sont retenus en fonction de l'adéquation entre leur secteur de compétence et le domaine d'application du référentiel.

AFAQ / Experts

Le groupe d'Experts Service examine le rapport d'audit et propose une décision.

La Fonction certification AFAQ délivre la certification, sur avis du groupe

d'Experts Service, pour une durée de 3 ans.

2.4 - Maintien de la certification

AFAQ réalise, durant la période de validité du certificat, 2 audits de suivi selon les mêmes modalités que l'audit initial.

Auditeurs formés et qualifiés par AFAQ Personnel Permanent AFAQ

Chaque audit de suivi porte sur les points suivants :

- respect des engagements de service,
- dispositions d'organisation, de suivi et de pilotage du respect des engagements,
- respect des modalités de communication définies dans le référentiel et dans le règlement d'utilisation de la marque AFAQ Service Confiance® .
- résultats des enquêtes de satisfaction client et mise en œuvre des plans d'actions correspondant,
- dispositions mises en place suite à la détection d'un écart lors d'un audit précédent.

Après chaque audit de suivi, le dossier de maintien de la certification est analysé par AFAQ sur la base du rapport d'audit et de la proposition du responsable d'audit.

3. Critères de contrôle des engagements :
Les tableaux suivants reprennent les engagements, les dispositions d'organisation, de suivi et pilotage et les critères de contrôle (les documents et les enregistrements à examiner sont signalés en caractère gras) :

Engagement de service	Critères
1 Un prestataire de service parfaitement identifié.	▪ Présence sur tous les **contrats de service** de l'identification du prestataire avec les informations ci-dessous : - nom commercial, - adresse géographique de son siège social, - nom de l'entité juridique responsable des échanges de données, - adresse géographique complète où un représentant du prestataire peut-être joint, - jours et horaires d'accueil téléphonique ; durant ces périodes, l'accueil ne peut être assuré par un répondeur, - numéros d'enregistrements légaux ou professionnels, - adresse électronique, - numéro d'enregistrement TVA. - nom des personnes habilitées à avoir accès aux informations suivantes : contenu du contrat, nature des données à sauvegarder, modalités de sauvegarde, clés de chiffrement, données elles-mêmes. ▪ Présence sur le **contrat de service** de la mention suivante : « *Le prestataire garantit qu'en aucun cas les informations du client ne seront accessibles à qui que ce soit sans son autorisation expresse* ». et de la référence aux articles 323-1 à 323-7 du code pénal traitant des atteintes aux systèmes de traitement automatisé de données. ▪ Classement des contrats de service dans les **dossiers clients.** ▪ Information dans le **contrat de service** et **accord écrit** du client en cas d'intervention d'un sous-traitant.

Engagement de service	Critères
2 Une description précise de la prestation proposée dans un contrat de service en termes d'obligation de résultat par le prestataire	▪ Présence dans les **contrats de service** du descriptif de la prestation avec au minimum les éléments suivants : - Identification du système à sauvegarder. - Identification des données à sauvegarder (taille, organisation...). - Dates et horaires des sauvegardes ou fréquence. - Engagement de restauration des données. - Obligations contractuelles du client et du prestataire. - Définition de la prestation et en garantir l'exécution dans le cadre d'un contrat de service. - Traçabilité de l'exécution de la prestation en apportant les preuves, étape par étape. - Engagement de performance de réalisation de sauvegarde (immobilisation de la donnée) et de restauration en fonction du volume. - Description des résultats de l'exécution dans un document référencé dans le contrat, selon une périodicité à définir avec le client. - Information du client en temps réel de tout événement concernant l'exécution de la prestation. - Mesure régulière de l'exécution de la prestation (comptes rendus d'exécution des sauvegardes et des restaurations), selon une périodicité à définir avec le client. - Référence au présent référentiel qui lui est annexé. - Engagement de restitution des données au client à l'expiration du contrat de service et engagement de destruction des données archivées sur le site du prestataire à la fin du contrat de service ▪ Classement des contrats de service dans les **dossiers clients.**

Engagement de service	critères
3 Une description précise des moyens mis en œuvre par le prestataire pour atteindre les objectifs de résultat définis dans le contrat de service.	▪ **Présence dans les** contrats de service **du descriptif des :** · moyens mis en œuvre pour assurer la prestation (moyens techniques et humains, garanties en terme de sécurité des équipements et description des composants techniques). · des menaces que doit contrer le système du prestataire, des mesures de sécurité prévues et justification de leur adéquation aux menaces potentielles. · de l'engagement du prestataire à faire bénéficier son client des progrès technique permanents dans le domaine de l'informatique et des télécommunications ● Moyens humains : -Correspondant nommément désigné par le prestataire pour répondre aux sollicitations du client. ● Moyens matériels : - Système informatique de l'abonné comprenant notamment un ou plusieurs disques. - Réseau numérique de communication. - Système central de sauvegarde comprenant deux sites géographiques distincts reliés par un réseau numérique de communication : - Système de traitement des données transmises. - Système d'archivage comprenant des mémoires de masses de grande capacité. - chiffrement (cryptage) ● Moyens logiciels : - Anti-virus dans le système informatique du client. - Chiffrement (cryptage). - Compression des données. - Sauvegarde automatique. ▪ Classement des contrats de service dans les **dossiers clients.**

Engagement de service	critères
4 Un stockage de vos données chiffrées (cryptées) dans un lieu sûr.	▪ Vérification visuelle des moyens de stockage pour mettre en mémoire les données traitées (par l'intermédiaire d'un robot ou d'un automate de gestion de cartouches magnétiques, par un système de gestion mécanique de multiples disques (juke-box)). ▪ stockage des données traitées dans une chambre forte du type de celles qui sont utilisées dans le domaine bancaire. Cette chambre forte est adaptée à résister à de nombreuses agressions et elle est dotée d'alarmes et de moyens de surveillance. ▪ formalisation des **dispositions internes** ci après et vérification de leur application : en dehors des opérations d'installation ou de maintenance, aucune personne n'est habilitée à pénétrer dans la chambre forte. ▪ formalisation des **dispositions internes** ci après et vérification de leur application : les fichiers à sauvegarder font l'objet d'une opération de chiffrement avec un système de chiffrement à clé publique ou privé conforme à la législation en vigueur. *(L'opération de chiffrement consiste à substituer à un ensemble de données que l'on veut protéger un texte inintelligible pour quiconque ne connaît pas l'algorithme et les paramètres de chiffrement.)*
5 Une hot-line client pour répondre à toutes vos attentes.	▪ mise à disposition des clients d'une hot-line, accessible selon des horaires et des modalités précisés dans le contrat de service, afin de répondre à toutes questions et sollicitations des clients concernant la prestation. ▪ Vérification dans le **contrat de service** du délai fixé pour résoudre tout dysfonctionnement intervenant dans le déroulement de la prestation.(Le délai d'intervention ne doit excéder 12 heures). Présence dans **le dossier client** de la copie d'un fichier informatique précisant l'heure de début de l'intervention, l'heure de fin ainsi que la nature de l'intervention. ▪ Enregistrement des appels horodatés des clients dans une base de données ; ▪ Enregistrement des réponses horodatées apportées à un appel client.

Engagement de service	critères
6 Une analyse systématique et régulière de vos besoins.	▪ Mise en place d'un dispositif d'analyse systématique et régulier des besoins des clients (**questionnaire d'évaluation** de leurs besoins selon une périodicité annuelle ou entretien personnalisé régulier ou contact sur site ou revue de contrat initial). ▪ Présence et application de **dispositions internes formalisées** en matière d'évaluation des besoins clients. ▪ Enregistrement des **questionnaires datés envoyés aux clients, des réponses des clients, des comptes rendus d'entretien clients**. ▪ **analyse et traitement et enregistrement** des besoins clients permettant d'optimiser les prestations .
7 Une réponse à vos réclamations en 48 heures maximum.	▪ Présence et application de **dispositions internes formalisées** en matière de gestion des réclamations des clients. ▪ Examen du **taux de réponse écrite** aux réclamations dans les 48 heures. Mise en place en place d'un **plan de progrès annuel** formalisé pour améliorer ce taux. ▪ Enregistrement des réclamations des clients et des réponses apportées dans **une base de données** (les réclamations sont horodatées). ▪ Analyse et traitement des réclamations ayant pour objectif d'apporter une solution au problème posé. Examen des **enregistrements correspondants (**courriers de réclamation clients, courriers de réponse du prestataire)

Engagement de service	Critères
8 Une évaluation régulière de la satisfaction des clients.	▪ Présence et application de **dispositions internes formalisées** en matière de satisfaction des clients. Prise en compte dans le **questionnaire d'enquête** des engagements de service, réalisation de l'enquête selon un panel représentatif. ▪ Périodicité de ces enquêtes précisée dans le **contrat de service**, à savoir tous les 6 mois au minimum. ▪ Analyse des points forts et des points faibles , mise en œuvre et le suivi **d'un plan d'amélioration.** ▪ Conservation des enquêtes de satisfaction envoyées aux clients et des résultats d'enquête de satisfaction.

Engagement de service	Critères
9 Un interlocuteur unique par client.	▪ Désignation dans le **contrat de service** du correspondant privilégié pour chaque client. (nom, adresse, n° de téléphone, n° de fax, adresse e-mail, heures de présence, boîte vocale en cas d'absence). ▪ Examen des **dossiers clients**.
10 Un respect systématique des délais.	▪ Présence dans chaque **dossier client** de la copie d'un fichier informatique précisant pour chaque opération l'heure de début de la prestation ainsi que sa durée. ▪ Mise en place et suivi d'un **indicateur de performance** relatif au respect des délais (nombre mensuel d'interventions hors délais contractuels). Mise en place d'un **plan de progrès annuel** formalisé pour améliorer ce taux.
11 Un service disponible en permanence.	. ▪ Examen des **résultats de l'enquête de satisfaction** de la disponibilité du service 24 heures sur 24 et 7 jours sur 7. ▪ Information immédiate du client en cas d'indisponibilité du service afin de ne pas perturber le déroulement de la prestation de service : examen des messages (E-mail, fax, tél. …) enregistrés adressés aux clients ▪ Mise en place un indicateur de performance relatif à la disponibilité de son service **(taux mensuel d'indisponibilité du service).** Mise en place d'un **plan de progrès annuel** formalisé pour améliorer ce taux.

Engagement de service	Détail de l'engagement
12 Un personnel compétent et régulièrement formé à votre service.	▪ Mise à disposition d'un **document d'information** sur les systèmes exploités destiné au personnel du prestataire. ▪ Existence d'un **plan de formation** pour chaque poste de travail et **enregistrement** du cursus suivi pour tout titulaire d'un poste de travail et des formations suivies par les personnels. ▪ Formation de tout nouveau personnel sur les engagements du présent référentiel : examen **des attestations de formations**. ▪ Existence d'un **engagement de confidentialité signé** par chaque membre du personnel.
13 Une information systématique du client sur l'exécution de la prestation de sauvegarde.	▪ Envoi d'un **compte-rendu d'exécution** à l'issue de chaque opération de sauvegarde des données du client , ce compte rendu précise : ● le résultat de la sauvegarde, ● le résultat de l'éventuelle détection de virus, ● le résultat de l'éventuelle décontamination, ● la fin des opérations de réception des fichiers, ● la liste des fichiers sauvegardés, ● les heures de début et de fin de la sauvegarde. ▪ Examen des **dossiers clients**. ▪ Envoi du **compte rendu** par tout moyen précisé dans le contrat de service en accord avec le client (fax, e-mail, message émis par le système de sauvegarde sur l'imprimante du client). ▪ Information du client lorsque les fichiers devant être sauvegardés sont stockés dans le centre de sauvegarde du prestataire, cette information se fait par tout moyen précisé dans le contrat de service en accord avec le client (appel téléphonique, **fax, e-mail, message émis** par le système de sauvegarde sur l'imprimante du client).

Engagement de service	Critères
14 Une information immédiate du client, sous forme de message d'alerte, en cas de détection de virus, sur son site, dans ses fichiers	▪ information immédiate du client si un virus a été détecté dans ses fichiers. ▪ Cette information se fait par tout moyen précisé dans le contrat de service en accord avec le client (fax, e-mail, message émis par le système de sauvegarde...), examen des **enregistrements** correspondants. ▪ mise en œuvre de fonctions de décontamination des données du client à sa demande. Examen des **comptes rendus d'incident**. ▪ Arrêt des opérations de sauvegarde en cas de détection d'un virus sur le site du client. Examen des **comptes rendus d'incident**.
15 Une information immédiate du client, sous forme de message d'alerte, en cas de détection d'incident ou d'anomalie.	▪ Information dans les 2 heures du client dans l'hypothèse où un incident ou une anomalie survient au cours de la sauvegarde par tout moyen précisé dans le contrat de service en accord avec le client (fax, e-mail, message émis par le système de sauvegarde sur l'imprimante du client). Examen des **enregistrements correspondants (**dossier client, compte-rendu d'incident).
16 Une évaluation régulière des prestations réalisées par un organisme indépendant.	▪ Vérification de conformité réalisée dans un délai d'un mois après démarrage de la prestation, par un organisme indépendant afin de vérifier si la prestation respecte les engagements du présent référentiel. Examen des **comptes rendus d'évaluation**. ▪ Vérification de conformité chez le client à fréquence semestrielle des prestations de service de sauvegarde à distance réalisée par le même organisme indépendant . ▪ Présence d'un **relevé des écarts** éventuels. ▪ Diffusion du résultat de chaque vérification de conformité au client ainsi qu'au prestataire. ▪ aucune facturation de la vérification de conformité pour le client.

Engagement de service	Critères
17 Une restauration de vos données à la demande	▪ restauration des données du client sur sa demande. Examen des enregistrements correspondants dans les **dossiers clients**. ▪ Examen des **résultats des enquêtes** de satisfaction.

N°	DISPOSITION D'ORGANISATION, DE SUIVI ET PILOTAGE	CRITERES
1	Définition des responsabilités	▪ **définition écrite** des responsabilités de toute personne dont l'activité a une incidence sur le respect des engagements de service dans un **organigramme**, ainsi que dans les **définitions de fonctions correspondantes.** ▪ Désignation par le prestataire d'un Rssi (Responsable Sécurité des Systèmes d'Information) : ses autres responsabilités, s'il en a, ne doivent pas d'interférer avec la Sécurité des Systèmes d'Information ▪ Description précise dans le **contrat de service** de sauvegarde / restauration de la prestation afin de retracer fidèlement l'exécution des processus techniques mis en œuvre. ▪ **Engagement de confidentialité** du prestataire pour les données qui lui sont confiées par engagement avec mise en œuvre d'une application informatique nécessaire à la protection des données confiées et des mesures adaptées au contrôle de la fiabilité des matériels et des logiciels, de la capacité de résistance aux atteintes accidentelles ou volontaires.

N°	DISPOSITION D'ORGANISATION, DE SUIVI ET PILOTAGE	CRITERES
2	Organisation documentaire	▪ Présence de **documents de référence** servant à mettre en œuvre les différents éléments du référentiel et d'enregistrements apportant la preuve de cette mise en œuvre.(Les principaux documents et enregistrement sont définis dans le chapitre IV, au regard de chaque engagement de service concerné). ▪ Mise à disposition du personnel réalisant le prestation de service des documents suivants : ● Document d'exploitation précisant les modalités techniques de fonctionnement des systèmes mis en œuvre pour réaliser la prestation. ● Contrat de service ● Dossier nominatif par client précisant les contraintes spécifiques à chaque client ● Planning d'exécution des opérations de sauvegarde ● Document de suivi des opérations de sauvegarde dans lequel sont consignés tous les événements concernant la sauvegarde ● Document de suivi des opérations de restauration dans lequel sont consignés tous les événements concernant la restauration ▪ **impression de fichiers « log »** dans le cadre de la traçabilité de l'exécution des différentes opérations techniques automatisées. ▪ Définition et respect des dispositions de gestion des documents en matière de rédaction, diffusion et mise à jour. ▪ Information sans délai du client de toute modification des dispositions prises dans le cadre du référentiel (changement de personne, d'organisation, de matériels, de logiciels…) , accompagnée des justifications nécessaires établissant que cette modification n'amoindrit pas la sécurité, examen des **courriers clients**. ▪ Présence de la **liste des enregistrements** et leurs **modalités de gestion**.

N°	DISPOSITION D'ORGANISATION, DE SUIVI ET PILOTAGE	CRITERES
3	Formation du personnel	▪ formation concernant les engagements relatifs au présent référentiel assurée dans le cadre d'une structure spécialisée dans le domaine de la sécurité des systèmes d'information. ▪ Vérification et maintien des compétences requises du personnel pour réaliser les tâches dont il a la responsabilité, ▪ information diffusée de manière approprié au sein de l'entreprise prestataire, ▪ réalisation des formations nécessaires afin de favoriser le maintien du respect des engagements. ▪ mise en œuvre d'un plan annuel de formation portant sur les exigences ci-dessus et plus particulièrement : - l'accueil téléphonique pour la mise en œuvre des garanties, du traitement des réclamations et erreurs de l'offre de service après-vente, - la formation de tout nouveau personnel sur les engagements relatifs au présent référentiel, ▪ enregistrement des formations .
4	Audits internes	▪ réalisation d'un audit interne deux fois par an (dont un avant l'audit de certification) avec vérification du respect : - des engagements, - des dispositions d'organisation décrites dans le présent référentiel. ▪ établissement du **programme d'audit** et désignation des auditeurs internes par le responsable qualité.(Ces audits sont réalisés par des personnes qualifiées et indépendante de l'activité auditée). ▪ réalisation d'une formation à l'audit pour les auditeurs internes. ▪ Utilisation de supports définis. ▪ Elaboration, mise en œuvre et suivi d'un **plan d'amélioration** par le responsable qualité en cas d'écarts lors de l'audit.

N°	DISPOSITION D'ORGANISATION, DE SUIVI ET PILOTAGE	CRITERES
5	Enquêtes de satisfaction clients	▪ réalisation d'enquêtes de satisfaction au moins **2 fois par an** .voir les critères de contrôle de l'engagement n°8.
6	Traitement des réclamations clients	▪ Définition et application de **dispositions de traitements des réclamations clients**. ▪ Toute réclamation fait l'objet d'un enregistrement puis d'une réponse écrite dans un délai de **48 heures**.
7	Bilans annuels	▪ Réalisation d'un bilan au moins **1 fois par an**. Ce bilan a pour objet : ● d'examiner l'ensemble des données reflétant la qualité de ce service et le respect des engagements à partir de l'analyse : ■ des indicateurs mis en place : ◆ taux de réponse aux réclamations dans les délais, ◆ taux mensuel d'indisponibilité du service, ◆ nombre mensuel de dysfonctionnements, ◆ nombre mensuel d'interventions hors délais contractuels ■ des enquêtes de satisfaction, ■ des audits internes, ■ des réclamations, ■ des besoin en formation. ● de fixer des **plans d'actions** correspondants fixant les mesures correctives qu'il convient d'entreprendre pour remédier aux écarts constatés. ▪ Diffusion du **bilan annuel** à l'ensemble du personnel concerné.