

En partenariat avec :  



Cahier des charges

Version à jour au : 12 octobre 2026

TABLE DES MATIÈRES

1. INTRODUCTION.....	3
2. CONTEXTE	3
2.1 L'importance de la cybersécurité.....	3
2.2 Le cadre réglementaire	4
2.3 La cybersécurité au Luxembourg	5
3. ENTREPRISES ÉLIGIBLES	5
4. CONCEPT	6
5. PÉRIMÈTRE DE LA MISSION, MÉTHODOLOGIE ET LIVRABLES.....	6
5.1 Méthodologie.....	6
5.2 Livrables	7
5.3 Clôture et suite du diagnostic Fit 4	7
6. BASE LÉGALE	8
7. NATURE ET MONTANT DES FRAIS ÉLIGIBLES.....	8
8. PROCÉDURE	9
9. RÉFÉRENCEMENT DES CONSULTANTS : CONDITIONS D'ACCÈS AU RÉFÉRENCEMENT ET COMPÉTENCES REQUISES.....	12
9.1 Compétences et qualifications.....	12
9.2 Procédure de référencement.....	13
9.3 Durée du référencement	13
10. OBLIGATIONS	14
10.1 Obligations de la société prestataire	14
10.2 Obligations de l'entreprise bénéficiaire	16

1. INTRODUCTION

Les programmes « Fit 4 » permettent aux entreprises luxembourgeoises d'accéder à l'expertise de consultants spécialisés et à des subventions publiques afin de renforcer la performance de leurs démarches d'innovation, de digitalisation, et de durabilité. Ils aboutissent à un diagnostic approfondi ainsi qu'à une feuille de route chiffrée, précisant les priorités, actions concrètes, et investissements à envisager par l'entreprise. Ces programmes ne couvrent pas le financement de la mise en œuvre des actions recommandées, qui peut toutefois faire l'objet d'autres dispositifs de soutien, sous réserve de leur éligibilité.

Le présent cahier des charges définit les conditions de mise en œuvre du programme **Fit 4 Cybersecurity**, qui est piloté par Luxinnovation en partenariat avec la Luxembourg House of Cybersecurity (LHC). Ce programme a pour ambition d'accompagner les entreprises dans leur démarche de sécurisation vis-à-vis des cyberattaques. Le programme vise à produire des recommandations utiles et concrètes pour les entreprises bénéficiaires, tout en garantissant la qualité, l'indépendance et la pertinence des interventions.

Le présent document définit notamment :

- Le périmètre du programme et les livrables attendus ;
- Les taux et seuils de subvention ;
- Les conditions d'éligibilité des entreprises bénéficiaires ;
- Les conditions d'accès au référencement des prestataires ;
- Les procédures à suivre ;
- Les obligations respectives des prestataires, des entreprises bénéficiaires et de Luxinnovation/de la LHC.

2. CONTEXTE

2.1 L'importance de la cybersécurité

Dans une économie digitalisée, les cyberattaques portant atteinte aux technologies de l'information et de la communication (TIC) peuvent revêtir de multiples formes (phishing, ransomware, malware, déni de service, social engineering, etc.), et leurs conséquences financières peuvent s'avérer particulièrement lourdes pour les entreprises :

- l'indisponibilité de données peut provoquer l'interruption de l'activité commerciale, et par là un important manque à gagner ;
- les violations des règles de protection des données à caractère personnel prévues par le RGPD peuvent donner lieu à des amendes ;
- les attaques cybercriminelles peuvent donner lieu à des poursuites judiciaires, engendrant des frais de justice.

L'image de l'entreprise peut être atteinte et provoquer une perte de confiance chez ses clients, voire un désengagement et une baisse du chiffre d'affaires. Par ailleurs, l'impact de la directive NIS2, dont les exigences s'étendent au-delà des entreprises concernées pour inclure leurs fournisseurs de services, ainsi que la multiplication des vecteurs d'attaque due à l'adoption massive des outils d'IA, accroissent et renforcent d'autant plus les défis actuels en matière de cybersécurité.

Les objectifs généraux en matière de sécurité des TIC sont donc les suivants :

- intégrité ;
- confidentialité ;
- disponibilité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyber-environnement.

Elle ne se résume donc plus à des « pare-feu » et à des logiciels antivirus standard mais se définit plutôt à présent comme « l'ensemble des outils, des technologies, des processus et des pratiques qui peuvent être utilisés pour protéger les réseaux, les ordinateurs et les données contre un accès non autorisé ou une attaque ».

2.2 Le cadre réglementaire

La directive NIS2¹ (directive sur la sécurité des réseaux et des systèmes d'information) élargit les objectifs et le périmètre de la directive NIS1 afin de renforcer la protection contre les cybermenaces au sein de l'Union européenne.

Au Luxembourg, NIS2 est transposée par la loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité, entrée en vigueur le 10 mai 2026. Elle remplace le dispositif NIS1 issu de la loi du 28 mai 2019. À l'échelle européenne, le règlement d'exécution (UE) 2024/2690 du 17 octobre 2024 précise par ailleurs les exigences techniques applicables à certaines catégories d'entités.

La loi distingue deux catégories d'organisations : les « entités essentielles » (EE) et les « entités importantes » (EI). Ce classement repose sur la taille de l'entité, son impact économique et social et son rôle dans l'infrastructure de l'Union. Sont visés les secteurs hautement critiques (énergie, transports, banques, infrastructure des marchés financiers, santé, eau potable et eaux usées, infrastructure numérique, gestion des services TIC, administration publique, espace) ainsi que d'autres secteurs critiques (fournisseurs numériques, gestion des déchets, alimentation, produits chimiques, fabrication, services postaux et d'expédition, recherche). Au total, l'Institut luxembourgeois de régulation (ILR) estime à plus de 1 200 le nombre d'entreprises concernées au Luxembourg.

La supervision repose sur trois acteurs : l'ILR, autorité compétente pour la cybersécurité ; le Haut-Commissariat à la Protection nationale (HCPN), chargé de la gestion des incidents majeurs et des crises cyber ; et la Commission de surveillance du secteur financier (CSSF) pour les acteurs financiers. Pour ces derniers, le règlement (UE) 2022/2554 (DORA) prime sur NIS2 pour les aspects qu'il couvre.

Enfin, NIS2 s'inscrit dans un cadre réglementaire plus large. Elle se combine avec la directive (UE) 2022/2557 sur la résilience des entités critiques, qui traite de la protection physique des opérateurs critiques, et avec le Cyber Resilience Act (règlement (UE) 2024/2847), qui impose des exigences de cybersécurité aux produits comportant des éléments numériques, avec une pleine application prévue pour 2027.

¹ EUR-lex, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

2.3 La cybersécurité au Luxembourg

Au Luxembourg, le secteur des TIC joue un rôle majeur dans la société, contribuant tant au développement de l'économie qu'à la sécurité et au bien-être des citoyens. Il a par ailleurs un impact important sur d'autres secteurs qui assurent le bon fonctionnement du pays, tels que l'éducation, la santé, les transports, les finances, ou encore l'énergie.

La transformation numérique de l'économie luxembourgeoise, fondée sur les données, l'intelligence artificielle et les technologies émergentes, doit s'accompagner d'un renforcement continu de la cybersécurité et de la résilience numérique, afin de permettre à tous les acteurs de participer pleinement à la société numérique dans un environnement de confiance.

Le Luxembourg fait partie des pays les plus avancés en Europe et dans le monde pour son engagement en matière de cybersécurité. Selon le Global Cybersecurity Index (GCI) 2024 de l'Union internationale des télécommunications (UIT), le Grand-Duché se classe dans le Tier 1 « Role-modelling » composé de 46 pays. Ce groupe réunit les nations leaders sur les cinq piliers de l'indice : juridique, technique, organisationnel, développement des capacités et coopération.

En pratique, l'écosystème national de cybersécurité repose sur une collaboration active entre les acteurs publics et privés. Le rôle clé du ministère de l'Économie fait du Luxembourg un cas unique en Europe, où la cybersécurité est considérée non seulement comme une question de défense, mais aussi comme une question économique.

Ainsi, le ministère de l'Économie est directement partie prenante de la Luxembourg House of Cybersecurity (anciennement SECURITYMADEIN.LU) ou LHC.

La LHC, grâce à une équipe multidisciplinaire d'une cinquantaine de personnes, fournit expertise et solutions en matière de cybersécurité aux entreprises de toutes tailles ainsi qu'aux municipalités par l'intermédiaire de ses trois centres (Computer Incident Response Center Luxembourg ou CIRCL, National Cybersecurity Competence Center – Luxembourg ou NC3, et Luxembourg Cybersecurity Factory ou LCSF).

En quelques années, le nombre de cyberattaques enregistré par la LHC a grandi de manière exponentielle et a déclenché une réelle prise de conscience au sein des entreprises luxembourgeoises. Toutefois, les réponses apportées au questionnaire d'auto-évaluation en matière de maturité cyber-digitale, montrent qu'elles ont encore besoin d'un accompagnement et d'un soutien pour sécuriser leur environnement digital.

Par conséquent, en complément des dispositifs déjà notamment mis en place par la LHC, le ministère de l'Économie, s'appuyant sur Luxinnovation et la LHC et faisant appel aux différentes compétences présentes au sein de l'écosystème national, propose un programme d'accompagnement et de co-financement à l'attention des entreprises luxembourgeoises, afin de leur donner les moyens d'évaluer la disponibilité, l'intégrité, la confidentialité, la traçabilité de leurs données et flux d'information, et d'identifier les moyens à mettre en œuvre pour se prémunir contre les cyberattaques.

3. ENTREPRISES ÉLIGIBLES

Les programmes Fit 4 sont ouverts aux **entreprises de toutes tailles** qui remplissent les conditions cumulatives suivantes :

- disposer d'une [autorisation d'établissement](#) en cours de validité, délivrée par le ministère de l'Économie ;
- avoir leur siège social au Luxembourg ;
- exercer une activité économique à titre principal.

4. CONCEPT

Le programme ouvre aux entreprises la possibilité de faire réaliser un diagnostic des vulnérabilités et risques d'exposition aux cyberattaques, complété par un plan d'action détaillé et chiffré.

Ce diagnostic ne peut pas comprendre les mesures de sécurité obligatoires dans le cadre de la directive NIS2 (par exemple élaborer des politiques et procédures relatives à la gestion des risques) pour les entités qui rentrent dans le champ d'application de cette directive. Le site de l'ILR permet de consulter les mesures obligatoires et le périmètre des entreprises concernées².

Le diagnostic complété par le plan d'action sera réalisé par des consultants préalablement référencés par Luxinnovation et la LHC. La durée totale de la mission est, en principe, limitée à 6 mois.

Luxinnovation et la LHC conçoivent et pilotent le programme, référencent les consultants qui répondent aux exigences du programme et veillent à ce que chaque projet Fit 4 Cybersecurity respecte les critères définis dans le présent document. Les subventions publiques liées au programme sont accordées aux entreprises bénéficiaires par le ministère de l'Économie, conformément au cadre légal applicable.

À l'issue du diagnostic Fit 4 Cybersecurity, l'entreprise peut choisir de mettre en œuvre toutes ou une partie des recommandations définies dans le plan d'actions. Bien que cette mise en œuvre ne relève pas du périmètre de Fit 4 Cybersecurity, Luxinnovation conseille l'entreprise sur les autres dispositifs de soutien susceptibles d'être mobilisés.

5. PÉRIMÈTRE DE LA MISSION, MÉTHODOLOGIE ET LIVRABLES

5.1 Méthodologie

Le diagnostic réalisé par l'expert externe se déroule en deux phases : d'abord une auto-évaluation de la maturité générale en matière de cybersécurité et des axes de travail prioritaires, et ensuite une analyse approfondie d'un ou plusieurs axes de travail prioritaires.

Phase 1 : Évaluation « Cybercheck in-depth »

Le « Cybercheck » est un outil d'évaluation des risques cyber mis à disposition par la LHC. Il est proposé en deux versions : « light » et « in-depth ». L'entreprise doit compléter la version « light » avant le lancement d'un projet Fit 4 Cybersecurity (voir chapitre 8), tandis que la version « in-depth » est intégrée au périmètre de la mission réalisée avec le consultant. Dans ce cadre, le consultant accompagne l'entreprise dans la réalisation du Cybercheck « in-depth » et organise (au moins) un workshop pour expliquer les résultats et s'aligner sur les priorités pour la suite. Les résultats du rapport Cybercheck « in-depth » servent ensuite de base aux travaux d'analyse de la phase 2 et sont intégrés au rapport final du consultant (voir section 5.2).

Le consultant pourra facturer un montant maximal de 4 500 € HTVA pour cette première phase.

Dans le cas où une évaluation Cybercheck « light » ou « in-depth » a déjà été faite dans le cadre des services proposés par le L-DIH, alors l'entreprise en est dispensée dans le cadre de Fit 4 Cybersecurity.

² <https://www.ilr.lu/secteurs-activites/niss/nis-2/>

Phase 2 : Analyse approfondie

Le consultant réalise une analyse approfondie sur mesure des risques de sécurité de l'entreprise cliente afin de mieux la préparer face aux cyberattaques. Cette analyse aboutit à un rapport, et peut inclure un ou plusieurs **des audits techniques de sécurité informatique suivants** (selon les besoins préalablement identifiés sur base de l'auto-évaluation « Cybercheck ») :

- audit d'architecture ;
- audit de l'efficacité des systèmes de sauvegarde ;
- audit de la sécurité physique des installations ;
- audit de configuration ;
- audit de code source ;
- audit organisationnel ;
- audit de conformité avec les normes et réglementations en matière de sécurité informatique (RGPD, norme ISO 27001, NIS2, etc.) ;
- test d'intrusion (pentest).

Les consultants sont libres de définir la méthodologie applicable à la réalisation de ces audits. Il est toutefois recommandé de s'appuyer sur une méthodologie ou une norme reconnue. Le consultant mettra en œuvre les moyens à sa convenance (outils, logiciels, méthodologie ...) pour mener à bien sa mission. Si le consultant le souhaite, il pourra faire usage des outils développés par la LHC et mis gracieusement à sa disposition. Une formation sera assurée au préalable par la LHC pour les consultants intéressés.

5.2 Livrables

Le livrable de la mission Fit 4 Cybersecurity est un **rapport incluant des recommandations**, structuré de la manière suivante :

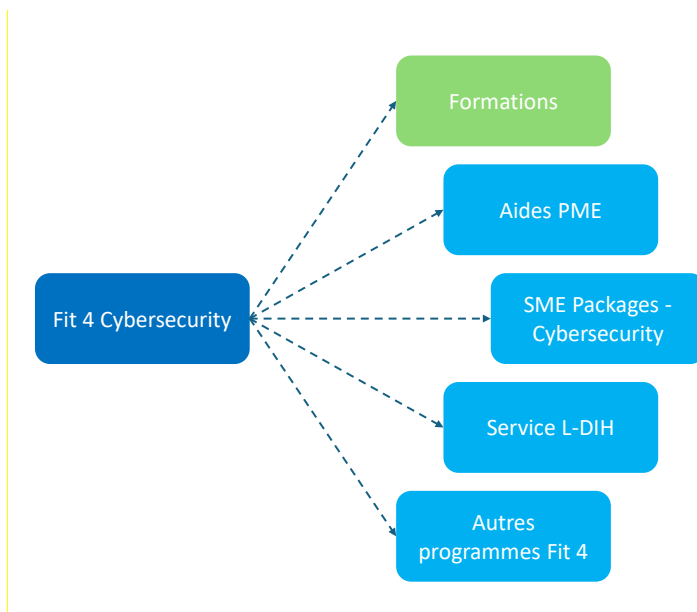
- rapport résultant de l'auto-évaluation « Cybercheck » (in-depth) ;
- description des systèmes d'information ;
- rappel de la méthode et des outils utilisés pour réaliser les analyses approfondies ;
- synthèse des vulnérabilités classées selon leur niveau de vulnérabilité et la portée de leur impact sur les systèmes d'information ;
- mesures correctives (classées par priorité et indiquant un budget estimatif pour chacune d'elle) portant sur les investissements en biens corporels ou incorporels liés à la protection réseau, aux solutions de cyber veille, investissements liés à la sécurité physique, etc., et à la mise en conformité aux règlements RGPD, RGS et NIS2.

5.3 Clôture et suite du diagnostic Fit 4

Le prestataire restitue les conclusions de son diagnostic Fit 4 au moyen d'une présentation formelle adressée à la direction et aux équipes opérationnelles (en présence de Luxinnovation et de la LHC), et remet un plan d'action structuré précisant, pour chaque mesure recommandée, le calendrier prévisionnel, ainsi que les ressources humaines et financières à mobiliser.

À l'issue du diagnostic Fit 4 Cybersecurity, l'entreprise peut choisir de mettre en œuvre toutes ou une partie des recommandations définies dans le plan d'actions.

À la réception du rapport final, Luxinnovation procède à une analyse systématique des recommandations formulées par l'expert afin d'identifier les schémas d'aide susceptibles d'en co-financer la mise en œuvre — qu'il s'agisse de programmes d'accompagnement gérés par Luxinnovation, d'aides gérées par le ministère de l'Économie (SME Packages Cyber, aide à l'investissement, aide aux services de conseil, etc.) ou de dispositifs européens mobilisables. Si l'entreprise souhaite solliciter une aide d'État pour la mise en œuvre d'une recommandation, elle doit faire la demande associée avant le début de la mise en œuvre.



Luxinnovation ainsi que la LHC pourront également orienter l'entreprise vers les formations appropriées (telles que celles du catalogue du Digital Learning Hub, de la House of Training, etc.) et de manière plus générale, la mettre en relation avec tout intervenant pertinent pour la suite de son parcours.

6. BASE LÉGALE

Le présent programme est basé sur les dispositions de la loi du 20 décembre 2019 ayant pour objet la mise en place d'un régime d'aides de minimis.

7. NATURE ET MONTANT DES FRAIS ÉLIGIBLES

Les frais éligibles correspondent exclusivement aux honoraires du consultant choisi, hors frais de déplacement et autres frais annexes, sur la base d'un devis préalablement établi à l'attention de l'entreprise et conforme au présent cahier des charges.

Les frais éligibles sont co-financés par une aide étatique, versée sous la forme d'une subvention en capital. **Par projet, le montant de l'aide doit être supérieur à 1 000 euros et ne peut excéder 100 000 euros.**

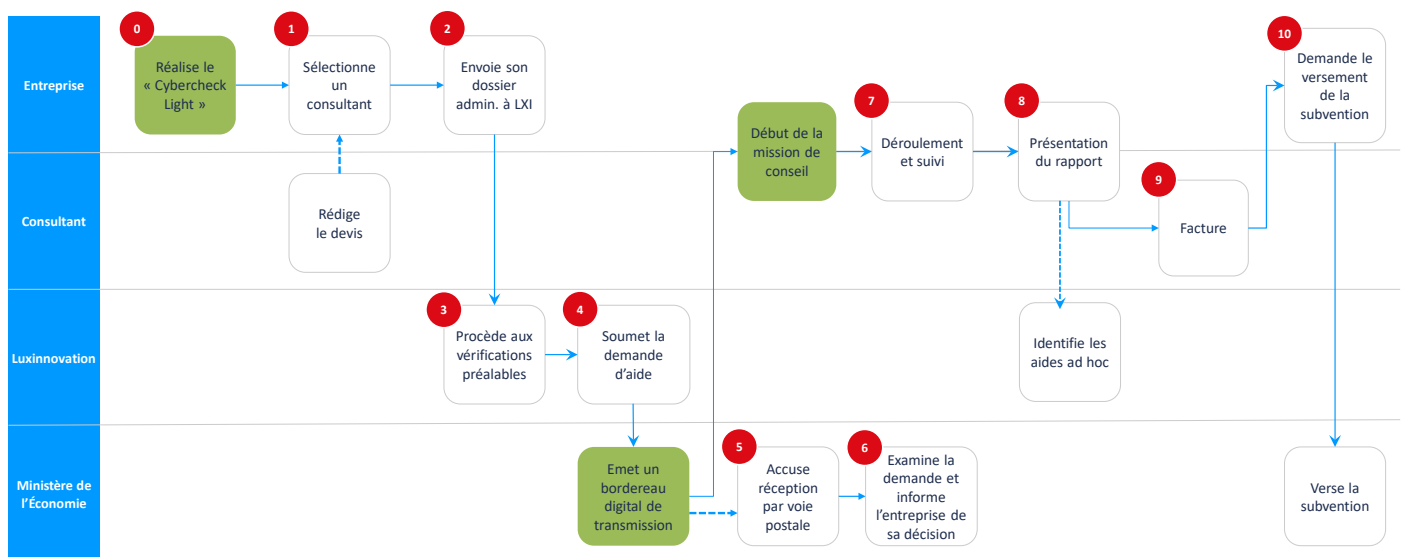
L'intensité maximale de l'aide est déterminée en fonction de la taille de l'entreprise, elle-même définie selon les

critères fixés par la réglementation européenne³ :

	Petite entreprise	Moyenne entreprise	Grande entreprise
Intensité de l'aide	70 %	60 %	50 %

8. PROCÉDURE

Pour solliciter la subvention prévue dans le cadre du présent cahier des charges, la procédure est la suivante :



Étape préliminaire : Auto-évaluation Cybercheck « light »

Le Cybercheck « light » est un outil d'auto-évaluation mis à disposition par la LHC. L'entreprise remplit le questionnaire et reçoit ensuite un rapport sommaire lui permettant de connaître ses failles incluant des recommandations d'axes sur lesquels travailler en priorité.

Étape 1 : Sélection & devis du consultant

L'entreprise sélectionne un consultant dans la liste des consultants référencés pour le programme Fit 4 Cybersecurity - dont le répertoire est accessible sur le site Internet de Luxinnovation et de la LHC - et obtient un devis conforme au présent cahier des charges.

Le consultant établit son devis détaillant les analyses et études à mener dans les domaines prioritaires mis en évidence par le Cybercheck « light ».

³ Annexe I du règlement (UE) n° 651/2014 de la Commission du 17 juin 2014 déclarant certaines catégories d'aides compatibles avec le marché intérieur en application des articles 107 et 108 du traité, tel que modifié : <https://eur-lex.europa.eu/eli/reg/2014/651>

Étape 2 : Envoi des documents administratifs à Luxinnovation

L'entreprise complète le formulaire de demande sur le portail de Luxinnovation (JWay) et communique les pièces nécessaires, notamment :

- Organigramme faisant apparaître toutes les sociétés, en amont ou en aval, avec lesquelles il existe un lien de participation supérieur ou égal à 25%. Pour chacune de ces sociétés, l'organigramme devra préciser le nombre d'ETP, le total au bilan et le montant du chiffre d'affaires du dernier exercice (exemplaire en annexe de ce document) ;
- Comptes annuels clôturés (bilan et compte de résultat) des deux derniers exercices fiscaux de l'entreprise requérante et, le cas échéant, du groupe dont elle fait partie ;
- Devis du consultant (**non signé**) ;
- Rapport résultant du Cybercheck « light » ;
- Relevé d'identité bancaire ;
- Procuration à Luxinnovation pour compléter la démarche MyGuichet au nom de l'entreprise.

Étape 3 : Vérifications préalables

Luxinnovation vérifie au préalable l'éligibilité de la demande sur base des informations communiquées par l'entreprise, puis délivre un certificat attestant que le devis est conforme aux prescriptions du présent cahier des charges.

Étape 4 : Demande de subvention

Luxinnovation introduit la demande de subvention sur MyGuichet.lu, au nom de la société requérante.

Le bordereau digital généré à l'issue de la saisie et de la transmission électronique constitue la preuve du dépôt. Luxinnovation envoie à l'entreprise une copie du bordereau digital généré à l'issue de la transmission, qui devra le conserver dans son dossier administratif.

L'entreprise peut signer le devis et commencer la mission dès réception du bordereau digital. Elle peut aussi décider d'attendre la décision définitive du ministère (étape 6).

Étape 5 : Accusé de réception du ministère

Le ministère de l'Économie accuse réception de la demande d'aide dans les quinze jours à compter de sa réception et informe le demandeur de tout document manquant ainsi que des délais de traitement du dossier. La réception des pièces manquantes sera suivie, dans le même délai, d'un nouvel accusé de réception, qui fera débiter le délai imparti.

Cet accusé de réception ne constitue toutefois pas une décision relative à l'octroi ou au refus de l'aide étatique

Étape 6 : Instruction de la demande et décision du ministère

Le ministère instruit la demande, puis confirme sa décision à l'entreprise par courrier. La décision est transmise endéans 2 mois à compter de la réception du dossier complet, avec prolongation possible de 3 mois en cas de complexité accrue de la demande. Le demandeur est informé avant la fin de la période des 2 mois que la date limite sera repoussée de 3 mois, sauf lorsque l'accusé de réception a clairement indiqué que la durée de la procédure serait de 5 mois.

L'absence de décision dans le délai imparti vaut accord tacite.

En cas de décision favorable, le courrier de notification précise les éléments suivants :

- Le montant de l'aide ;
- La période d'éligibilité des coûts (date limite à laquelle le consultant devra avoir émis la dernière facture) ;
- La date de forclusion (date à laquelle l'entreprise requérante devra avoir retourné au ministère le rapport, la facture et les preuves de paiement, pour déclencher le versement de la subvention par le ministère).

Étape 7 : Déroulement et suivi de la mission

La mission est réalisée conformément au devis et au périmètre présentés dans la demande de subvention. La durée totale de la mission est limitée à 6 mois. En cas de prolongation, une demande devra être adressée en ce sens à l'instructeur en charge du dossier auprès du ministère de l'Économie, au plus tard avant la fin de la période d'éligibilité des coûts.

Étape 8 : Finalisation de la mission et communication du rapport

Le consultant communique le rapport final à l'entreprise et à Luxinnovation et à la LHC, et organise une réunion commune afin de présenter les résultats de l'analyse et les recommandations formulées.

L'identification des aides étatiques susceptibles de contribuer au financement de ces recommandations relève de la responsabilité de Luxinnovation.

Étape 9 : Facturation

L'entreprise règle la ou les factures du consultant.

Étape 10 : Versement de la subvention

L'entreprise introduit auprès du ministère de l'Économie, via MyGuichet.lu, sa demande de paiement, accompagnée du rapport du consultant, de la ou des factures et des preuves de paiement. La demande de paiement doit être introduite au plus tard 6 mois après la date de fin du projet fixée dans la décision d'octroi.

9. RÉFÉRENCEMENT DES CONSULTANTS : CONDITIONS D'ACCÈS AU RÉFÉRENCEMENT ET COMPÉTENCES REQUISES

Les missions décrites ci-dessus sont réalisées par des sociétés de conseil référencées par Luxinnovation et la LHC, qui ont démontré qu'elles emploient des experts justifiant des compétences et qualités requises, comme décrit ci-dessous.

9.1 Compétences et qualifications

Seules des **personnes morales régulièrement immatriculées au RCS du Luxembourg** (à l'exclusion de travailleurs indépendants) pourront soumettre leur candidature.

Les personnes morales régulièrement immatriculées dans un autre État membre de l'Union européenne peuvent également être référencées, à condition de justifier des compétences définies ci-dessous et de produire un devis rédigé à l'attention d'une entreprise luxembourgeoise.

Les prestataires sont tenus de démontrer que les experts engagés dans la mission disposent des compétences suivantes :

Compétences générales et expérience

- Maîtrise de la méthodologie d'audit d'entreprise, idéalement conforme aux exigences de la norme EN/ISO 17021-2 : 2018 applicable à l'audit de PME ;
- Maîtrise d'une ou plusieurs méthodes de conduite de mission de conseil en organisation ou en management, qu'il s'agisse d'approches structurées par phases (diagnostic, recommandations, mise en œuvre, suivi) ou d'approches itératives permettant des ajustements en cours de mission en fonction des retours terrain ;
- Expérience minimale de 3 ans dans la conduite de missions comparables, exigée pour chaque expert impliqué ;
- Maîtrise du français ou de l'anglais. L'allemand et le luxembourgeois sont un plus.

Compétences spéciales

- Connaissance des standards en vigueur en matière de gouvernance des risques (par exemple : normes ISO/EIC 27000, méthode MONARC, méthode EBIOS Risk Manager, etc.) ;
- Maîtrise des principes de gestion de la donnée et de gestion d'un SI ;
- Architecture des systèmes et des réseaux, technologies, protocoles usuels de communication ;
- Administration d'un ou plusieurs systèmes d'exploitation ;
- Architectures et protocoles réseau (leurs vulnérabilités et leur sécurisation) ;
- Méthodes d'exploitation des vulnérabilités affectant les composants d'un système informatique ;
- Compréhension des architectures de systèmes d'information ;
- Pratique d'au moins un langage de programmation ;
- Expérience d'au moins trois ans dans le domaine de la sécurité des systèmes d'information ;

- Capacité à identifier des solutions logicielles.

Sous-traitance : la sous-traitance d'une partie des prestations est autorisée sous réserve d'en informer Luxinnovation et la LHC, ainsi que l'entreprise concernée qui devra donner son accord. La société de consultance devra définir et encadrer la mission confiée au sous-traitant.

9.2 Procédure de référencement

Les sociétés intéressées devront faire parvenir à Luxinnovation un dossier de candidature comprenant les éléments suivants :

- Fiche de renseignements (*modèle fourni*) ;
- Déclaration sur l'honneur (*modèle fourni*) ;
- Présentation de l'entreprise (*modèle fourni*) ;
- Bilans et comptes de résultats des 3 derniers exercices de la société ;
- CV détaillés des experts appelés à intervenir ;
- Divers documents justificatifs (certification ISO, attestations de formation, diplômes type école d'ingénieur, master 2 ou sanctionnant une formation universitaire technique dans le domaine des technologies de l'information et de la communication - une formation spécialisée en sécurité du numérique ou une expérience dans ce domaine est appréciable, etc.) ;
- Références de missions : au minimum 3 missions similaires réalisées dans les 3 dernières années, auprès d'entreprises luxembourgeoises ou européennes (*modèle fourni*) ;
- Optionnel : Exemples de livrables anonymisés : cartographies de processus, rapports de diagnostic, feuilles de route, présentations de restitution ;
- Logo de l'entreprise ;
- Devis adressé à un client basé au Luxembourg (*si la société de conseil n'est pas établie au Luxembourg*).

Les dossiers de candidature peuvent être déposés à tout moment en utilisant le formulaire prévu à cet effet sur le site de Luxinnovation : <https://www.luxinnovation.lu/wizard-fit-4-consultants>

Pour les sociétés de consultance souhaitant réaliser des audits auprès d'entreprises stratégiques, notamment celles répertoriées dans le Luxembourg Industry Defence Catalogue (liste non exhaustive), la LHC peut exiger des tests ou examens complémentaires.

Le référencement pourra être accordé au vu du seul dossier de candidature, ou après un entretien complémentaire. À l'issue de leur analyse, Luxinnovation et la LHC rendent une décision officielle : si celle-ci est favorable, le consultant est autorisé à recruter un premier client dans le cadre du programme afin de réaliser un premier diagnostic.

Le référencement définitif sur le site internet de Luxinnovation et de la LHC est confirmé après évaluation conjointe de la première mission réalisée, sous réserve que celle-ci soit concluante et conforme aux critères énoncés dans le présent document.

9.3 Durée du référencement

Le référencement est accordé pour une durée de trois ans, sans reconduite automatique.

Tout manquement à l'une des obligations prévues par le présent cahier des charges, toute insuffisance qualitative avérée dans la réalisation des missions, ou toute atteinte portant préjudice à l'entreprise accompagnée, à Luxinnovation, la LHC ou au ministère de l'Économie, est susceptible d'entraîner le retrait avant terme du référencement de la société prestataire.

Constituent notamment des motifs de retrait :

- des appréciations insuffisantes ou récurrentes laissées par les entreprises accompagnées à l'issue des enquêtes de satisfaction ;
- une qualité des livrables jugée insuffisante au regard des standards définis dans le présent cahier des charges, sur la base de la relecture du rapport final conduite par Luxinnovation ou la LHC ;
- le non-respect des règles déontologiques, notamment en matière de conflits d'intérêts, de confidentialité ou de communication relative au programme ;
- la communication d'informations erronées, incomplètes ou trompeuses, que ce soit dans le dossier de candidature ou dans le cadre des missions réalisées ;
- la falsification de documents ou tout acte frauduleux en vue d'obtenir ou de conserver le référencement ;
- une condamnation prononcée par un jugement ayant autorité de chose jugée pour tout délit affectant la moralité professionnelle de l'expert ;
- la non-atteinte du seuil minimal de missions requis pour maintenir le référencement dans le programme.

Avant toute décision de retrait, la société prestataire est informée par écrit des manquements qui lui sont reprochés et dispose d'un délai de sept jours pour fournir toute explication utile.

Luxinnovation peut mettre en demeure la société prestataire de procéder au remplacement de l'expert concerné dans un délai qu'elle fixe. Si la société ne donne pas suite à cette mise en demeure, ou si le manquement constaté est d'une gravité telle qu'il porte atteinte à la qualité du programme ou à la réputation de Luxinnovation ou de la LHC, le retrait du référencement peut être prononcé à l'encontre de la société dans son ensemble, sans préjudice des autres voies de recours ouvertes à Luxinnovation.

Toute exclusion emporte l'interdiction immédiate de se prévaloir du référencement au programme. Les missions en cours au moment du retrait doivent être menées à terme dans les délais convenus, sauf volonté expresse de l'entreprise accompagnée d'y mettre fin immédiatement, auquel cas les conditions de la rupture sont réglées selon le droit commun des contrats.

La société prestataire peut également renoncer à tout moment à son référencement, sous réserve de mener à terme l'ensemble des missions en cours.

10. OBLIGATIONS

10.1 Obligations de la société prestataire

Les relations entre la société prestataire et l'entreprise bénéficiaire sont régies par les conditions spéciales fixées dans le devis, les conditions générales de vente du prestataire, et le droit commun des contrats. Le ministère de l'Économie, Luxinnovation ou la LHC n'interviennent pas dans la relation contractuelle entre le prestataire et l'entreprise et ne sauraient voir leur responsabilité engagée en cas de défaut ou de mauvaise exécution des prestations, ni pour quelque autre cause que ce soit liée à l'exécution de la mission.

Outre le respect des dispositions du présent cahier des charges, le prestataire s'engage à :

- Facturer un tarif journalier maximum de 1 300 € HTVA, applicable à l'ensemble des experts mobilisés dans le cadre de la mission, quel que soit leur profil ou leur niveau de séniorité ;
- Réaliser un minimum de deux missions dans le cadre du programme au cours de chaque année civile, ce seuil* constituant une condition de maintien actif dans le répertoire de prestataires référencés ;

- Exécuter la mission dans un délai de 6 mois. Au besoin, l'entreprise pourra solliciter une prolongation du délai en adressant une demande en ce sens à l'instructeur en charge du dossier auprès du ministère de l'Économie ;
- Effectuer l'analyse sur site, dans les locaux de l'entreprise bénéficiaire ;
- Adresser à l'entreprise, préalablement au démarrage de la mission, un devis détaillé comprenant au minimum les éléments suivants :
 - o le périmètre organisationnel et opérationnel de la mission (c'est-à-dire par exemple : audit d'application mobile -> audit de code source + audit de configuration / audit de SI industriels -> audit organisationnel et physique + audit d'architecture + audit de configuration, etc.) ;
 - o le calendrier prévisionnel : réunion de lancement, étapes intermédiaires et réunion de clôture ;
 - o la composition de l'équipe projet et le rôle de chaque intervenant ;
 - o le détail des livrables attendus : modalités de restitution et supports + synthèse des vulnérabilités classées selon leur niveau de vulnérabilité et la portée de leur impact sur les SI + mesures correctives (priorité et budget) ;
 - o la durée totale de la mission exprimée en nombre de jours ;
 - o le tarif journalier HTVA appliqué.
- Informer Luxinnovation et la LHC avec un préavis minimum de 15 jours ouvrables de la date prévue pour la restitution des conclusions. Luxinnovation et la LHC se réservent la possibilité d'assister à la présentation du rapport final, sans que cette présence n'emporte de validation des conclusions du prestataire ;
- Rédiger le rapport final dans un langage accessible à un dirigeant non-expert, en évitant un jargon technique non défini.

NB : le plan d'action devra être synthétisé en respectant le modèle figurant à l'annexe 2, de manière à en faciliter la lecture par l'entreprise, et l'identification des aides publiques disponibles.

*Pour les prestataires référencés en cours d'année, le premier seuil annuel est calculé à compter du premier anniversaire de la date de référencement. Aucune exigence minimale n'est applicable pour la période antérieure à ce premier anniversaire.

Luxinnovation se réserve le droit de procéder à une revue périodique de l'activité de chaque prestataire référencé. En cas de non-atteinte du seuil minimal sur une période annuelle, Luxinnovation en informe le prestataire par écrit et lui accorde une période de remédiation de 6 mois. À l'issue de cette période, si le seuil n'est toujours pas atteint, le retrait du référencement peut être prononcé.

Déontologie et obligations comportementales

Les prestataires s'engagent à promouvoir le programme Fit 4 de manière loyale et transparente. Ils s'abstiennent de tout démarchage commercial agressif ou de toute pression exercée sur les entreprises en lien avec l'obtention de la subvention, et veillent à communiquer les informations relatives au programme de façon claire, complète et non trompeuse.

Ils s'assurent préalablement que le programme Fit 4 est adapté à la situation et aux besoins réels de l'entreprise, et s'abstiennent d'orienter une entreprise vers le programme dans un but principalement commercial ou lorsque ses besoins ne correspondent pas aux objectifs du programme.

Les prestataires sont tenus de respecter la confidentialité de l'ensemble des informations qui leur sont communiquées dans le cadre de leur mission. Cette obligation s'applique pendant toute la durée de la mission et

se poursuit après son terme, sans limitation de durée pour les informations présentant un caractère sensible ou stratégique.

Tout prestataire qui se trouve ou qui est susceptible de se trouver en situation de conflit d'intérêts avec une entreprise accompagnée est tenu d'en faire la déclaration écrite à Luxinnovation sans délai et au plus tard avant le démarrage de la mission. Constituent notamment des situations de conflit d'intérêts :

- toute participation, directe ou indirecte, au capital social de l'entreprise accompagnée ;
- l'exercice d'une fonction au sein des organes de direction ou de surveillance de cette entreprise ;
- l'existence d'un lien familial ou personnel étroit avec un dirigeant ou un actionnaire significatif de l'entreprise accompagnée ;
- toute situation analogue impliquant une personne morale liée au prestataire.

La déclaration d'un conflit d'intérêts n'entraîne pas automatiquement l'exclusion du prestataire. Luxinnovation examine chaque situation au cas par cas et se réserve le droit d'écarter le prestataire concerné si elle estime que le conflit d'intérêts est de nature à compromettre l'objectivité de la mission ou l'intégrité du programme. L'absence de déclaration d'un conflit d'intérêts connu du prestataire constitue un manquement grave susceptible d'entraîner le retrait immédiat de son référencement.

10.2 Obligations de l'entreprise bénéficiaire

Pour permettre la bonne exécution du programme, l'entreprise bénéficiaire s'engage à apporter à la société prestataire sa pleine coopération, notamment en :

- désignant en début de mission la personne en charge du projet au sein de l'entreprise ;
- mettant à disposition les moyens matériels et humains nécessaires à l'exécution de la mission, en ce compris la désignation d'un interlocuteur interne identifié, disponible et habilité à communiquer les informations utiles au bon déroulement de la mission ;
- communiquant au prestataire, dans les meilleurs délais, toute information, donnée ou document nécessaire à la réalisation du diagnostic et à l'élaboration du plan d'action ;
- suivant la procédure décrite ci-dessus et, en particulier, en respectant l'étape d'auto-évaluation au moyen de l'outil en ligne Cybercheck ;
- complétant le questionnaire d'évaluation mis à disposition par Luxinnovation à l'issue de la restitution des travaux. Ce retour conditionne le suivi qualitatif du programme et constitue une obligation à part entière de la participation au dispositif.

Accès aux résultats de la mission :

En acceptant les conditions du présent cahier des charges, l'entreprise bénéficiaire autorise la transmission à Luxinnovation et à la LHC du diagnostic et du plan d'action élaborés dans le cadre de la mission.

Ces informations seront analysées par Luxinnovation afin d'identifier toute mise en relation, tout accompagnement et tout financement approprié pour leur mise en œuvre. Elles sont traitées de manière confidentielle et ne sont pas communiquées à des tiers sans l'accord préalable de l'entreprise.

L'entreprise requérante donne également son accord pour que la LHC consolide les informations contenues dans le rapport dans le cadre de l'observatoire « Threat Observatory Platform » (« T.O.P. »).

Avec l'accord de l'entreprise, Luxinnovation peut utiliser le projet comme cas d'étude pour promouvoir le programme, sans divulguer d'informations confidentielles. Luxinnovation se réserve également le droit de publier le nom ou le logo de l'entreprise bénéficiaire dans le répertoire des entreprises ayant participé au programme.

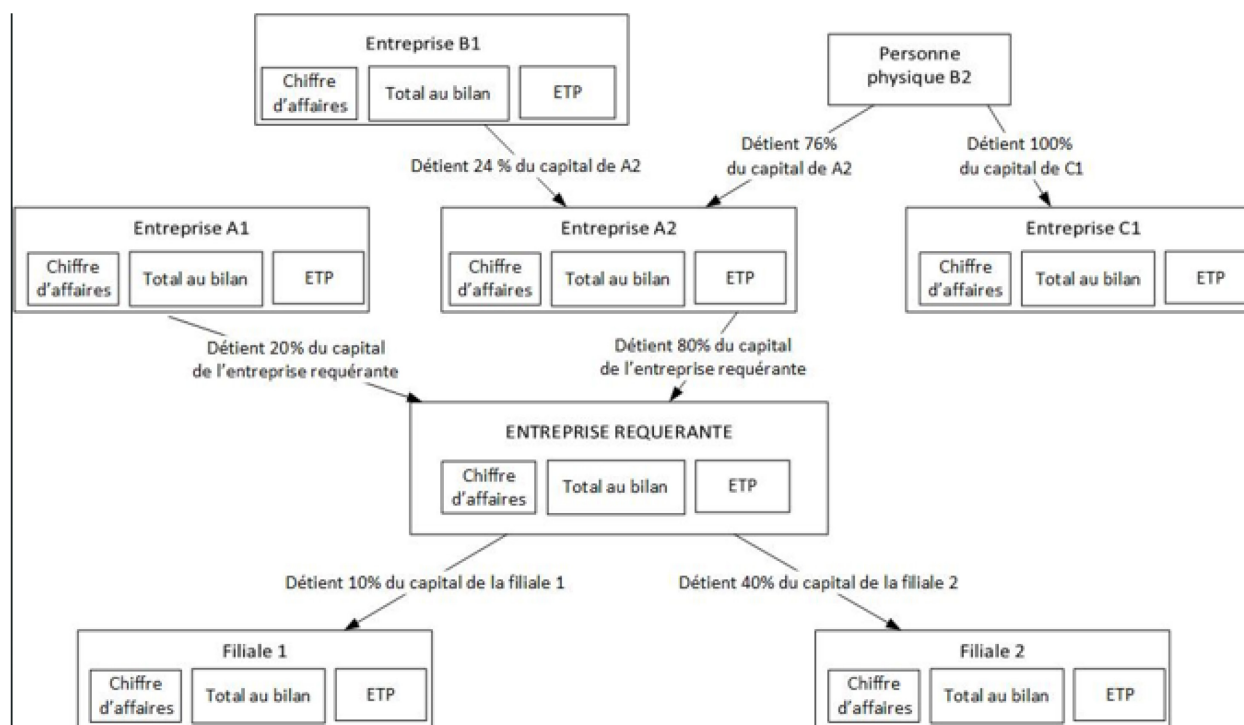
Le ministère de l'Économie et Luxinnovation se réservent la possibilité de modifier à tout moment et sans préavis les conditions du programme, ou de supprimer celui-ci.

Attribution de compétence

Le présent programme est régi par le droit luxembourgeois.

En cas de litige relatif à son existence, son interprétation ou son exécution, les tribunaux luxembourgeois seront seuls compétents.

ANNEXE 1 – Modèle d'organigramme



ANNEXE 2 – Plan d'action Fit 4 - Tableau de synthèse

Les informations du plan d'action doivent obligatoirement être synthétisées sous la forme ci-dessous.

Le consultant peut ajouter d'autres colonnes si cela est pertinent.

Recommandation <i>(Description synthétique et indication des pages concernées du rapport)</i>	Priorité	Horizon <i>(Court terme, MT, LT)</i>	Budget estimé	ROI <i>(Estimation)</i>	Type de frais <i>(Opex/Capex/ Conseil/Formation)</i>	Aide étatique éligible <i>(à compléter par Luxinnovation)</i>