Version	Révision	Modification	Rédigé par	Approuvé par
05	07.2024	Mise à jour du document : Relecture par la CNPD, Ajout d'un critère dans le rapport annuel	SCS	ZES
04	07.2024	Mise à jour du document : Relecture par la CNPD, Précision du délai de traitement des réclamations et appels Précision de l'accessibilité des informations relatives quant aux traitements des réclamations et appels Précision des critères d'informations relatifs à la suspension et au retrait d'un membre Précision sur l'audit de suivi anticipé Mise à jour des modalités d'acceptation de la mission d'audit	SCS	ZES
03	05.2024	Mise à jour du document : Relecture par la CNPD, Précision auditeurs externes Mise à jour des définitions Ajout de logigrammes sur le traitement des réclamations et des appels Ajout d'un chapitre « Communication avec la CNPD »	SCS	ZES
02	03.2024	Mise à jour du document : Relecture par la CNPD, Ajout de définitions, Ajout d'une analyse de risques	SCS	ZES
01	06.2023	Création du document	SCS	ZES

1 OBJET

Cette procédure décrit le déroulement d'un audit de suivi du code de conduite RGPD du FSI pour le secteur du travail intérimaire par ESCEM.

2 DOMAINE D'APPLICATION

La présente procédure est applicable à tous les auditeurs ainsi qu'au comité de certification d'ESCEM.

3 DEFINITIONS ET ABREVIATIONS

FSI	Abréviation de « Fonds de formation Sectoriel pour l'Intérim » ; organisme chargé notamment de gérer les budgets de formation du personnel permanent et intérimaire des entreprises du secteur. Le FSI est investi du rôle de porteur du Code de Conduite.
ETI	Abréviation de « entreprise de travail intérimaire » au sens de l'article L.131-1 du Code du Travail.
RGPD	Règlement Général sur la Protection des Données
Propriétaire du référentiel	Dans ce cas le FSI
Organisme de surveillance	Dans ce cas ESCEM
Service de Certification	Service chargé de la validation et la prise de décision de certification
Auditeur	Personne chargée de la réalisation des audits de systèmes de management.
Auditeur/Expert Externe	Tout auditeur/expert n'appartenant pas à la structure ESCEM

4 ORGANISATION D'ESCEM

4.1 Structure Juridique

ESCEM est une entreprise de prestation de services de droit luxembourgeois ayant la forme juridique d'une "asbl", "association sans but lucratif".

ESCEM est financée par les revenus de son activité d'audit et de certification.

4.2 Organisation pour les audits du FSI

4.2.1 Auditeur :

Les auditeurs du code de conduite RGPD sont nommés par ESCEM sur base des éléments suivants :

- Ayant suivi une formation d'auditeur externe ou d'auditeur interne pour système de management
- Ayant suivi une formation sur le RGDP
- Ayant suivi une formation spécifique sur le code de conduite RGPD du FSI

La nomination d'auditeurs/experts externes est identique à la nomination des auditeurs internes.

4.2.2 Comité de certification

Les membres du comité de certification sont des auditeurs expérimentés qui ont autorité de valider les dossiers et prendre les décisions de certifications. Les décisions sont prises par un des membres du comité. Le membre attribué à un dossier est désigné par la Direction d'ESCEM sur base des règles d'impartialités. La prise de décision ne pourra en aucun cas être externalisé.

5 PROCEDURE D'ADHESION AU CODE

5.1 Acceptation de la mission d'audit

L'ETI envoie par email une demande d'adhésion selon l'annexe 4 du Code ainsi que les documents annexes auprès d'ESCEM à l'adresse email indiquée sur le site internet dans la rubrique dédiée au Code.

Le FSI informe ESCEM de la vérification concluante de la demande de confirmation de l'ETI au FSI.

Dans un délai de 8 jours ouvrables à compter de la réception de la demande d'adhésion ET de l'information de la vérification par le FSI, ESCEM vérifie s'il n'existe pas de conflit d'intérêts vis-à-vis de l'ETI concernée (en ce compris entre ses éventuels sous-traitants et l'ETI) et en informe l'ETI.

En cas de conflit d'intérêt avéré, l'ETI adresse, si possible, le dossier à un autre organisme de suivi .

Dans un délai d'un mois et en l'absence de conflits d'intérêts vis-à-vis de l'ETI concernée, ESCEM vérifie l'éligibilité de l'ETI à son adhésion au Code et vérifie que la demande est complète :

- Si l'analyse est concluante, l'audit de conformité au Code de Conduite RGPD peut être déclenché sous un délai de 6 mois l'année d'adhésion des premiers membres. À compter de l'année suivante, dans un délai de 3 mois.

- Si l'analyse relève des points bloquants ou si le plan de mise en conformité et la documentation est jugée insuffisante, l'audit de conformité au Code de Conduite RGPD est mis en suspens. L'ETI dispose d'un délai de 6 mois pour apporter la correction aux points relevés.

Les auditeurs mandatés pour les missions d'audit sont définis dans le cadre de l'agrément CNPD.

Au cas où l'équipe d'audit ne dispose pas des compétences techniques, il est possible de recourir à un expert, au moins pour l'analyse de l'audit de conformité de sécurité des systèmes de l'information.

Pour les auditeurs internes à l'organisation, des sous-commandes ne sont pas éditées.

Pour les auditeurs externes à l'organisation, une sous-commande est émise. Le sous-traitant confirme l'acceptation de la commande de sous-traitance.

Dans tous les cas, les auditeurs mandatés doivent informer ESCEM d'un conflit d'intérêt potentiel.

ESCEM s'assure que les auditeurs ont l'indépendance et l'impartialité nécessaire vis-à-vis de l'ETI par signature de l'engagement des auditeurs et des sous-commandes.

Pour l'ensemble des points abordés dans cette procédure, il est à noter que l'application est identique qu'il s'agisse d'un auditeur interne ou d'un auditeur/expert externe.

5.2 Préparation à l'audit d'adhésion

Chaque ETI aura accès en amont aux critères d'audit par envoi par ESCEM des documents suivants :

- Procédure « Déroulement d'un audit de suivi du Code de Conduite RGPD – FSI par ESCEM » dans la version en vigueur.
- Questionnaire d'audit identifiant les points du Code de Conduite RGPD qui seront audités, les éventuels documents qui seront demandés ainsi que les points bloquants qui empêcheraient l'adhésion de l'ETI au dit code.

5.3 L'audit d'adhésion

Le déroulement suivant s'applique à tout type d'audit.

5.3.1 Réunion d'ouverture

L'auditeur explique la systématique de l'audit :

- La recherche de la conformité vis-à-vis de du Code de Conduite RGPD.
- Le programme d'audit
- La confidentialité des informations reçues lors de l'audit
- L'échantillonnage

5.3.2 Réunion de clôture

A l'issue de l'audit, le client est informé lors d'une réunion de restitution des résultats de l'audit.

- Informer des constats d'audit (points forts, remarques, non-conformités, conclusion finale),
- Présenter les points bloquants, le cas échéant
- Informer sur la suite (actions correctives),
- Expliquer les actions correctives demandées,
- Remettre l'attestation d'adhésion,
- Rendre à l'ETI, si souhaité, les documents fournis.

5.3.3 Points bloquants

Les non-conformités (ou points bloquants) constatées sont documentées dans le rapport d'audit.

La non-conformité doit être formulée clairement et sans ambiguïté et elle doit répondre aux éléments suivants : Exigence – Défaillance - Preuve

En fonction de la sévérité de la non-conformité, les actions correctives exigées par les auditeurs peuvent être déterminées comme suit :

- Transmission des actions correctives définies dans un plan d'action ; Vérification de la mise en œuvre lors du prochain audit
- Transmission des rapports de non-conformité avec les actions correctives effectuées et des documents modifiés ; Vérification de la mise en œuvre lors du prochain audit
- Réalisation d'un audit complémentaire

5.3.4 Refus d'adhésion

Dans le cas où un audit révélerait des non-conformités dont la gravité empêcherait les auditeurs de recommander l'adhésion au Code, ESCEM peut proposer à l'entreprise auditée d'interrompre l'audit.

Dans ce cas l'entreprise se verrait facturer au moins les frais encourus jusqu'à l'interruption de l'audit (y compris la préparation de l'audit et l'édition du rapport).

Au cas où l'équipe d'audit se verrait dans l'impossibilité de recommander l'adhésion au Code de Conduite à l'issue de l'audit, le rapport d'audit est remis à l'ETI pour qu'il dispose des raisons du refus. Le FSI ainsi que la CNPD sont notifiés de ce refus par ESCEM, sans pour autant avoir accès aux raisons de ce refus.

5.3.5 Audit complémentaire

Le but de l'audit complémentaire est la levée d'un point bloquant. Il porte donc sur l'objet de l'action corrective prévue. Il est soit documenté dans le rapport d'audit, soit dans un rapport particulier. Au moins un des auditeurs de l'équipe d'audit réalise l'audit complémentaire. Cet audit doit être réalisé dans un maximum de 6 mois après l'audit initial.

L'audit complémentaire est facturé suivant le temps passé sur la base des tarifs journaliers indiqués dans la liste de prix en vigueur.

5.3.6 Suite à l'audit

L'auditeur principal remet un rapport au client dans les plus brefs délais.

Le rapport d'audit résume les résultats de l'audit, comme suit :

- Etat du processus d'adhésion (Vue générale des rapports établis),
- Résumé de l'audit (Conclusion finale),
- Résultats de l'audit (Résumé des constats et des points bloquants),
- Remarques concernant l'audit (Commentaires de la part de l'équipe d'audit),
- Remarques générales.

Suite à l'audit, les auditeurs donnent une conclusion sur l'état d'adhésion de l'ETI

CONSTATS	CONCLUSIONS
La société a pu démontrer dans le cadre de l'audit qu'elle répond aux exigences du code de conduite RGPD.	Adhésion ou renouvellement d'adhésion de l'ETI
La société a pu démontrer dans le cadre de l'audit qu'elle reste conforme aux exigences du code de conduite RGPD.	Maintien de l'adhésion de l'ETI
La société n'a pas pu démontrer dans le cadre de l'audit qu'elle répond aux exigences du code de Conduite RGPD.	Retrait ou refus d'adhésion de l'ETI

Remarques générales des auditeurs concernant l'application du Code de Conduite

Ce paragraphe est important pour l'ETI car il étend l'audit au-delà d'un simple constat "Conforme" ou "Non-conforme" en rendant attentif à des points forts et faibles par rapport au code de conduite RGPD.

Les résultats de l'audit (constats des audits) sont classés comme suit :

Constat	Explication	Suite à donner par le client
Non-conformité majeure	Exigence du code non traitée ou respectée que partiellement qui affecte la capacité de l'ETI à atteindre les résultats escomptés.	Réaliser un audit complémentaire sur place pour vérifier la mise en place des actions correctives
Non-conformité mineure	Exigence du code non traitée ou respectée que partiellement qui n'affecte pas l'ETI à atteindre les résultats escomptés.	Réaliser des actions correctives et transmission pour vérification et approbation aux auditeurs
Remarque	Point faible devant être davantage formalisé ou précisé	Réaliser des actions correctives documentées en interne
Point fort	Eléments qui constituent des éléments particulièrement forts	Aucune

5.3.7 Délivrance et maintien de l'adhésion

A l'issue de l'audit, l'auditeur donne un avis sur l'adhésion de l'ETI.

Cet avis est validé après analyse du dossier de l'ETI par un membre du comité de certification d'ESCEM (principe des 4 yeux), cf. chapitre 6.

Sous un délai d'un mois, l'ETI reçoit son rapport d'audit ainsi que son certificat d'adhésion. L'adhésion aura une validité de 5 ans.

ESCEM informe le FSI et la CNPD de l'adhésion de l'ETI.

5.4 Audits de contrôle

Afin de maintenir son adhésion au Code Conduite RGPD, l'ETI fait l'objet d'un audit de contrôle avant la fin de la 3ème année. L'ETI est avisée par écrit avec un préavis d'un mois au minima.

Toutefois cette périodicité sera susceptible d'être modifiée en cas :

- de plainte émanant d'une partie concernée ;
- d'un changement notoire dans la structure de la société adhérente lequel pourrait potentiellement affecter le suivi des prescriptions du Code ;
- d'un changement notoire dans l'application et l'interprétation de la loi, les nouveaux développements technologiques
- d'une mise à jour, amendements et/ou extensions du code selon la décision du propriétaire du code.

De tels changements feront l'objet d'une revue systématique de la part d'ESCEM, qui décidera, au cas par cas, de la modification de la périodicité.

5.5 Renouvellement de l'adhésion

L'adhésion peut être considérée comme ininterrompue jusqu'à la date limite de validité indiquée sur le certificat sous condition que l'audit de renouvellement soit réalisé et que le nouveau certificat soit émis avant cette date limite de validité. ESCEM informe le FSI et la CNPD du renouvellement de l'adhésion de l'ETI.

5.6 Délais d'archivage des documents d'audits

Tous les documents liés à un audit sont archivés sur le serveur utilisé par ESCEM pour au moins 5 ans.

5.7 Suspension de l'adhésion

Lors d'un audit de contrôle ou d'un audit de renouvellement, en cas d'identification de points bloquants sans actions correctives efficientes, ou de retard dans la réalisation des audits, l'adhésion peut également être suspendue par ESCEM.

ESCEM informe le FSI et la CNPD de la suspension d'adhésion de l'ETI sans délai indu et par écrit. Cette information comprendra notamment le membre suspendu ; le(s) motif(s) de la suspension ; une copie du rapport envoyé au membre ; les mesures prises par le membre et ESCEM suite à la suspension.

5.8 Retrait de l'adhésion

Lors d'un audit de contrôle ou d'un audit de renouvellement, en cas d'identification de points bloquants, l'adhésion peut être retirée, notamment s'il est identifié un non-respect des exigences du Code de Conduite RGPD.

ESCEM informe le FSI et la CNPD du retrait d'adhésion de l'ETI sans délai indu et par écrit. Cette information comprendra notamment le membre retiré ; le(s) motif(s) du retrait ; une copie du rapport envoyé au membre ; les mesures prises par le membre et ESCEM suite au retrait.

5.9 Audit de suivi anticipé

Le but de l'audit de suivi anticipé est la vérification d'une ou plusieurs actions correctives effectuées depuis le dernier audit régulier, actions destinées à traiter des remarques – ou non-conformités mineures - relatives à la mise en œuvre opérationnelle du système de management. Il permet ainsi au membre de vérifier avant le prochain audit régulier, si les actions menées sont adéquates.

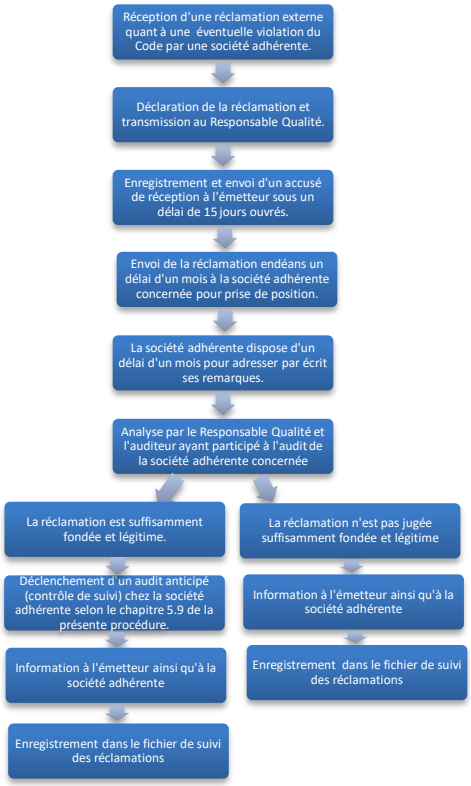
L'audit de suivi anticipé pourra également être déclenché par ESCEM en cas de réception d'une réclamation fondée et légitime, émise à l'encontre du membre (Cf chapitre 5.10 de la présente procédure).

Il est réalisé par au moins un des auditeurs de l'équipe d'audit et est documenté dans un rapport particulier. Cet audit doit être réalisé dans un délai convenu entre l'équipe d'audit et l'ETI.

ESCEM informe le FSI ainsi que la CNPD de l'ouverture du processus de contrôle.

5.10 Réclamation d'une partie intéressée de l'ETI

Dans le cas où ESCEM reçoit une réclamation d'un tiers intéressé ou une information de la part de la CNPD quant à la conformité d'une société adhérente relative au code de conduite RGPD du FSI, ESCEM procédera à une analyse et pourra déclencher un audit de suivi anticipé selon le logigramme ci-dessous.



Le retour d'information à l'émetteur de la réclamation ainsi qu'à la société adhérente quant au traitement de la réclamation, sera délivré sous un délai de trois mois à compter de la réception de la réclamation. Si nécessaire, une extension de ce délai pourra être envisagée. Celle-ci serait justifiée et communiquée aux parties intéressées.

L'ensemble des réclamations ainsi que le traitement associé sera enregistrée dans un fichier de suivi des réclamations et des appels. Ce fichier sera mis à disposition pour consultation dans les locaux d'ESCEM.

6 PRISE DE DECISION SUITE A L'AVIS DE L'AUDITEUR

L'ensemble des rapports et des documents d'audit est transmis par l'auditeur au service de certification d'ESCEM.

Les conclusions de l'audit sont évaluées par le Responsable du Service de Certification ou un membre du comité de certification, qui valide la décision de l'auditeur.

Un refus de validation peut être exprimé dans 2 cas :

- suite aux résultats de l'audit, les auditeurs ne donnent pas d'avis favorable quant à l'adhésion de l'ETI.
- les documents remis de la part des auditeurs ne permettent pas au Responsable du Service de Certification de conclure sur l'avis favorable émis par les auditeurs.

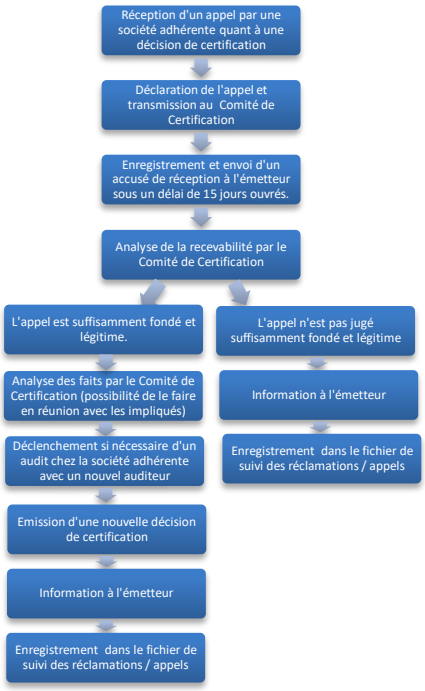
Dans le cas où le Service de Certification déciderait de la non-adhésion de l'ETI ou d'un retrait de l'adhésion, cf chapitre 5.8.

La prise de décision ne pourra en aucun cas être externalisé.

L'ETI est en droit d'appel contre les décisions du service de certification. Un tel appel est à soumettre à la direction d'ESCEM endéans un mois de la décision de certification. Passé ce délai, l'ETI ou la société adhérente est présumée accepter la décision.

Si la direction d'ESCEM est impliquée dans la décision de certification en question, il nommera à sa place une personne du comité de certification indépendante à la prestation.

L'appel sera traité selon le logigramme ci-dessous.



En cas de désaccord à l'issue de la procédure de réclamation, la société adhérente dispose de la faculté de demander l'avis de la CNPD dans un délai d'un mois à compter de la décision rendue à l'issue de la procédure de réclamation. A défaut d'introduire une telle demande auprès de la CNPD, l'ETI ou la société adhérente est présumée accepter la décision.

Dans le cas où une ETI ou une société adhérente estimerait qu'ESCEM n'exerce pas ses missions conformément au Code, l'ETI ou la société adhérente peut introduire une réclamation auprès du FSI ou de la CNPD. Si la réclamation est adressée au FSI, celui-ci la transmet à la CNPD dans un délai de 8 jours ouvrables à compter de la réception de la réclamation. Si la réclamation a été introduite auprès de la CNPD, cette dernière en informe le FSI lorsqu'elle l'estime nécessaire et dans l'intérêt du Code.

Le retour d'information à l'émetteur quant au traitement de l'appel, sera délivré sous un délai de trois mois à compter de la réception de la réclamation. Si nécessaire, une extension de ce délai pourra être envisagée. Celle-ci serait justifiée et communiquée aux parties intéressées.

L'ensemble des appels ainsi que le traitement associé sera enregistrée dans un fichier de suivi des réclamations et des appels. Ce fichier sera mis à disposition pour consultation dans les locaux d'ESCEM.

7 COMMUNICATION

7.1 Communication avec le FSI et la CNPD

ESCEM tiendra à jour un fichier de suivi des membres. Ce fichier comprendra notamment l'état du statut de certification de chaque membre (Valide / Suspendu / Exclu) ; les dates de validité de la certification. Ce fichier sera accessible au FSI et à la CNPD sur demande.

ESCEM s'engage à communiquer au FSI ainsi qu'à la CNPD toute modification substantielle de la base de l'accréditation qui aurait une incidence sur le respect par l'organisme de contrôle des exigences d'accréditation, telles que l'impartialité/l'indépendance, l'expertise ou créerait des conflits d'intérêts. Ces changements peuvent inclure, sans s'y limiter :

a. son statut juridique, commercial, de propriété ou d'organisation et son personnel clé ;
b. les ressources et le(s) lieu(x) ; et
c. toute modification de la base d'accréditation.

ESCEM signalera immédiatement au FSI et à la CNPD toute modification substantielle par écrit, sans retard injustifié.

ESCEM fournira au FSI, à la CNPD et à tout autre établissement ou institution visé par le code de conduite un rapport annuel sur le fonctionnement du code. Ce rapport comprendra notamment :

a. les informations concernant les nouveaux membres du code ;
b. le nombre de missions de suivi effectuées et leurs conclusions ;
c. le nombre et le type de réclamations adressées contre des sociétés adhérentes ainsi que le type de mesures correctives ou de sanctions prises ;
d. Le nombre d'exclusions de sociétés adhérentes ainsi que le nombre de suspension du processus d'évaluation de conformité
e. le nombre et le type de réclamations adressées contre l'organisme de suivi ainsi que les mesures prises ;
f. des informations concernant les violations du Code rencontrées, ainsi que les mesures adoptées ;
g. les questions posées par les ETI ou sociétés adhérentes par rapport au questionnaire d'audit qui leur été transmis en vue de leur évaluation ;
h. de manière anonymisée, les points de non-conformité des sociétés adhérentes ;
i. la confirmation qu'un examen du code a eu lieu et qu'aucune modification n'est nécessaire à la suite de l'examen
j. la confirmation qu'il n'y a pas de changements substantiels dans l'organe de contrôle ;

7.2 Communication au public

ESCEM tiendra à jour un fichier de suivi des membres. Ce fichier comprendra notamment l'état du statut de certification de chaque membre (Valide / Suspendu / Exclu) ; les dates de validité de la certification. Ce fichier sera accessible et mis à disposition pour consultation sur le site internet d'ESCEM.

ESCEM tiendra à jour un fichier de suivi des réclamations et des appels. Ce fichier comprendra notamment le nombre et le type de réclamations/appels reçus ; les actions correctives définies ou encore les décisions de suspensions ou d'exclusion du membre. Ce fichier sera mis à disposition pour consultation dans les locaux d'ESCEM.

8 PROCEDURES / FORMULAIRES / LISTES ASSOCIEES

Questionnaire d'audit

9 ANNEXES : ANALYSES DE RISQUES

Sujet	Risques	Moyens	Evaluation
Propriété	Influence sur les décisions de certification	ESCEM asbl est une société indépendante	Faible
Gouvernance	Influence sur les décisions d'audit et de certification par la direction	La direction d'ESCEM asbl n'exerce aucune pression ni sur les résultats des audits ni sur les résultats des décisions de certification	Faible
	Influence sur les décisions d'audit et de certification par le FSI et l'ETI	Vérification de la décision de l'auditeur par le comité de certification (principe des 4 yeux)	Faible
	Influence sur les décisions d'audit et de certification par l'ETI qui est également client pour une certification de système de management	Vérification de la décision de l'auditeur par le comité de certification (principe des 4 yeux)	Faible
	Influence sur les décisions d'audit et de certification par des ETI, représentés dans le comité de maitrise et d'impartialité	Ni le FSI ni un ETI font partie du comité de maitrise.	Faible
Personnel	Familiarité ou connaissance trop proche avec l'ETI ; Risque d'un audit de complaisance	Vérification lors des revues de contrat et des sous-commandes Devoir des auditeurs d'informer le responsable certification.	Faible
	Personnel externe effectuant du conseil ou des audits internes en lien avec le RGPD	Signature des auditeurs externes de ne pas avoir effectué du conseil les 2 derniers années.	Faible
	Personnel quittant ESCEM et reprenant une fonction clé chez un ETI certifié	Le prochain audit devra être réalisé par un auditeur externe	Faible
Ressources partagées	ESCEM asbl partage des ressources avec LUXCONTROL, notamment IT, Administration et Ressources Humaines	Les personnes en question pouvant avoir connaissance des résultats d'audit et des décisions de certification ont signé une charte de confidentialité	Faible
Situation financière	Obtention d'une certification sur base d'un paiement excessif d'un client	La rémunération du personnel est indépendante du résultat de l'audit	Faible

Sujet	Risques	Moyens	Evaluation
Situation financière	Dominance d'un client, Influence sur les décisions de certification	Suivi et analyse de la répartition des clients et leur chiffre d'affaires	Faible
	Obligation de faire du chiffre au détriment de la qualité	Le chiffre d'affaire et le budget d'ESCEM est suivi et voté par le conseil d'administration	Faible