

EXIGENCES DE CITI APPLICABLES AUX FOURNISSEURS

PROPRIÉTAIRES :
Head of Citi Procurement & Risk

DATE DE PUBLICATION :
Janvier 2015

RÉVISION :
Septembre 2026

VERSION :
9

SOMMAIRE

1	APERÇU GÉNÉRAL	3
2	ÉGALITÉ DES CHANCES EN MATIÈRE D'EMPLOI	5
3	LOIS ANTI-CORRUPTION	6
4	CADEAUX ET DIVERTISSEMENTS	7
5	ENGAGEMENT DES FOURNISSEURS ET PRINCIPES APPLICABLES AUX FOURNISSEURS	7
6	PROHIBITION DE L'ESCLAVAGE MODERNE	8
7	PERSONNEL DU FOURNISSEUR	10
8	GESTION DES FRAUDES	11
9	INTERACTION AVEC LES MÉDIAS ET APPARITIONS PUBLIQUES	13
10	COMMUNICATIONS ELECTRONIQUES ECRITES	14
11	ACTIVITÉS ET CONTRIBUTIONS POLITIQUES	15
12	ANTI-MONEY LAUNDERING (« AML »)	15
13	GESTION DES DOSSIERS	17
14	RÉSILIENCE/CONTINUITÉ DES ACTIVITÉS	19
15	NORMES MONDIALES EN MATIÈRE D'EXAMEN DES ANTÉCÉDENTS	26
16	DÉPENSES	28
17	SÉCURITÉ DES INFORMATIONS (IS)	29
18	DIRECTIVES RELATIVES A LA SECURITE SUR LE LIEU DE TRAVAIL	70
19	INTELLIGENCE ARTIFICIELLE/APPRENTISSAGE AUTOMATIQUE (Y COMPRIS L'IA GENERATIVE/L'IA AGENTIQUE)	71
20	PLAINTES DE CLIENTS	72
21	POLITIQUE RELATIVE AUX OPÉRATIONS PERSONNELLES ET AUX INVESTISSEMENTS	73
22	NORMES EN MATIÈRE DE FACTURATION	73
23	POLITIQUE D'ABSENCE OBLIGATOIRE	74
	ANNEXE - DÉFINITIONS	75

1 APERÇU GÉNÉRAL

1.1. Exigences générales

Les présentes Exigences de Citi à l'égard des Fournisseurs (« **Exigences** ») détaillent certaines des obligations que les Fournisseurs doivent respecter dans le cadre de leurs relations commerciales avec Citi. Certaines Exigences s'appliquent à tous les Fournisseurs, tandis que l'applicabilité d'autres Exigences à un Fournisseur particulier dépend des types de produit(s) et de service(s) que le Fournisseur procure à Citi (ces derniers sont résumés dans la Section 1.2 ci-dessous et sont indiqués au début de chaque disposition qui y figure). Les termes commençant par une majuscule auront le sens qui leur est attribué dans les présentes, y compris dans l'Annexe ci-jointe, à moins qu'un tel sens ne soit indiqué dans les présentes, auquel cas ils auront le sens qui leur est attribué dans le Contrat, tel que défini ci-dessous.

Ces Exigences constituent des obligations contractuelles en vertu des accords conclus entre le Fournisseur et Citi (y compris, mais sans s'y limiter, les documents transactionnels, par exemple, les ordres de travail, les calendriers de licence) (chacun étant un « **Contrat** »), et s'ajoutent à toutes les obligations spécifiées dans tout Contrat, à toutes les obligations en vertu du Droit applicable (comme défini ci-dessous), à tout avis de Citi informant le Fournisseur de ses obligations dans ce cadre (chacun étant un « **Avis** »), ou à toute autre exigence plus spécifique mise en œuvre par les activités ou fonctions de Citi. En cas de conflit entre l'une des exigences susmentionnées et les présentes exigences, ce sont les obligations et exigences les plus restrictives qui s'appliquent. Les Fournisseurs doivent jouer un rôle proactif et consulter leur principal contact commercial Citi (ou son représentant) pour toute question concernant ces Exigences, y compris toute modification de celles-ci, toute demande d'exemption de celles-ci ou tout conflit perçu dans celles-ci ou conflit avec le Droit applicable.

Le Fournisseur devra rapidement se conformer à toute demande raisonnable que Citi pourra soumettre au Fournisseur relativement à des données que Citi exige liées aux services du Fournisseur ou à son Personnel en association avec l'obligation de Citi de se mettre en conformité avec la loi applicable. Le non-respect par le Fournisseur de ces obligations sera considéré comme une violation substantielle des conditions du présent Accord.

Le non-respect de ces Exigences ou de toute exigence supplémentaire spécifiée par une entreprise de Citi avec laquelle le Fournisseur fait affaire peut entraîner la résiliation du Contrat conclu entre le Fournisseur et Citi. En outre, les violations des Exigences peuvent également constituer des infractions au droit applicable et entraîner des dommages civils dus à Citi (ou à des tiers) ou des sanctions pénales pour le Fournisseur. Le Fournisseur ne peut pas utiliser la conformité à ses propres politiques comme substitut à son obligation de se conformer à toute disposition des présentes Exigences sans le consentement écrit de Citi.

1.2. Exigences applicables aux Fournisseurs sélectionnés

Le tableau ci-dessous énumère certaines exigences applicables à des Fournisseurs spécifiques, selon les critères d'applicabilité qui y sont définis. Les sections non mentionnées ci-dessous s'appliquent à TOUS les Fournisseurs.

Section n°	Titre de la section	Applicabilité
2	ÉGALITÉ DES CHANCES EN MATIÈRE D'EMPLOI / ACTION POSITIVE	Applicable aux contrats et bons de commande nécessaires à l'exécution d'un contrat conclu entre Citi et le gouvernement fédéral américain. En cas de doute quant à savoir si le contrat ou le bon de commande constitue un contrat de sous-traitance ou un bon de commande du gouvernement fédéral, veuillez ajouter la mention « Le cas échéant » au début ou à la fin de la clause, selon le cas.
12	LUTTE CONTRE LE BLANCHIMENT D'ARGENT	Applicable aux Fournisseurs qui dispensent certains services liés au client (c'est-à-dire l'intégration, le filtrage des comptes et des transactions clients) ou la livraison de données/d'indicateurs liés aux activités susmentionnées ; <u>ET/OU</u> Aux Fournisseurs qui agissent en tant qu'intermédiaires en ce qui concerne les espèces ou les instruments financiers (p. ex., collecte de dépôts à distance, services de messagerie, de transport blindé ou de coffre-fort).
13	GESTION DES DOSSIERS	Applicable aux Fournisseurs qui accèdent à/traitent/stockent des Informations de Citi.
14	CONTINUITÉ DES ACTIVITÉS	Applicable aux Fournisseurs qui fournissent des services ou hébergent des infrastructures technologiques/applications utilisées par Citi. Le Business Activity Owner (BAO) de Citi est responsable de la communication de l'applicabilité et des exigences en matière de continuité des activités au Fournisseur.
15	NORMES MONDIALES EN MATIÈRE D'EXAMEN DES ANTÉCÉDENTS	Applicable aux Fournisseurs qui fournissent des services à Citi.
16	DÉPENSES	Applicable aux Fournisseurs contractuellement éligibles à réclamer le défraiement de dépenses professionnelles remboursables.
17	SÉCURITÉ DES INFORMATIONS (IS)	Applicable aux Fournisseurs, y compris les Sous-traitants, qui accèdent aux informations de Citi, les traitent, les gèrent ou les stockent ; <u>ET/OU</u> aux Fournisseurs chargés, en tant qu'hébergeurs, des applications en ligne portant la marque Citi ; <u>ET/OU</u> aux Fournisseurs disposant d'une connexion aux ressources réseau de Citi ; <u>ET/OU</u> aux Fournisseurs nécessitant un accès sans accompagnement aux locaux de Citi.
18	DIRECTIVES RELATIVES À LA SÉCURITÉ SUR LE LIEU DE TRAVAIL	
19	INTELLIGENCE ARTIFICIELLE/APPRENTISSAGE AUTOMATIQUE (y compris l'IA générative/l'IA agentique)	Applicable aux Fournisseurs qui utilisent l'Intelligence artificielle/Apprentissage automatique (AI/AA) tel que défini par Citi dans toute partie du produit/service qu'ils fournissent.
20	POLITIQUE RELATIVE AUX OPÉRATIONS PERSONNELLES ET AUX INVESTISSEMENTS	Applicable aux Fournisseurs qui nécessitent un accès régulier aux renseignements importants non rendus publics (MNPI) dans le cadre de leurs responsabilités professionnelles chez Citi.

Section n°	Titre de la section	Applicabilité
23	OLITIQUE D'ABSENCE OBLIGATOIRE	Cette Politique s'applique aux personnes non salariées (« Intervenants ») occupant des postes sensibles (tels que définis dans le glossaire) (« Intervenants occupant des postes sensibles »), ainsi qu'aux responsables hiérarchiques et superviseurs directs des employés occupant des postes sensibles (« Responsables ») et aux interlocuteurs professionnels de Citi des personnes non salariées occupant des postes sensibles.

2 ÉGALITÉ DES CHANCES EN MATIÈRE D'EMPLOI

2.1 Égalité des chances en matière d'emploi.

Citi a développé un programme et des politiques en faveur de l'égalité des chances en matière d'emploi qui sont conçus pour garantir l'égalité des chances en matière d'emploi à toutes les personnes qualifiées sans tenir compte de l'origine ethnique, de la couleur de peau, de la religion, du sexe biologique, de l'orientation sexuelle, de l'identité de genre, de l'origine nationale, de la citoyenneté, du statut d'immigré, de l'âge, de l'état civil, des informations génétiques, du handicap, du statut d'ancien combattant protégé ou de toute autre caractéristique protégée en vertu de la loi.

Les Fournisseurs doivent se conformer, et veiller à ce que leur personnel se conforme, aux obligations de toutes les lois et réglementations applicables en matière de non-discrimination, y compris, mais sans s'y limiter, à toutes les lois ou réglementations qui leur sont notifiées par écrit par Citi et auxquelles ils doivent se conformer.

Les Fournisseurs doivent examiner et prendre les mesures appropriées conformément à la déclaration de politique d'égalité des chances en matière d'emploi de Citi aux États-Unis, disponible à l'adresse suivante www.citigroup.com/qGlobal/eeo-aa-policy.

2.2 Marchés publics

Les contrats et les bons de commande nécessaires à l'exécution d'un contrat de Citi passé avec le gouvernement fédéral doivent contenir textuellement la clause suivante, en gras, comme indiqué ci-dessous. (En cas d'incertitude à savoir s'il s'agit d'un contrat de sous-traitance/d'un bon de commande passé avec le gouvernement fédéral, opter pour la prudence en ajoutant la mention « S'il y a lieu » au début de la section.)

[Le cas échéant,] le Fournisseur se conformera à toutes les lois fédérales anti-discrimination applicables et certifie qu'il n'exploite aucun programme en violation d'une loi fédérale anti-discrimination applicable quelle qu'elle soit

2.3 Annexe relative aux marchés publics

Les contrats et les bons de commande nécessaires à l'exécution d'un contrat de Citi passé avec le gouvernement fédéral doivent contenir l'avis suivant dans l'annexe du contrat de sous-traitance ou du bon de commande. (En cas d'incertitude à savoir s'il s'agit d'un contrat de sous-traitance/d'un bon de commande passé avec le

gouvernement fédéral, opter pour la prudence en ajoutant la mention « S'il y a lieu » à la fin de l'avis ci-dessous.)

En tant que prestataire agissant pour le gouvernement fédéral, Citigroup fournit par la présente au prestataire ou au Fournisseur soussigné un avis écrit de nos obligations quant à l'égalité des chances en matière d'emploi pour le compte des anciens combattants protégés et des personnes atteintes de handicap. Citigroup est en pleine conformité avec la Section 503 du Rehabilitation Act et du Vietnam Era Veterans' Readjustment Assistance Act, ainsi qu'à ses règlements applicables en vertu des articles 41 C.F.R. § 60-741 et 41 C.F.R. § 60-300, respectivement. Notre Equal Employment Opportunity Policy Statement (Déclaration de politique d'égalité des chances en matière d'emploi) se trouve à l'adresse www.citigroup.com/global/eeo-aa-policy. Toute question concernant notre déclaration de politique EEO peut être adressée au contact indiqué dans ladite déclaration.

[Le cas échéant], nous vous demandons de prendre les mesures appropriées conformément à notre Policy Statement et aux réglementations en vigueur.

3 LOIS ANTI-CORRUPTION

Citi dispose de politiques, de procédures et de contrôles internes raisonnablement conçus pour lui permettre de se conformer aux lois anti-corruption applicables et interdit strictement les actes de corruption ou les paiements de facilitation sous quelque forme que ce soit. Les Fournisseurs (y compris les apporteurs d'affaires), leur personnel ou toute personne agissant au nom de Citi, directement ou indirectement, doivent mener leurs activités conformément aux normes éthiques les plus élevées et conformément au US Foreign Corrupt Practices Act (FCPA), au UK Bribery Act (UKBA), chacune sous sa forme amendée, et à toutes les autres lois locales applicables en matière de lutte contre la corruption en vigueur dans les pays dans lesquels Citi opère.

Ni le Fournisseur, ni aucun membre de son Personnel opérant au nom de Citi, ou dans le cadre d'un quelconque accord ou de la relation qui lie le Fournisseur à Citi, (i) n'effectuera, ne confèrera, n'autorisera ou n'offrira aucun paiement, avantage ou toute autre chose de valeur à quiconque ; ou (ii) ne recevra ou n'acceptera tout paiement, avantage ou toute autre chose de valeur de la part de quiconque, dans chacun des cas (i)-(ii) en violation du FCPA, de l'UKBA ou de toute autre loi en matière de lutte contre la corruption. Le Fournisseur et son personnel doivent mener leurs activités et transactions pour le compte de Citi, ou dans le cadre de l'un des accords ou de la relation qui lie le Fournisseur à Citi, en conformité avec les exigences, y compris celles énoncées dans la présente section. Le Fournisseur et son Personnel devront également maintenir un programme de conformité aux lois anti-corruption, et des politiques et procédures conçues et appliquées pour assurer sa conformité à toutes les lois anti-corruption.

Pour un aperçu du programme anti-corruption de Citi, veuillez consulter [Citigroup's Investor Relations](#) (Relations avec les investisseurs de Citigroup, sous Citi Policies [Politiques de Citi], sélectionnez AB&C Program [Programme anti-corruption]).

4 CADEAUX ET DIVERTISSEMENTS

Il est interdit aux Fournisseurs ainsi qu'à leur Personnel d'offrir des cadeaux ou quoi que ce soit de valeur (y compris des divertissements) aux employés de Citi, lorsque cela peut engendrer un conflit d'intérêts réel ou apparent, représente une contrepartie ou est susceptible de compromettre l'intégrité ou le jugement de l'employé ou risque de quelque autre façon que ce soit d'avoir des répercussions inappropriées sur la prise de décision de l'employé dans le cadre de son travail, ou d'aller à l'encontre des lois applicables de quelque façon que ce soit. Sans limiter ce qui précède, l'employé doit respecter la section Cadeaux et divertissements interdits de la Citi Gifts and Entertainment Standard. Les Fournisseurs et leur Personnel ne doivent pas offrir de cadeaux commerciaux non monétaires dépassant une valeur totale de 300 \$ américains par personne et par année civile à un employé de Citi.

Lorsqu'un Fournisseur offre un divertissement commercial (par exemple une invitation à un repas, à une manifestation culturelle ou sportive ou à tout autre événement comparable) à un employé de Citi, le Fournisseur devra être présent à l'événement. Le divertissement devra être approprié, usuel et raisonnable, sans être luxueux ou d'une fréquence excessive. En outre, si le Fournisseur n'est pas présent à l'événement, le divertissement sera considéré comme un cadeau commercial et soumis aux seuils de déclaration applicables de la Citi Gifts and Entertainment Standard. Le Fournisseur ne peut pas, au nom de Citi ou prétendument au nom de Citi, offrir quelque chose de valeur, y compris aux propres frais du Fournisseur ou aux frais d'un employé de Citi, à qui que ce soit, directement ou indirectement, ou inciter une autre personne à faire la même chose, si cela constituait (de façon effective ou raisonnablement perçue comme telle) un acte de corruption, ou était autrement inapproprié ou en violation de la loi applicable.

5 ENGAGEMENT DES FOURNISSEURS ET PRINCIPES APPLICABLES AUX FOURNISSEURS

<https://www.citigroup.com/citi/fournisseur/> Citi collabore avec ses Fournisseurs dans le cadre de plusieurs initiatives et s'efforce de faire connaître son programme d'achats auprès de Fournisseurs potentiels issus des communautés que nous servons. Par ailleurs, ces collaborations visent à identifier des Fournisseurs prometteurs, en particulier ceux qui proposent des solutions innovantes pour répondre aux nouveaux défis commerciaux. Des informations supplémentaires sur les attentes de Citi envers les Fournisseurs sont disponibles sur le site [Doing Business with Citi](#) sous :

[Citi Statement of Supplier Principles](#)
[Citi Sustainable Progress Strategy](#)

6 PROHIBITION DE L'ESCLAVAGE MODERNE

Citi s'engage à maintenir des pratiques visant à identifier et à prévenir le risque de traite des êtres humains et d'esclavage moderne pouvant survenir au sein de son organisation ou dans ses chaînes d'approvisionnement. Les Fournisseurs de Citi doivent adhérer aux exigences énoncées ci-dessous et développer des politiques, des procédures et des pratiques efficaces à l'échelle de l'entreprise afin d'identifier et de traiter le risque d'exposition à l'esclavage moderne et la traite des êtres humains au sein de leurs propres organisations et chaînes d'approvisionnement. Les Fournisseurs sont tenus de remplir le Questionnaire sur la responsabilité sociale des entreprises de Citi lorsque celle-ci en fait la demande, en incluant toutes les informations supplémentaires pertinentes, afin de permettre à Citi d'évaluer l'exposition au risque et les mesures d'atténuation potentielles, en particulier chez les Fournisseurs présents dans des secteurs et des zones géographiques à risque élevé. Les sous-traitants du Fournisseur doivent suivre le même processus.

6.1 Lutte contre le travail des enfants

Les Fournisseurs ne doivent pas recourir au travail des enfants. Le terme « enfant » désigne toute personne n'ayant pas atteint l'âge minimum d'admission à l'emploi prévu par la législation applicable ou, en l'absence d'une telle législation, toute personne âgée de moins de 15 ans ou n'ayant pas encore atteint l'âge de fin de scolarité obligatoire, l'âge le plus élevé étant retenu. Sous réserve de l'interdiction absolue relative à l'utilisation du travail des enfants, si des travailleurs de moins de 18 ans sont employés, un soin particulier doit être pris quant aux fonctions qu'ils exercent et aux conditions dans lesquelles ils sont tenus de travailler, afin de faire en sorte qu'ils ne soient victimes d'aucun préjudice physique, mental ou autre qui soit une conséquence directe ou indirecte de leur travail ou de leurs conditions de travail.

6.2 Emploi librement choisi

Le Fournisseur doit s'assurer qu'aucun collaborateur n'est contraint, soumis à une coercition mentale ou physique, lié par une dette, un contrat d'engagement forcé ou toute autre forme de servitude, astreint à du travail pénitentiaire involontaire, victime de traite des êtres humains ou d'esclavage ou affecté à toute forme de travail obligatoire, ceci comprenant les heures supplémentaires imposées. Tout travail doit être effectué volontairement. Les obligations du Fournisseur en vertu de ce qui suit comprennent, entre autres :

1. **Contrats, salaires et heures de travail** : Les collaborateurs doivent disposer d'un document écrit, rédigé dans une langue et un style aisément compréhensibles, exposant clairement les conditions de leur emploi ou de leur engagement ainsi que leurs droits et obligations. Ce document écrit devra énoncer, entre autres, des conditions transparentes en ce qui concerne les salaires, les heures supplémentaires, les périodes de paiement, les heures de travail et les droits en matière de pauses et de congés. Ces conditions écrites devront être remises au collaborateur avant le début de son activité. Elles devront être respectées par l'employeur et conformes aux normes du secteur

ainsi qu'aux exigences minimales des lois applicables et des conventions collectives en vigueur sur le lieu d'exécution du travail.

2. **Droit de libre résiliation du contrat de travail** : Les travailleurs doivent avoir le droit de mettre fin à leur emploi librement, selon le cas, après une période raisonnable de préavis conformément aux lois et conventions collectives et sans l'imposition de sanctions abusives.
3. **Traitement inhumain** : Les travailleurs, leurs familles et leurs proches ne doivent pas être soumis à des traitements durs ou inhumains, notamment : punitions corporelles, violences physiques, psychologiques ou sexuelles, violences verbales, harcèlement ou intimidation. Les travailleurs immigrés, leur famille et les personnes qui leur sont étroitement associées ne doivent pas faire l'objet de discrimination dans leurs conditions de travail au motif de leur nationalité.
4. **Salaires, avantages sociaux et heures de travail** : La rémunération doit être conforme à toutes les lois salariales applicables, y compris celles relatives au salaire minimum, aux heures supplémentaires et aux avantages sociaux légaux. Les employés doivent percevoir l'intégralité de leur salaire, dans les délais impartis, et disposer de bulletins de paie transparents. Aucune retenue punitive ni aucune retenue sur le salaire ou les prestations ne pourra être effectuée à titre de mesure disciplinaire. La durée hebdomadaire du travail ne doit pas dépasser le maximum fixé par la législation locale et les heures supplémentaires doivent être effectuées sur une base volontaire, dans les limites légales ; le refus d'effectuer des heures supplémentaires ne doit pas donner lieu à des sanctions.
5. **Interdiction de confiscation des documents d'identité** : Les documents d'identité, documents de voyage, passeports ou autres documents officiels ou autres objets précieux des travailleurs ne doivent pas être confisqués ou retenus comme condition de leur emploi, et la rétention de biens ne doit pas servir directement ou indirectement à restreindre les libertés des travailleurs ou à créer une situation d'esclavage sur le lieu de travail.
6. **Interdiction de frais de recrutement et des servitudes pour dette** : Les frais ou coûts liés à l'embauche des travailleurs (y compris mais sans y être limité, les frais liés aux visas de travail, frais de déplacement et frais de traitement de document) ne peuvent pas être imputés aux travailleurs, que ce soit directement ou indirectement. De même, les travailleurs ne seront pas tenus d'effectuer des paiements ayant pour but ou pour effet de créer une situation d'esclavagisme sur le lieu de travail, y compris des paiements garantissant leur sécurité, et ne seront pas tenus de rembourser des dettes par le biais du travail. S'il s'avère que des frais ou des coûts ont été facturés aux travailleurs dans le cadre du processus de recrutement ou ont été engagés au cours de la relation de travail, le Fournisseur prendra les mesures raisonnables pour que ces coûts soient remboursés sans délai. Lorsqu'il est

nécessaire de recruter des travailleurs par l'intermédiaire d'une tierce partie, telle qu'une agence pour l'emploi, seules des agences pour l'emploi de bonne réputation devront être engagées. Lorsque les travailleurs sont recrutés pour être employés directement, seules des agences de recrutement de bonne réputation doivent être engagées. L'interdiction des frais de recrutement à la charge des travailleurs s'applique à tous les recruteurs, agents et sous-agents. Les Fournisseurs doivent mettre en place des mesures de contrôle afin de garantir le respect des exigences. **Libre circulation** : Les travailleurs doivent être libres de se déplacer sans restrictions déraisonnables et ne doivent pas être physiquement confinés sur le lieu de travail ou dans d'autres lieux contrôlés par l'employeur (par exemple, des logements collectifs). Aucun collaborateur ne doit être contraint de résider dans un logement contrôlé par l'employeur, sauf lorsque cela est nécessaire en raison de la localisation ou de la nature du travail effectué.

7. **Plaintes sans représailles** : Les travailleurs doivent être libres de déposer des plaintes auprès de leurs employeurs au sujet du traitement que l'employeur leur réserve et les travailleurs ne doivent pas subir de préjudice, de représailles ou de victimisation pour avoir déposé une plainte.

7 PERSONNEL DU FOURNISSEUR

7.1 Formation, affectation, réaffectation et gestion du Personnel du Fournisseur

Le Fournisseur emploiera un nombre suffisant de personnes ayant une formation, une éducation, une expérience et des compétences appropriées pour exécuter les Services de la manière la plus efficace conformément à tout Contrat et justifiera les qualifications de ces personnes sur demande. Une fois que du personnel a été affecté à un projet, le Fournisseur ne doit pas le réaffecter ni l'utiliser à d'autres tâches susceptibles de réduire sa disponibilité pour le projet, sauf accord écrit préalable de Citi. Le Fournisseur doit également affecter son personnel aux projets de manière à limiter les perturbations liées à la nécessité d'une réorientation. Le Fournisseur veillera à ce que son personnel ne se présente pas comme employé ou agent de Citi, ni ne cherche à être traité comme tel à quelque fin que ce soit, y compris pour prétendre à des avantages sociaux offerts par Citi, à des prestations d'invalidité, à des cotisations ou prestations de sécurité sociale, à des cotisations fédérales d'assurance chômage, à des prestations d'assurance chômage de l'État ou à des retenues fédérales sur le revenu. Le Fournisseur est seul responsable de toutes les obligations liées à l'employeur en ce qui concerne son Personnel, y compris, mais sans s'y limiter, le maintien de toutes les couvertures d'assurance requises, le dépôt de toutes les déclarations d'impôts applicables et le versement de tous les paiements et dépôts d'impôts requis d'une manière compatible avec le statut d'entrepreneur indépendant du Fournisseur.

7.2 Remplacement du personnel du Fournisseur

Le Fournisseur procédera au remplacement de tout membre du personnel affecté par ses soins à un projet si Citi lui notifie que cette personne est jugée inacceptable pour

Citi pour toute raison non discriminatoire. Le Fournisseur s'engage en outre à retirer et à remplacer tout membre du personnel affecté à un projet et à lui interdire de fournir des services à Citi (ou d'assumer toute responsabilité relative à la prestation ou à la supervision des services) dès lors qu'il n'est pas en mesure ou n'est pas disposé à fournir les services de manière professionnelle et dans les délais impartis.

7.3 Politiques relatives au personnel du Fournisseur

Le Fournisseur déclare, garantit et s'engage à tenir à jour et à administrer efficacement des politiques et procédures complètes pour qualifier son Personnel constitué de personnes physiques affectées à la prestation de Services sur site pour Citi, et ces politiques et procédures incluent la vérification des autorisations de travail, la vérification des antécédents professionnels et des condamnations pénales, comme indiqué plus en détail dans le présent document, et le dépistage de drogues avant l'embauche, le tout dans la mesure autorisée par le Droit applicable et toute convention collective applicable. Sans porter atteinte à la portée générale de ce qui précède, le Fournisseur déclare, garantit et s'engage en outre à disposer de dispositifs et de procédures permettant d'assurer sa pleine conformité à l'ensemble de la législation applicable en matière d'immigration, notamment en validant que tout membre de son personnel affecté à Citi est autorisé à travailler pendant toute la durée de sa mission, conformément à ladite législation. Sur demande, le Fournisseur remettra rapidement à Citi une preuve écrite de l'autorisation de travail de tout ou partie du Personnel du Fournisseur affecté à Citi et de sa conformité avec le Droit applicable en matière d'immigration. Il remplacera tout Personnel ne disposant pas d'une autorisation de travail conforme au Droit applicable par des employés dûment qualifiés, en incluant toute la formation et l'orientation nécessaires pour garantir la prestation opportune et efficace des Services, dans chaque cas sans frais supplémentaires.

7.4 Propriété du Fournisseur

Afin de se conformer aux lois et règlements applicables dans les juridictions où Citi exerce ses activités, sur demande de Citi, les Fournisseurs sont tenus de communiquer les informations relatives aux propriétaires, personnes physiques et/ou morales, y compris les détenteurs de contrôle immédiat du Fournisseur jusqu'au bénéficiaire effectif ultime exerçant directement ou indirectement la propriété ou le contrôle, notamment par influence ou tout autre moyen, sur l'engagement, le produit ou le service.

8 GESTION DES FRAUDES

Dans le cadre des efforts de Citi pour identifier et atténuer le risque de fraude (« Gestion des fraudes ») :

8.1 Tous les Fournisseurs doivent :

1. Coopérer à toute enquête menée par Citi concernant tout vol, fraude ou autre activité criminelle ou méfait potentiel suspecté ou allégué, ainsi qu'à toute poursuite pour comportement frauduleux ou criminel, dans toute la mesure permise par la loi.
2. S'assurer du signalement et de la transmission en temps utile de tout événement de fraude potentielle à Citi par le biais de la [Ethics Hotline](#). Cela

inclut, sans s'y limiter, les tentatives, les soupçons, les allégations ou les cas de vol, de fraude (par exemple, la soumission de données sciemment fausses, inexactes ou déformées concernant le Fournisseur, les systèmes de facturation, la disparition de fonds ou de titres, etc.), les activités criminelles ou les actes répréhensibles impliquant Citi, un employé de Citi, un Fournisseur ou un agent de Citi ou un non-employé de Citi (par exemple, les employés temporaires et les sous-traitants) ;

3. Autoriser le suivi et la supervision par Citi et ses représentants, et collaborer dans les enquêtes menées par Citi et les autorités chargées de l'application de la loi sur des activités potentiellement frauduleuses impliquant ledit Fournisseur ;
4. Signaler, en temps opportun, tout conflit d'intérêts (y compris les conflits d'intérêts entre Fournisseurs/Employés du Fournisseur et/ou Employés de Citi) dont les Fournisseurs sont informés ; et
5. Soutenir les processus de prévention de la fraude de Citi pendant la mise en place ou la mise à jour du compte bancaire d'un Fournisseur dans le système de paiement du Fournisseur de Citi.

8.2 En outre, les Fournisseurs qui délivrent des services intrinsèquement plus exposés au risque de fraude **sont tenus** de :

1. Documenter et suivre un programme de gestion des risques de fraude qui identifie les risques de fraude importants liés aux services fournis à Citi, ainsi que les contrôles et procédures mis en place pour atténuer ces risques.
2. Suivre une formation de sensibilisation à la fraude (dans les 90 jours civils suivant l'embauche et chaque année par la suite) et former le personnel sur les éléments spécifiques du risque de fraude qui se rapportent aux services particuliers fournis à Citi.
3. Surveiller les tentatives de fraude et maintenir des contrôles efficaces pour atténuer le risque de fraude dans le cadre des services fournis à Citi, documenter les procédures de contrôle et tester l'efficacité des contrôles, en signalant toute lacune au Business Activity Owner (BAO).
4. Fournir toutes les informations requises pour la diligence raisonnable/la surveillance continue/l'évaluation de l'exposition au risque de fraude au Business Activity Owner (BAO).
5. La diligence raisonnable inclut l'utilisation du modèle d'évaluation d'impact de la fraude des tiers (Third-Party Fraud Impact Assessment Template, TP-FIAT), conçu pour réaliser des évaluations des dispositifs de contrôle des Fournisseurs en matière de capacité à atténuer les risques de fraude. Cette procédure opérationnelle décrit un ensemble d'étapes à effectuer par le Business Activity Owner (« BAO ») ou le Third-Party Officer (« TPO ») et le Fraud Risk Management Officer (« FRMO ») pour identifier et gérer le risque de fraude.

8.3 Parmi les Fournisseurs présentant un risque de fraude inhérent plus élevé, on peut citer, entre autres, ceux qui :

1. Ont accès à des données classées Confidentielles ou de niveau supérieur (lorsqu'elles ne sont pas sous le contrôle ou la supervision directe de Citi) qui peuvent être utilisées pour permettre la fraude, comme l'accès aux comptes internes, aux transactions financières, aux transactions en espèces.
2. Peuvent se connecter aux réseaux/systèmes de Citi ; et
3. Fournissent, soutiennent ou ont accès à des services et des capacités qui pourraient être ciblés pour commettre ou permettre des fraudes, notamment :
 - a) L'identification, l'intégration ou le traitement des demandes de nouveaux clients ;
 - b) Les activités de paiement/transfert de fonds de Citi ou du Client et/ou l'authentification des clients Citi qui accèdent à ces services ;
 - c) Le fait d'effectuer, de vérifier ou d'apporter des modifications aux données de Citi ou aux données clients de Citi (par exemple, démographiques) ;
 - d) La fourniture, la gestion ou l'autorisation d'instruments transactionnels (p. ex., cartes bancaires, portefeuilles électroniques, chéquiers, etc.) ;
 - e) La fourniture ou la prise en charge d'activités de gestion de la fraude opérationnelle à Citi, en relation avec la prévention, la détection ou la réponse aux incidents frauduleux ;
 - f) La fourniture d'un accès physique aux espèces, aux instruments financiers et aux actifs/marchandises physiques ;
 - g) L'accès sans escorte ou en dehors des heures d'ouverture dans les installations de Citi ;
 - h) Les états financiers : activités comptables, telles que les entrées portées au grand livre et aux dossiers comptables ;
 - i) L'obtention et l'utilisation de récompenses pour des activités incitatives.

9 INTERACTION AVEC LES MÉDIAS ET APPARITIONS PUBLIQUES

Citi Enterprise Services and Public Affairs est le seul service autorisé à publier des communiqués de presse ou des déclarations publiques au nom de Citi. Les Fournisseurs ne peuvent publier aucun communiqué de presse qui identifie directement ou indirectement Citi, aucun Contrat ou arrangement entre un Fournisseur et Citi ni aucun produit ou service acquis auprès d'un Fournisseur par Citi. Les Fournisseurs ne pourront permettre ni effectuer aucune opération de relations publiques relatives à Citi auprès de Clients, d'employés de Citi, d'autres Fournisseurs de Citi, d'autres clients des Fournisseurs ou de toute autre tierce partie sans l'accord préalable écrit du contact professionnel principal concerné.

Les Fournisseurs ne pourront publier ou mettre en ligne aucun contenu sous forme écrite ou électronique (y compris des livres, articles, podcasts, webcasts, blogs, publications sur des sites Web, photos, vidéos, publications sur les réseaux sociaux ou autres supports), animer ou faire des discours, donner des interviews ou faire des apparitions publiques qui mentionneraient Citi, les activités de Citi, les Clients, les produits ou services de Citi, sans l'accord préalable écrit de leur principal interlocuteur commercial chez Citi et du responsable des affaires publiques du pays concerné.

Que ce soit dans le cadre ou non de la fourniture de services ou de produits à Citi, les Fournisseurs ne pourront utiliser aucun indice, marque commerciale, marque de service, nom commercial, logo, symbole ou nom de marque exclusif de Citi, sans l'accord préalable écrit de Citi au cas par cas. Les Fournisseurs ne sont pas autorisés à utiliser le nom, le logo ou les marques commerciales, les installations ou les relations de Citi à des fins lucratives ou pour des activités extérieures à Citi (y compris sur du papier à en-tête, des sites Web personnels, des blogs ou d'autres sites de réseaux sociaux). En outre, les Fournisseurs ne peuvent utiliser le nom, les sites ou les relations de Citi à des fins caritatives ou pro bono.

10 COMMUNICATIONS ELECTRONIQUES ECRITES

Lors des échanges avec le personnel de Citi, ou en réponse à leurs obligations pour le compte ou au nom de Citi, les Fournisseurs sont autorisés à utiliser uniquement les équipements, systèmes et services de communications électroniques fournis, validés ou approuvés par Citi. Les canaux de communication électronique de Citi nouveaux, élargis ou modifiés, qu'il s'agisse d'un outil autonome ou intégré à une plateforme plus large, fourni par Citi ou par un tiers, doivent être approuvés conformément aux Exigences applicables de Citi contenues dans le présent document ou pour lesquelles le BAO a informé le Fournisseur par écrit. Toute communication des activités de Citi avec des employés de Citi sur des plateformes de messagerie non validées par Citi, telles que WhatsApp, WeChat, LINE, Slack, Signal, Telegram, iMessage, SMS, Viber ou d'autres plateformes électroniques interactives, est interdite.

De plus, les Fournisseurs ne peuvent prétendre à un quelconque respect de la confidentialité vis-à-vis des Communications électroniques écrites créées, identifiées, utilisées, consultées, téléchargées, stockées, transmises, reçues ou supprimées via les Équipements, systèmes et services de communications fournis par Citi. Citi est susceptible de surveiller les Équipements, systèmes et services de communication électroniques et le contenu des Communications électroniques. Ces communications électroniques sont la propriété de Citi et peuvent être conservées conformément aux exigences applicables en matière de conservation des enregistrements (sous réserve de la loi et de la réglementation locales).

<https://policydirectory.citi.net/cpd/ layouts/15/DocIdRedir.aspx?ID=CPDPROD-13-8739>

11 ACTIVITÉS ET CONTRIBUTIONS POLITIQUES

Diverses lois, telles que celles relatives à : l'influence étrangère ; le financement des campagnes électorales ; les cadeaux et les invitations ; le lobbying législatif, citoyen, de bonne volonté et réglementaire ; les marchés publics et les pratiques de « pay-to-play » ; ainsi que les valeurs mobilières, régissent les activités politiques et les obligations de déclaration liées à ces activités, tant pour Citi que pour ses fournisseurs. Toute activité politique des Fournisseurs qui ne respecte pas la politique ou les normes, la loi ou la réglementation pertinentes de Citi est interdite.

L'activité politique comprend, mais sans s'y limiter :

1. Le versement de contributions politiques au nom de l'entreprise ou à titre personnel, la sollicitation du versement de contributions politiques, l'utilisation de fonds ou de ressources (telles que : installations, équipements, logiciels ou personnel) de l'entreprise ou le concours volontaire pendant ses heures travaillées au profit ou en faveur d'un candidat en campagne pour un mandat public, d'un comité de parti politique ou d'une commission politique ;
2. Le lobbying ou le fait de chercher à influencer des agents publics, directement ou par l'intermédiaire de tierces parties, y compris le fait de chercher à influencer des décisions législatives, officielles et, selon les pays ou territoires, le fait de chercher éventuellement à influencer l'adoption d'une règle administrative ou l'attribution d'un marché public ; ou
3. Le fait de postuler à, d'accepter ou d'exercer une quelconque responsabilité politique associée à une administration gouvernementale, y compris au sein d'un conseil gouvernemental, d'une commission gouvernementale ou de toute instance similaire.

Aucune activité politique ne peut être entreprise ou menée par un Fournisseur pour le compte (ou prétendument pour le compte) de Citi, ou de ses clients, sans autorisation écrite préalable du Government Affairs Global Operations Control de Citi (ggacontrol@citi.com). Bien que Citi puisse payer des frais et/ou rembourser des coûts engagés pour des services d'activité politique contractuels et autorisés fournis par le Fournisseur, tels que le lobbying, Citi ne remboursera jamais un Fournisseur ni l'un de ses employés pour des contributions politiques personnelles ou d'entreprise de quelque nature que ce soit.

12 ANTI-MONEY LAUNDERING (« AML »)

Applicable aux Fournisseurs qui dispensent certains services liés aux clients (c'est-à-dire l'intégration, le filtrage des comptes et des transactions client) ou la livraison de données/d'indicateurs liés aux activités susmentionnées ; ET/OU aux Fournisseurs qui agissent en tant qu'intermédiaires en ce qui concerne les transactions ou instruments financiers (p. ex., la collecte de dépôts à distance, les services de messagerie, de transport blindé ou de coffre-fort).

12.1 Obligations liées à l'AML :

1. Respect des procédures de Citi et des lois applicables :

- Tenir à jour et respecter les processus et procédures de Citi conçus pour satisfaire aux exigences des lois applicables, notamment (i) la loi Gramm-Leach-Bliley et ses règlements d'applications ; (ii) la loi USA PATRIOT Act et ses règlements d'application ; (iii) toute loi ou tout règlement relatif au blanchiment d'argent ; et (iv) toute loi ou tout règlement relatif aux sanctions économiques. Ces politiques et procédures porteront sur les rôles et responsabilités en matière de lutte contre le blanchiment de capitaux, y compris l'obligation de signaler sans délai toute activité observée qui semble inhabituelle ou potentiellement inhabituelle en lien avec des activités financières, des transactions et des encaissements en espèces.

2. Formation annuelle et éléments du programme destinés au Personnel :

- Veiller à ce que les membres de son Personnel fournissant des Services à Citi suivent une formation annuelle portant sur leurs rôles et responsabilités en matière de lutte contre le blanchiment de capitaux, y compris l'obligation de signaler sans délai toute activité observée qui semble inhabituelle ou potentiellement inhabituelle, qu'il s'agisse d'activités financières, de transactions ou d'encaissements. Cette formation doit inclure, sans s'y limiter, les éléments suivants :
 - a. Signalement et remontée des activités suspectes.
 - b. Un programme « Know Your Customer » (KYC), comprenant un Customer Identification Program (CIP), la vérification des sanctions et des noms, la customer due diligence (CDD), la enhanced due diligence (EDD), ainsi que l'identification et la vérification des **Ultimate Beneficial Owners (UBOs)**.
 - c. Le suivi des transactions portant sur l'ensemble des instruments financiers et activités concernés.
 - d. La communication de rapports/indicateurs périodiques, y compris les rapports sur les changements légaux et réglementaires et les changements importants apportés au programme d'AML.
 - e. Des tests et contrôles de l'efficacité du programme AML, avec notamment des visites sur site.

3. Respect des dispositions contractuelles :

- Respecter toutes les dispositions du Contrat qui définissent tout programme qui doit être institué par le Fournisseur.

4. Signalement rapide des violations présumées :

- Signaler sans délai à Citi, par écrit, tout manquement présumé à la loi, y compris toute activité observée qui semble inhabituelle ou potentiellement inhabituelle, liée à l'encaissement d'espèces, à des activités financières ou à des transactions impliquant Citi ou ses clients.

5. Prévention et signalement en matière d'évasion fiscale :

- Respecter toutes les lois et réglementations fiscales applicables dans les pays où l'entreprise exerce ses activités.
- En aucun cas les Fournisseurs ne doivent se livrer à une évasion fiscale illégale délibérée ou faciliter une telle évasion pour le compte d'autres acteurs, ce qui peut inclure la participation à des activités visant à éviter le paiement des impôts dus et exigibles ou à dissimuler des informations aux autorités fiscales.
- À ce titre, les Fournisseurs doivent adopter des procédures de prévention raisonnables relatives à l'évasion fiscale et signaler rapidement à Citi par écrit toute violation ou violation présumée liée à Citi.

12.2 Politiques et procédures internes du Fournisseur :

Les Fournisseurs doivent tenir à jour des politiques et procédures internes appropriées pour se conformer à toutes les lois et réglementations AML actuellement en vigueur ou mises en vigueur par la suite.

13 GESTION DES DOSSIERS

Applicable aux Fournisseurs qui accèdent à/traitent/stockent des Informations de Citi.

Citi exige que tous les Fournisseurs ayant la garde d'Informations de Citi travaillent avec leur Business Activity Owner (« **BAO** ») ou le contact principal de Citi pour (i) identifier et classer les Informations en tant que Dossiers ou en tant qu'informations transitoires à des fins de gestion des dossiers de Citi, (ii) classer les Dossiers conformément au Master Record Catalogue (« **MRC** ») de Citi, (iii) conserver les Informations en respectant les exigences de conservation et (iv) en l'absence de mesure de conservation des informations, éliminer les informations de manière appropriée à la fin du Cycle de vie desdites Informations.

Le BAO ou le contact commercial principal de Citi doit travailler avec le Fournisseur pour s'assurer que celui-ci a identifié et classé les enregistrements conformément aux codes d'enregistrement de Citi dans le MRC et que l'inventaire est mis à jour au moins une fois par an. Le Fournisseur a l'obligation de se conformer aux exigences de gestion des dossiers communiquées par le BAO. Les enregistrements répondant aux critères de destruction doivent être éliminés de manière appropriée dès que possible, mais au plus tard six mois après que les exigences de conservation ont été satisfaites, sauf s'ils font l'objet d'une mesure de conservation obligatoire des informations. Les informations transitoires pourront être détruites dans un délai maximal de deux ans après leurs dernières utilisations, sauf si elles sont sous le coup d'une mesure de conservation obligatoire des informations. Les informations transitoires contenant des informations à caractère personnel doivent être supprimées dès que l'objectif pour lequel elles ont été collectées est atteint, sauf si elles font l'objet d'une mesure de conservation obligatoire des informations. Le Fournisseur doit suspendre la destruction ou la modification des Informations de Citi lorsqu'il est informé d'une mesure de conservation obligatoire des informations. Le Fournisseur devra consulter son contact professionnel principal chez Citi ou le BAO en cas d'incertitude.

Chaque trimestre, les règles de conservation figurant dans les calendriers de conservation par pays sont examinées et mises à jour, si nécessaire, afin de rester conformes aux évolutions réglementaires et internes, sous la responsabilité du DRIM. Lorsqu'il y a un changement qui impacte le Fournisseur, le BAO en informera le Fournisseur. Le Fournisseur doit évaluer l'impact et mettre en œuvre les changements nécessaires au niveau des systèmes, des processus et des stocks concernés. Il doit recenser les types de documents dont il est responsable et les gérer dans un délai de 90 jours à compter de la notification émanant du BAO.

Les Fournisseurs qui conservent des documents pour le compte de Citi sont responsables de la préservation, de la collecte et de la production de toute information jugée pertinente dans le cadre d'une procédure judiciaire ou autre, dans les délais requis, tels que définis par le BAO. Le Fournisseur est tenu, sur demande, de restituer à Citi les informations requises conformément aux dispositions contractuelles applicables. Les Fournisseurs ne doivent se défaire d'aucune Information de Citi, quelle que soit sa classification (par exemple, Confidentielle, Non Confidentielle) sans l'approbation de leur principal contact commercial Citi ou du BAO, qui doit inclure la confirmation qu'aucune mesure de conservation des informations active ne s'applique aux informations à éliminer. Les obligations de gestion et de conservation des dossiers et toute autre obligation relative à la gestion des informations resteront effectives ultérieurement à la résiliation ou à l'expiration du contrat, sauf convention contraire expresse.

Les Fournisseurs doivent conserver une documentation énumérant l'ensemble de leur Personnel responsable de la supervision de la gestion des Informations de Citi sous la

garde du Fournisseur et organiser des réunions périodiques avec leur contact commercial principal de Citi ou le Records Management Officer afin de passer en revue et de mettre à jour les noms des contacts, les détails des procédures, les rôles et responsabilités et l'Inventaire des dossiers du Fournisseur de Citi.

14 RÉSILIENCE / CONTINUITÉ DES ACTIVITÉS

Applicable aux Fournisseurs qui fournissent des services ou hébergent des infrastructures technologiques/applications utilisées par Citi. Le Business Activity Owner (BAO) de Citi est responsable de la communication de l'applicabilité et des exigences en matière de continuité des activités au Fournisseur.

14.1 Ressources de récupération

Les plans de reprise après sinistre des Fournisseurs doivent prévoir des ressources de substitution permettant de livrer tous les produits et services à Citi dans l'éventualité où les sites principaux du Fournisseur deviendraient non opérationnels. Les Ressources de récupération doivent se trouver dans des endroits géographiquement distincts des sites principaux et suffisamment distants pour minimiser ou éliminer le risque que la même catastrophe puisse affecter à la fois les sites principaux et les sites de récupération.

1. Les Ressources de récupération ne se limitent pas aux Systèmes informatiques, mais incluent également toutes les ressources nécessaires pour continuer à livrer les produits et services à Citi. Elles pourront consister en personnel, locaux, équipements professionnels, centres de données, réseaux de données et téléphoniques, services de transport.
2. Les Fournisseurs d'applications peuvent mettre en œuvre une architecture de type Hot/Hot pour assurer une configuration HA (High Availability [Haute Disponibilité]). Cette architecture nécessite la présence d'au moins deux systèmes configurés de manière identique, opérationnels et disponibles pour les clients/utilisateurs. La caractéristique la plus importante de ce modèle est que les environnements alternatifs fonctionnent simultanément avec le centre de données principal (de production).

14.2 Niveaux de service de récupération

Afin d'être suffisamment efficaces du point de vue de Citi, la continuité des activités du Fournisseur doit respecter les niveaux de service établis. Le Plan de reprise après sinistre du Fournisseur doit au moins établir des valeurs spécifiques pour :

1. Durée maximale d'interruption admissible (RTO ou DMIA)
2. Perte de données maximale admissible (RPO ou PDMA)
3. Ressources de récupération/capacité technologique
4. Durée de récupération

14.3 Plan de reprise après sinistre

Le Fournisseur tiendra à jour un Plan de reprise après sinistre pour la poursuite des activités (et fournira des preuves de tests actuels et périodiques de ce plan si Citi le demande) de sorte que, même en cas de perturbation dans la capacité du Fournisseur à assurer les Produits/Services ou à remplir ses autres obligations en vertu des présentes, et ce, à partir d'un lieu particulier ou grâce aux efforts d'individus particuliers, le Fournisseur sera rapidement en mesure de fournir les Produits/Services et de remplir ses obligations à partir d'un autre lieu ou avec du Personnel de remplacement. Une copie du Plan de reprise après sinistre doit être remise à Citi dans un délai de dix (10) jours civils à compter de la Date d'entrée en vigueur de chaque Ordre de travail conclu entre Citi et le Fournisseur, puis annuellement tant que chaque Ordre de travail reste en vigueur. Le Fournisseur transmettra à Citi toutes les instructions ou autres informations nécessaires afin que Citi puisse continuer à recevoir les produits/services du Fournisseur dans des circonstances où le Fournisseur a dû faire appel à son plan de reprise après sinistre. Le Fournisseur déclare, garantit et s'engage à ce que son plan de reprise après sinistre comprenne au minimum :

1. Des procédures et stratégies de reprise, y compris la relocalisation, le transfert de travail et/ou l'accès à distance pour atténuer les effets des perturbations, y compris la non-disponibilité des technologies (Déni de service/DoS), la non-disponibilité de l'emplacement de travail principal (Déni d'accès/DoA) et la non-disponibilité du personnel (y compris des sous-traitants) ;
2. La maintenance par le Fournisseur d'un site secondaire de reprise après sinistre (au minimum) distinct des emplacements du Produit/Service, le stockage de supports de sauvegarde dans un emplacement distinct des emplacements du Produit/Service, l'utilisation de lignes de communication et de serveurs redondants ;
3. Des procédures de sauvegarde/restauration du fonctionnement et de l'application des Produits/Services, y compris un plan détaillé et documenté pour répondre à une perturbation prolongée des Produits/Services causée par une panne de courant, une panne du système, une catastrophe naturelle ou d'autres circonstances imprévues qui comprend des processus et des procédures pour reprendre les opérations dans un délai mutuellement convenu ;
4. Des procédures de protection de tous les Contenus ;
5. Des procédures et des accords avec des tiers pour le remplacement du matériel (par exemple, le matériel informatique) ;
6. Des procédures pour toutes les installations de production hors site ; et
7. Le Plan de reprise après sinistre du Fournisseur prévoira que :
 - a. Le Fournisseur informe rapidement Citi de tout sinistre susceptible d'avoir un impact négatif sur les Produits/Services ;
 - b. Le Fournisseur communique à Citi, dans les 24 heures suivant ladite notification, un plan de continuité de la fourniture des Produits/prestation des Services dans un site de traitement de substitution ;

- c. Les produits/services devront être pleinement opérationnels dans le délai requis par l'objectif de temps de reprise (RTO). Si aucun délai n'est spécifié dans le Contrat applicable, le RTO est fixé comme suit : 4 heures ou moins pour les processus classés par Citi comme ayant une criticité « Critique pour l'entreprise » ou « ÉLEVÉE », 24 heures ou moins pour les processus classés comme ayant une criticité « MOYENNE », et 72 heures ou moins pour les processus classés comme ayant une criticité « FAIBLE. »
- d. Dans le cas où une partie des installations du Fournisseur seraient inopérantes, le Fournisseur traitera Citi de la même manière que ses autres clients commerciaux.

14.4 Exigences du Plan de reprise après sinistre applicables aux Services hébergés

Dans la mesure où le Fournisseur gère et fournit un service hébergé à Citi, les dispositions qui suivent s'appliquent également. Le Plan de reprise après sinistre comprendra au minimum :

1. Des procédures de sauvegarde/restauration du fonctionnement et de l'application des Services hébergés, y compris un plan détaillé et documenté pour répondre à une interruption prolongée des services causée par une panne de courant, une panne du système, une catastrophe naturelle ou d'autres circonstances imprévues qui comprend des processus et des procédures pour reprendre les opérations dans un délai mutuellement convenu ;
2. Le plan de reprise après sinistre du Fournisseur prévoira que : (a) Le Fournisseur informe Citi par écrit dans les deux (2) heures de tout sinistre qui pourrait avoir un impact négatif sur les Services hébergés ; (b) Le Fournisseur fournisse à Citi, dans les 24 heures suivant cet avis, un plan de continuité des services hébergés dans une autre installation de traitement, et (c) les Services hébergés soient pleinement opérationnels dans les 48 heures suivant l'avis initial ;
3. Le Fournisseur s'engage à divulguer sur demande, les informations nécessaires pour permettre à Citi d'élaborer un plan de reprise après sinistre et un plan de continuité des activités, qui fonctionneront de concert avec le plan de reprise après sinistre et le plan de continuité des activités du Fournisseur ; et
4. Dans le cas où une partie des installations du Fournisseur seraient inopérantes, le Fournisseur traitera Citi de la même manière que ses autres clients commerciaux.

14.5 Modifications apportées au plan de reprise après sinistre

Le Fournisseur peut modifier son plan de reprise après sinistre tant que les changements ne dégradent pas le plan de reprise après sinistre d'une manière

susceptible d'affecter négativement les services (par exemple, en prolongeant ses RTO). Le Fournisseur communiquera rapidement tout changement dans son plan de reprise après sinistre à Citi et, à la demande de Citi, expliquera les changements afin que Citi comprenne pleinement les changements et soit en mesure d'y répondre.

14.6 Plan de reprise après sinistre relatif aux sous-traitants

Le Fournisseur veillera à ce que tout Sous-traitant du Fournisseur dispose d'un plan de reprise après sinistre et de mesures de continuité des activités conformes aux exigences de Citi applicables aux Fournisseurs. Le Fournisseur doit assurer une surveillance adéquate des Sous-traitants, notamment en procédant à un examen périodique des contrôles et des résultats des tests de ces derniers, et veiller à ce que toute lacune identifiée soit corrigée dans les meilleurs délais.

14.7 Invocation du plan de reprise après sinistre et notification de crise

Le Fournisseur informera rapidement le contact commercial principal de Citi :

1. Lorsqu'il fait intervenir son plan de reprise après sinistre et ;
2. Concernant toute crise, menace, avertissement ou événement cybernétique contre le Fournisseur ou ses sous-traitants raisonnablement susceptible d'avoir un impact négatif sur les services ou produits fournis à Citi.

14.8 Tests

L'ensemble des ressources et plans de reprise du Fournisseur doivent être testés dans un délai de 120 jours suivant leur mise en production (90 jours pour les applications classées par Citi comme « Critiques pour l'entreprise »), et faire l'objet de tests annuels (tous les 12 mois) au minimum. Les tests doivent démontrer la capacité du Fournisseur à assurer les niveaux de service de récupération pour tous les produits et services fournis à Citi. Ces tests doivent être complets et inclure l'ensemble des Services fournis à Citi. Les Fournisseurs doivent donner à Citi un préavis d'au moins 30 jours civils avant de tester la récupération des services/services fournis à Citi. Citi se réserve le droit de participer ou d'observer les tests de reprise effectués par le Fournisseur sur les applications utilisées par Citi, afin de valider leur fonctionnalité métier dans l'environnement de reprise. Si Citi souhaite participer, le Fournisseur fournira à Citi les objectifs du test, le plan de test et les procédures de connexion au site de test avant d'effectuer le test. Sous dix (10) jours civils ouvrables après la fin de chaque test, le Fournisseur transmettra un résumé des objectifs du test, le plan de test et les résultats du test à Citi, y compris les délais requis pour la récupération et la preuve des résultats du test (par exemple, captures d'écran).

14.9 Validation des volumes

Un Fournisseur qui héberge des applications classées par Citi comme critiques pour l'entreprise doit démontrer que les volumes de production peuvent être traités dans son environnement COB/de reprise après sinistre. Citi et le Fournisseur doivent s'entendre sur la méthodologie à utiliser pour la validation.

14.10 Utilisation des systèmes de Citi pour fournir des services

À la demande de Citi ou de ses entités affiliées, les Fournisseurs utilisant les systèmes de Citi devront participer, sans frais ni facturation pour Citi, aux exercices de reprise après sinistre organisés par Citi.

14.11 Traitement des résultats des tests

Si les résultats des tests du Fournisseur indiquent que les objectifs du test ou les délais RTO applicables n'ont pas été respectés, le Fournisseur s'engage à effectuer une analyse de la cause initiale et à remédier dans les plus brefs délais à toute lacune décelée. À la suite de la mise en œuvre de mesures correctives, le Fournisseur devra effectuer un nouveau test dans un délai maximal de cent vingt (120) jours calendaires (90 jours calendaires pour les applications classées par Citi comme « Critiques pour l'entreprise » suivant l'échec du test initial (ou dans le délai spécifié dans le bon de commande concerné).

14.12 Gestion de crise

Parallèlement au plan de continuité des activités, le Fournisseur devra disposer d'un plan de gestion de crise opérationnel afin de diriger et de contrôler les opérations de récupération. Au minimum, le plan de gestion de crise du Fournisseur devra identifier nominativement les personnes disposant d'une autorité suffisante pour activer une opération de récupération, définir les protocoles de communication et d'intensification pour la collecte et la diffusion des informations de crise, et intégrer des protocoles de notification et d'intensification permettant de communiquer avec Citi en cas de crise.

14.13 Évaluations de la continuité des activités

Les Fournisseurs sont soumis au processus d'évaluation de la continuité des activités par des tiers de Citi pour évaluer les politiques, procédures et contrôles du Fournisseur concernant la conformité aux exigences de Citi et toute exigence juridique et/ou réglementaire (applicable à Citi ou au Fournisseur) relative à la continuité des activités. L'évaluation comprend des questionnaires nécessitant des réponses du Fournisseur avec des preuves à l'appui et peut inclure des visites des sites du Fournisseur. Si les conclusions d'une évaluation font apparaître ou indiquent des problèmes ou des préoccupations, Citi documentera les conclusions et travaillera avec le Fournisseur pour identifier un moyen de corriger les problèmes. Les Fournisseurs devront rapidement apporter les corrections nécessaires et/ou ajouter des contrôles compensatoires afin de répondre aux préoccupations de Citi à la satisfaction raisonnable de cette dernière.

14.14 Résilience opérationnelle

Les services commerciaux essentiels sont les services qui, si leur prestation était perturbée, pourraient avoir un impact négatif important sur Citi, ses clients ou le système financier. Le Fournisseur veillera à ce que toute perturbation dans la prestation des éléments des Services qui constituent des services commerciaux essentiels ou qui soutiennent la prestation de services commerciaux essentiels par Citi, tels que spécifiés par Citi de temps à autre (« Services commerciaux essentiels ») ne dépasse pas la durée fixée par Citi ou n'enfreigne pas toute autre mesure pertinente fixée par Citi (« Tolérances d'impact ») telle que notifiée au Fournisseur de temps à autre. Les Tolérances d'impact seront exprimées sous la forme d'un indicateur clairement défini

en termes de durée, correspondant à la durée pendant laquelle la prestation de service peut être perturbée. Citi et le Fournisseur réviseront les tolérances d'impact chaque année dans le cadre du processus de gouvernance du contrat en cours. Lorsque Citi est tenu de définir deux tolérances d'impact pour un service commercial essentiel individuel en raison des exigences de plus d'un organisme de réglementation, Citi peut alors spécifier des tolérances d'impact distinctes pour ce service commercial essentiel. Le Fournisseur doit :

1. Informer Citi dès qu'il se rend compte qu'il n'a pas réussi (ou qu'il est raisonnablement susceptible de ne pas réussir) à fournir tout service dans les limites de la (des) tolérance(s) d'impact correspondante(s) fixée(s) par Citi, avec une explication des raisons de toute défaillance potentielle ou réelle et des mesures prises pour atténuer l'impact de cette défaillance ;
2. Sur demande, fournir une assistance raisonnable à Citi pour lui permettre d'identifier les personnes, les processus, les technologies, les installations et les informations nécessaires au Fournisseur pour assurer les services commerciaux essentiels ;
3. Fournir une assistance raisonnable à Citi pour permettre à Citi de mener :
 - a. tout scénario interne testant la capacité du Fournisseur à rester dans les limites de la ou des tolérances d'impact pour chaque Service commercial essentiel en cas de perturbation grave mais plausible de ses opérations ou de celles du Fournisseur ; et
 - b. tout enseignement tiré exercé à la suite d'un test de scénario pour permettre à Citi d'identifier les faiblesses et les actions nécessaires pour améliorer la capacité du Fournisseur à répondre efficacement et à se remettre des perturbations futures.

Lorsqu'un test de scénario interne effectué par Citi identifie des vulnérabilités ou des limitations sur la capacité du Fournisseur à délivrer des services dans le cadre de la (des) tolérance(s) d'impact correspondante(s) fixée(s) par Citi et à la suite de tout échec du Fournisseur à délivrer un service commercial essentiel dans le cadre de la (les) tolérance(s) d'impact correspondante(s) fixée(s) par Citi, les parties conviendront d'un plan (y compris un calendrier de mise en œuvre du plan) pour s'assurer que le Fournisseur prend les mesures nécessaires pour résoudre ou atténuer ces vulnérabilités ou limitations ou remédier à la cause du non-respect de la ou des tolérances d'impact (selon le cas) dès que cela sera raisonnablement possible.

14.15 Convention de dépôt fiduciaire

À la demande de Citi, les Fournisseurs (i) concédant des licences logicielles à Citi en vue d'une utilisation dans l'environnement informatique de Citi, ou (ii) fournissant un service hébergé à Citi, doivent s'assurer que les supports déposés sont remis à l'agent fiduciaire désigné par Citi, et doivent remplir un formulaire d'enregistrement du déposant ou tout autre document requis par l'agent fiduciaire, conformément au contrat

fiduciaire applicable. Par la suite, tout au long de la durée de l'accord applicable à la licence ou au service hébergé, le Fournisseur déposera des versions mises à jour des supports déposés auprès de l'agent fiduciaire afin de s'assurer que le code source sous contrat fiduciaire et les autres supports déposés restent à jour avec la dernière version du logiciel applicable à la version du logiciel ou des services hébergés utilisée par Citi. Les mises à jour du code source ou de tout autre support déposé devront être remises à l'agent fiduciaire dans un délai de trente (30) jours suivant la date de toute mise à jour du logiciel concédé sous licence à Citi ou de toute modification des services hébergés utilisés par Citi. Le Fournisseur se conformera pleinement à toutes les obligations et exigences du déposant énoncées dans la convention fiduciaire. Le Fournisseur est seul responsable de tous les coûts et frais liés aux dépôts fiduciaires, y compris, mais sans s'y limiter, les frais d'établissement, les frais annuels, les frais de dépôt, les frais de service et tous les autres coûts et frais liés aux dépôts fiduciaires. En cas d'événement de déliement, l'agent fiduciaire remettra les supports déposés à Citi ou à son représentant, conformément aux conditions de l'accord sous-jacent et de la convention fiduciaire.

Si le code source (ou d'autres supports déposés) est livré à Citi ou à son représentant (soit directement par le Fournisseur, soit par l'agent fiduciaire dans le cadre de ses obligations en vertu d'un accord de dépôt fiduciaire applicable), le code source et les supports déposés seront alors soumis à la licence existante en vertu de l'accord pertinent entre le Fournisseur et Citi ; à condition que chaque licence soit considérée comme conférant à Citi le droit d'utiliser et de modifier le code source et d'autres supports déposés comme raisonnablement nécessaires pour : (i) intégrer et assurer la compatibilité des logiciels et des autres supports déposés avec les systèmes de Citi, (ii) faire en sorte que les logiciels ou les autres supports déposés soient conformes à la loi applicable, aux normes industrielles ou aux pratiques du marché, (iii) permettre aux logiciels ou aux autres supports déposés de rester à jour par rapport aux innovations technologiques, et (iv) permettre aux logiciels et aux autres supports déposés de remplir les objectifs commerciaux de Citi et de ses sociétés affiliées dans le cadre de la licence existante. Toute version des logiciels incluant une modification développée par ou pour le compte de Citi à partir du code source est soumise à l'ensemble des dispositions de la présente section ainsi qu'à celles de l'accord sous-jacent ; étant entendu toutefois que le Fournisseur ne disposera d'aucun droit, titre ou intérêt sur lesdites modifications, et que tous les droits de propriété intellectuelle afférents aux modifications seront exclusivement dévolus à Citi.

Le Fournisseur s'engage à déployer des efforts commercialement raisonnables auprès des tiers ayant fourni toute application intégrée aux logiciels, afin de permettre au Fournisseur de déposer le code source de ces logiciels tiers dans le dépôt de code source. Si le tiers refuse d'accorder ce droit au Fournisseur, celui-ci devra alors déployer des efforts commercialement raisonnables pour que le contrat de licence de logiciel tiers applicable soit transférable à Citi en cas d'événement de déliement.

Le code source livré à Citi conformément à la présente section est soumis à la licence existante pour les logiciels ou les services autorisés applicables, à *condition que* Citi puisse utiliser et modifier le code source et les logiciels en fonction de ses exigences commerciales et opérationnelles, afin de permettre aux logiciels de rester en phase avec les innovations technologiques et d'être conformes à la loi applicable. Toute

version des logiciels incluant une modification développée par ou pour le compte de Citi à partir du code source est soumise à l'ensemble des dispositions de l'accord applicable ; étant entendu toutefois que le Fournisseur ne disposera d'aucun droit, titre ou intérêt sur lesdites modifications, et que tous les droits de propriété intellectuelle afférents aux modifications seront exclusivement dévolus à Citi.

15 NORMES MONDIALES EN MATIÈRE D'EXAMEN DES ANTÉCÉDENTS

Applicable à tous les Fournisseurs tiers qui fournissent des services à Citi.

15.1 Aperçu – Vérification des antécédents

La vérification des antécédents doit être effectuée conformément à toutes les lois et réglementations locales applicables. Toutes les informations et auto-divulgations décrites dans le présent document doivent être fournies par les représentants du Fournisseur, son personnel et ses Sous-traitants, le cas échéant. La falsification ou l'omission d'informations, que ce soit sur un curriculum vitae, lors de l'entretien, sur un formulaire d'intégration ou pendant le processus d'intégration, quelle que soit la date à laquelle elles sont découvertes, peut constituer un motif de refus ou de résiliation de la mission auprès de Citi conformément à la législation locale. Des résultats négatifs ressortant d'un quelconque examen d'antécédents, quel que ce soit le moment où ces résultats seront révélés, pourront également constituer un motif de refus ou de résiliation de la mission auprès de Citi conformément à la législation locale applicable en l'espèce.

Des informations supplémentaires sur l'examen des antécédents sont disponibles à l'adresse

https://www.citigroup.com/rcs/citigpa/storage/public/country_background_screening_requirements_tables.pdf

15.2 Collecte d'informations de base et vérification d'identité

Avant qu'un membre du personnel des Fournisseurs ne débute une mission pour Citi, les Fournisseurs doivent recueillir le prénom et le nom de famille, l'adresse postale et l'adresse permanente (si elle est différente), le numéro de téléphone et l'adresse électronique (le cas échéant) de cette personne. Les membres du personnel du Fournisseur doivent également fournir des documents qui valident leur identité. Il peut s'agir de fournir des informations et/ou un numéro d'identification national, ou de produire un passeport ou une carte d'identité avec photo émise par le gouvernement.

15.3 Examen des sanctions

Tout membre du personnel du Fournisseur effectuant des travaux pour le compte de Citi ou tout propriétaire détenant 25 % ou plus du capital d'un Fournisseur de Citi, y compris les sous-traitants, indépendamment de l'accès aux données/systèmes/réseaux de Citi ET/OU de l'accès aux locaux de Citi, doit être contrôlé par rapport à la liste des

Exigences de Citi à l'égard des Fournisseurs

Page 26 sur

Specially Designated Nationals and Blocked Persons (« SDN ») de l'Office of Foreign Assets Control (« OFAC ») du Département du Trésor des États-Unis et à la liste des régions et juridictions faisant l'objet de sanctions imposées par les États-Unis (« sanctions américaines »), ainsi que par rapport à toute liste publiée et aux noms des juridictions faisant l'objet de sanctions imposées par des autorités situées en dehors des États-Unis, notamment la liste consolidée des sanctions financières de l'Union européenne (UE), la liste consolidée du Conseil de sécurité des Nations unies (« ONU »), la liste des sanctions du Royaume-Uni (« RU ») et les listes établies en vertu des lois et réglementations applicables à la juridiction locale (« Sanctions non américaines »).

Les listes OFAC sont accessibles au public sur le site Web suivant : <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

15.4 Conformité en matière d'immigration

Le Fournisseur doit démontrer qu'il dispose et met en œuvre des protocoles permettant de vérifier que l'ensemble de son personnel est autorisé à travailler dans les pays d'affectation. En outre, le Fournisseur doit : (1) s'assurer que l'ensemble de son personnel dispose d'une autorisation de travail, et (2) veiller au respect de l'ensemble des lois, réglementations et politiques applicables (y compris les exigences en matière d'éligibilité à l'emploi et de vérification de cette éligibilité). Le Fournisseur doit en outre mettre en place et respecter des protocoles visant à garantir que son personnel se conforme à toutes les lois et réglementations applicables en matière d'immigration et qu'il dispose du statut ou de la catégorie de visa appropriés pour les missions et les activités auxquelles il participe.

15.5 Antécédents professionnels

Les Fournisseurs doivent valider l'expérience professionnelle de leur personnel au cours des sept (7) dernières années, ou des 10 dernières années si cela est exigé par la réglementation. L'historique d'emploi de la personne doit être validé afin de vérifier que les employeurs, les postes, les dates et les tâches ont été correctement présentés. Le personnel du Fournisseur doit également divulguer tout emploi ou toute mission préalable en tant que consultant ou travailleur temporaire auprès de Citi ou de l'une de ses sociétés précédentes (y compris, mais sans s'y limiter : Citibank, Citicorp, Travelers, Salomon Brothers et/ou Smith Barney).

15.6 Parcours académique

Les Fournisseurs doivent valider le niveau d'instruction le plus élevé de leur personnel. Les informations validées doivent indiquer les dates de présence, le(s) nom(s) et adresse(s) des institutions concernées et le(s) diplôme(s) obtenu(s).

15.7 Casier judiciaire

Sauf interdiction par les lois locales, tout employé ou sous-traitant d'un Fournisseur doit aviser Citi s'il fait l'objet d'un mandat d'arrêt, d'une citation à comparaître, d'une assignation, d'une interpellation, d'une mise en accusation ou d'une condamnation pour

une infraction pénale, y compris un plaidoyer de culpabilité ou de non-contestation et toute participation à un programme de déjudiciarisation avant le procès ou tout programme similaire. L'examen administratif des casiers judiciaires et/ou des vérifications d'empreintes digitales doit être réalisé avant la date de début de la mission lorsque cela est légalement permis et disponible. Les condamnations pénales pour des délits liés au vol, à la fraude, à la malhonnêteté ou à l'abus de confiance, ou des délits similaires définis différemment par la législation locale, sauf si la loi l'interdit, peuvent entraîner le refus et/ou l'inéligibilité à une mission chez Citi. D'autres condamnations seront également susceptibles d'entraîner l'inéligibilité à la mission ou la résiliation de celle-ci en fonction des lois et réglementations locales applicables.

15.8 Seconde vérification

Les membres du Personnel du Fournisseur dont la mission aurait pris fin devront se soumettre à de nouveaux examens dans le cas où ils seraient de nouveau affectés auprès de Citi. Pour plus d'informations sur les exigences en matière de nouvel examen,

consultez

https://www.citigroup.com/citi/suppliers/data/background_screening_requirements_tables.pdf

15.9 Transferts internationaux

Tous les examens et tests devront être effectués conformément aux réglementations du pays où la mission doit être effectuée. Si un membre du personnel du Fournisseur est muté dans un nouveau pays, le collaborateur concerné devra se soumettre à de nouveaux examens en conformité avec les exigences du nouveau pays.

16 DÉPENSES

Fournisseurs contractuellement éligibles à réclamer le défraiement de dépenses professionnelles remboursables

16.1 Présentation

Citi ne remboursera que les frais professionnels raisonnables ayant été préalablement approuvés par écrit par Citi, engagés par le Fournisseur dans le cadre de la fourniture de produits et la prestation de services à Citi, conformes aux termes du contrat applicable ou à la politique de gouvernance des dépenses opérationnelles de Citi et aux normes et procédures pertinentes, le cas échéant, et dûment justifiés par des reçus, factures, billets de transport ou autres pièces justificatives jugées acceptables par Citi.

16.2 Remboursements

Ces dépenses devront être correctement documentées et facturées à Citi conformément aux règles de facturation de Citi. Les dépenses du Fournisseur ne doivent pas être engagées par un employé de Citi pour le compte d'un Fournisseur. Toute dépense soumise à Citi pour le remboursement d'un ou plusieurs éléments de

dépense valides et approuvés doit inclure (en plus de toutes les autres exigences de facturation) :

1. L'objectif professionnel de la dépense ;
2. Le montant et la description de la dépense ;
3. Le lieu et la date de la dépense ;
4. Le nom/la description du projet pour lequel le Fournisseur assure des services ;
5. Les noms et la relation commerciale du représentant de Citi ayant demandé les services pour lesquels de telles dépenses ont été engagées ; et
6. Le numéro de commande, le cas échéant.

Pour obtenir des informations sur les dépenses commerciales remboursables autorisées, veuillez contacter votre contact commercial principal chez Citi. Les reçus justificatifs, factures, billets de transport ou autres formes de documents jugés acceptables par Citi doivent être soumis avec la demande de remboursement. Les demandes de remboursement doivent être conformes aux dispositions du contrat applicable ou à la politique de gouvernance des dépenses d'exploitation de Citi et à ses normes et procédures pertinentes, le cas échéant, et être approuvées par le commanditaire commercial approprié et/ou le contact commercial principal de Citi, ainsi que par une personne dûment autorisée et disposant d'un montant suffisant pour le produit correspondant. Les demandes non conformes ne seront pas remboursées.

17 SÉCURITÉ DES INFORMATIONS (IS)

Applicable aux Fournisseurs, y compris leurs Sous-traitants qui consultent, traitent, stockent ou gèrent toute Information de Citi telle que classée et définie dans l'Annexe ; ou hébergent des applications Internet de marque Citi ; ou sont connectés aux ressources réseau de Citi ; ou nécessitent un accès sans escorte aux locaux de Citi.

17.1 Aperçu

Cette section définit les exigences minimales auxquelles doivent satisfaire les Fournisseurs de Citi, y compris les sous-traitants, qui stockent, traitent, gèrent ou accèdent aux informations de Citi, hébergent des applications Citi ou disposent d'une connexion réseau à Citi, en matière de contrôles de protection des informations attendus par Citi. Ces exigences garantissent que les informations sont protégées conformément aux obligations légales et réglementaires en vigueur et aux normes les plus strictes du secteur (par exemple ISO/CEI 27001/2) dans tous les sites où Citi et ses Fournisseurs exercent une activité. Si les lois, les réglementations ou les normes sectorielles applicables localement définissent des normes plus strictes que celles figurant aux présentes, les Fournisseurs devront se conformer à ces lois, réglementations ou normes. En outre, les Fournisseurs pourront être tenus d'intégrer des procédures et pratiques de sécurisation des informations supplémentaires afin de se conformer aux autres politiques de Citi et aux conditions contractuelles. Si un Fournisseur décide de mettre en œuvre des pratiques de sécurité supplémentaires ou des procédures de sécurisation de l'information, le Fournisseur devra s'assurer que ces

pratiques et procédures ne sont pas incompatibles avec les contrôles minimums définis dans la présente section.

17.2 Politique de sécurité des informations et gouvernance

Les Fournisseurs doivent disposer de politiques et de normes documentées en matière de sécurité de l'information. La gouvernance de la politique doit inclure des rôles et des responsabilités clairement définis, ainsi qu'une révision/mise à jour annuelle de la politique et des normes pour assurer leur cohérence avec l'état actuel des technologies, les normes sectorielles, ainsi que les exigences légales et réglementaires.

17.3 Séparation des fonctions

Les Fournisseurs doivent avoir mis en place des processus garantissant qu'aucune personne ne puisse exécuter deux fonctions commerciales ou deux des fonctions informatiques, ou deux des fonctions du système informatique contrôlé avec un accès persistant pour la même activité, le même changement, le même système informatique ou la même transaction sans autorisation ou détection, à moins que des contrôles compensatoires adéquats ne soient présents pour atténuer le risque.

Tableau A

Fonctions	Description de la fonction
Développement/ingénierie	Concevoir, créer ou modifier des logiciels, du matériel informatique et des configurations. Voici quelques exemples : - Conception et développement de nouveau code d'application et des schémas de base de données associés - Conception de produits d'infrastructure et de composants d'applications - Adaptation de produits technologiques pour les intégrer à des logiciels et à des services
Approbation	Approuver la mise en œuvre des modifications apportées au code
Mise en œuvre/administration des systèmes	Installer, déployer ou gérer des logiciels, du matériel et des modifications de configuration Voici des exemples : - Réalisation d'une mise en production automatisée ou manuelle du code sur l'infrastructure de production - Installation d'un produit ou d'un appareil technologique - Démarrage ou arrêt de services afin de faciliter le dépannage et la correction des

	problèmes sur les systèmes contenant des données de production
Analyse de l'activité liée aux identifiants privilégiés	Vérification des activités de gestion des changements ou des événements système liés à la sécurité (p. ex., les pistes d'audit)
Administration des identifiants	Ajout, modification et suppression d'identifiants (utilisateurs, FID et robots), de droits d'accès ou de mots de passe
Fonction commerciale	Description de la fonction
Initiation de transactions commerciales	Initier les transactions commerciales et modifier les informations client (également appelé apport ou effectuer ou créer)
Approbation des transactions commerciales	Approuver les transactions commerciales (également appelé autoriser, vérifier ou donner son accord)
Fonction informatique	Description de la fonction
Opérations de réseau	Gestion des équipements et assistance opérationnelle pour les produits fournissant des services d'infrastructure réseau. Les routeurs, les commutateurs, les pare-feu et les serveurs DNS en sont des exemples.
Opérations hors réseau	Gestion des équipements et assistance opérationnelle pour les produits qui ne fournissent pas de services d'infrastructure réseau. Les serveurs, les téléphones et les ordinateurs en sont des exemples

17.4 Engagement de la direction à l'égard de la sécurité des informations

Les Fournisseurs qui hébergeront une application Internet de marque Citi ou auront accès à des Informations de Citi classées confidentielles ou de niveau supérieur sont assujettis au TPISA (Third Party Information Security Assessment Process) de Citi, un processus évaluant les politiques, les procédures et les contrôles mis en place par les Fournisseurs pour s'assurer de la conformité aux présentes Exigences et aux exigences légales et/ou réglementaires (applicables à Citi ou aux Fournisseurs) ayant trait à la sécurité des informations.

L'évaluation s'effectue sous la forme de questionnaires de sécurité exigeant des réponses du Fournisseur avec preuves à l'appui et peut inclure d'éventuelles visites des sites du Fournisseur où les Informations de Citi classées Confidentielles ou de niveau supérieur seront stockées, traitées, gérées ou consultées par la tierce partie. De plus, l'équipe TPISA chargée de la surveillance continue des tiers peut surveiller le Fournisseur à l'aide d'outils de cybersécurité reposant sur des informations accessibles

au public, afin d'identifier les systèmes, hôtes, applications et serveurs exposés à Internet susceptibles de présenter des failles, tels que des logiciels en fin de vie, des ports ouverts exploités, des vulnérabilités ou autres compromissions. Si les conclusions d'une évaluation TPISA révèlent des problèmes ou des préoccupations en matière de sécurité, Citi présentera ces conclusions dans un document qu'il notifiera au Fournisseur et travaillera avec lui afin d'identifier les moyens de corriger ces problèmes. Les Fournisseurs doivent apporter sans délai les corrections nécessaires et/ou mettre en place des mesures compensatoires afin de répondre aux préoccupations de Citi, à la seule discrétion de Citi, et respecter les délais requis de 180 jours calendaires pour les problèmes à haut risque, 240 jours calendaires pour les problèmes à risque moyen, et avant la prochaine échéance de conformité pour les problèmes à faible risque, selon la cote de risque de ces problèmes telle qu'évaluée par Citi.

1. Le Fournisseur devra effectuer régulièrement des évaluations de ses opérations commerciales et des contrôles associés par rapport à ses propres normes, politiques et procédures de sécurité de l'information. Les évaluations périodiques doivent comprendre au minimum :
 - a) Évaluation des processus dont le Fournisseur se sert pour assurer sa conformité avec ses propres politiques et normes en matière de Sécurité des informations ;
 - b) Évaluation des ressources de soutien, telles que les applications et l'infrastructure utilisées par le Fournisseur et les processus de Sécurité des informations employés par les sous-traitants du Fournisseur (le cas échéant) qui soutiennent leurs opérations commerciales ou permettent à Citi de mener ces évaluations. La conformité est requise dans le cas où une tierce partie signe un nouveau contrat ou renouvelle un contrat existant avec un sous-traitant qui accède, traite, gère ou élimine des Informations de Citi classées Confidentielles ou de niveau supérieur par Citi.
2. Les problèmes qui ont été identifiés à la suite de toute évaluation des risques de sécurité de l'information (par exemple TPISA) doivent être documentés et suivis jusqu'à leur résolution avec des preuves de leur résolution fournies à Citi.
3. Si la fonction de gestion de la sécurité des Informations du Fournisseur est relocalisée à l'étranger, le Fournisseur devra obtenir un agrément documenté de Citi avant une telle relocalisation.
4. Si le Fournisseur acquiert une nouvelle entité, le Fournisseur devra effectuer une évaluation de la conformité de l'entité acquise par rapport à ces Normes.
5. Le Fournisseur ne pourra en aucun cas, sauf approbation écrite préalable de Citi, externaliser les fonctions de gestion de la sécurité, notamment, sans toutefois s'y limiter, la gestion des pare-feu, la gestion des configurations de sécurité, la gestion des correctifs ou les fonctions d'Administration de la sécurité des informations (ISA ou « Information Security Administration »), concernant les systèmes utilisés pour stocker, traiter et/ou transmettre les Informations de Citi.
6. Si le Fournisseur héberge un logiciel ou un site Web qui contient des Informations de Citi ou qui porte la marque Citi, des évaluations périodiques de sa vulnérabilité devront être effectuées conformément à la norme System

Security Testing Standard (SSTS) de Citi et tout problème identifié lors de l'évaluation devra être résolu dans les délais spécifiés par cette norme. Comme la distribution externe de la SSTS n'est pas approuvée, les Fournisseurs devront travailler avec leur responsable des relations Citi pour assurer la conformité à la documentation de référence. En outre, le Fournisseur devra se conformer aux normes de gestion de la sécurité de l'information ISO/CEI 27001 pertinentes (ou aux normes de gestion de la sécurité de l'information qui leur succéderont et qui établiront des normes et des protocoles plus élevés) et se conformer aux dispositions relatives à la sécurité des informations contenues dans la présente Section (17).

7. S'il est nécessaire d'établir une connexion avec les serveurs et/ou les Systèmes informatiques fonctionnant sur le réseau interne de Citi, le Fournisseur devra en aviser leur contact commercial Citi principal afin que le processus actuel de provisionnement de la connexion puisse être suivi.
8. Le Fournisseur devra aviser rapidement l'interlocuteur concerné chez Citi (Business Activity Owner (BAO)), en cas d'accès non autorisé, d'acquisition, de perte, de corruption ou de suppression d'Informations de Citi, ou de toute autre altération des Systèmes informatiques permettant de stocker, traiter ou transmettre des Informations de Citi.
9. Le Fournisseur devra s'assurer que toutes les activités à haut risque ou tous les changements apportés aux données sensibles ont des pistes d'audit qui permettent de relier ces actions aux personnes qui les ont effectuées.
10. Le Fournisseur devra s'assurer que toutes les données confidentielles ou de niveau supérieur sont masquées à l'écran et sur papier, notamment, par exemple, les rapports de surveillance, les rapports d'exception, les rapports réglementaires et autres.
11. Le Fournisseur devra restreindre l'impression, l'enregistrement ou la copie de données sensibles, y compris par ses propres appareils. Le Fournisseur devra restituer ou détruire toutes les informations relatives à Citi à une date convenue pendant ou à la fin du contrat, sauf si la loi ou la réglementation l'interdit.
12. Le Fournisseur devra veiller à ce que l'ensemble de son personnel (employés, entrepreneurs, intérimaires, sous-traitants) ayant accès aux informations de Citi signe un accord de confidentialité ou de non-divulgaration.
13. Les employés du Fournisseur devront recevoir un manuel de l'employé ou un document similaire détaillant le processus disciplinaire en cas d'infraction au code de conduite et aux politiques de ressources humaines du Fournisseur qui doivent être acceptés dans le cadre du processus d'intégration.
14. Le Fournisseur aura mis en place un processus pour récupérer toutes les ressources lorsqu'un employé ou un non-employé sera licencié ou démissionnera.
15. Si des Informations Confidentielles sont conservées ou stockées de quelque manière que ce soit sur un site Web ou un système accessible sur le Web, le Fournisseur devra divulguer ces informations à Citi. Cette divulgation pourra être incluse dans la description des services. Si le Fournisseur gère ou stocke des informations confidentielles de Citi, le Fournisseur provoquera l'exécution d'un audit SSAE 18 (ou de toute évaluation faisant autorité qui lui succédera approuvée par Citi) une fois par an pendant la durée du présent accord, et fournira à Citi, au moins une fois par an, une copie des rapports documentant

les résultats de cet audit SSAE 18 ou de toute évaluation faisant autorité qui lui succédera, approuvée par Citi.

16. Si le Fournisseur est racheté ou acquiert une autre entité dans le cadre d'une fusion, d'une acquisition ou d'une transaction similaire, et que cette transaction est susceptible d'avoir un impact sur les Services, le Fournisseur doit rapidement en informer Citi par écrit et le Fournisseur doit effectuer une évaluation de la sécurité des informations sur l'entité résultante, conformément aux présentes exigences, afin de s'assurer que ce changement n'a pas d'impact sur la conformité avec ces dernières.

17.5 Risque lié à la sécurité des informations pour les sous-traitants

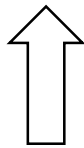
Le Fournisseur doit exiger de la part des sous-traitants ayant accès aux données confidentielles ou de niveau supérieur de Citi qu'ils se soumettent à des évaluations de l'Information Security (IS) avant la signature du contrat et périodiquement après la signature du contrat, effectuées par du personnel spécialisé dans la sécurité des informations. Ces évaluations doivent être réalisées conformément à un processus approuvé par la direction qui couvre toutes les étapes du processus d'évaluation, depuis son lancement jusqu'à la gestion des problèmes. L'évaluation IS du sous-traitant doit utiliser un questionnaire ou un outil équivalent qui évalue la posture du sous-traitant dans les domaines IS qui s'alignent sur ceux inclus dans le TPAQ (Third Party IS Assessment Questionnaire) de Citi et doit inclure une méthode logique de calcul du risque IS associé au recours au sous-traitant. Le Fournisseur doit suivre l'évaluation jusqu'à la fin et gérer les problèmes relevés et les plans de mesures correctives jusqu'à leur clôture.

17.6 Responsabilité des actifs

1. Le Fournisseur doit s'assurer de maintenir un inventaire de toutes les applications et de tout le matériel sous son contrôle utilisés pour stocker, traiter et/ou transmettre des Informations de Citi.
2. Le Fournisseur devra veiller à ce qu'un inventaire des actifs informationnels de Citi soit tenu sous son contrôle conformément à un processus utilisé pour maintenir de manière appropriée l'exactitude et l'exhaustivité dudit inventaire.
3. Le Fournisseur doit être responsable de la protection de toutes les informations de Citi sous son contrôle.
4. Le Fournisseur doit assumer la responsabilité de l'activité de ses utilisateurs conformément aux pratiques sectorielles.
5. L'accès utilisateur aux comptes de courrier électronique externes personnels stockés dans le Cloud et sur Internet à partir du réseau global du Fournisseur où résident des Informations de Citi devra être restreint.

17.7 Traitement et classification des informations.

Citi classe les informations selon le tableau de classification des informations ci-dessous. Consulter l'Annexe pour connaître les définitions et voir des exemples de chaque classification répertoriée ci-dessous.

RESTREINTES	Les plus sensibles
PII SENSIBLES	
PII CONFIDENTIELLES	
CONFIDENTIELLES	
PII INTERNES	
INTERNES	
PUBLIQUES	Les moins sensibles

1. En fonction de la classification des informations de Citi, Citi doit collaborer avec le Fournisseur afin de déterminer le niveau de sécurité requis pour protéger ces informations. Le Fournisseur doit s'assurer que des contrôles suffisants sont mis en place, y compris tout niveau accru ou adapté que Citi pourrait exiger.
2. Les informations classées Internes ou de niveau supérieur doivent être stockées sur des appareils gérés par des tierces parties faisant l'objet d'un contrat liant la tierce partie à Citi contenant des dispositions relatives à la confidentialité conformes aux règles et normes de Citi.
3. Si le Fournisseur autorise l'utilisation d'appareils n'appartenant pas à l'entreprise pour stocker des données de Citi (c'est-à-dire des appareils gérés par une 4^e partie), le Fournisseur doit avoir mis en place une politique qui requiert une approbation spécifique de la direction et avoir établi des directives et des procédures de contrôle pour l'utilisation et l'élimination des Informations de Citi.
4. Le Fournisseur doit toujours protéger les informations de Citi contre tout accès, modification ou suppression non autorisés.
5. Les Informations de Citi classées Confidentielles ou de niveau supérieur transférées via des supports électroniques transportables (ETM) doivent être chiffrées à l'aide d'un algorithme cryptographique approuvé et la réception doit être confirmée. Le Fournisseur doit confirmer que l'ETM a été reçu par le destinataire. Si la confirmation de réception n'est pas reçue à la date de livraison prévue, le Fournisseur devra en informer Citi.

17.8 Configuration sécurisée

1. Le Fournisseur doit respecter une norme de configuration sécurisée documentée pour tous les actifs susceptibles de stocker, traiter, accéder ou transmettre des informations de Citi.
2. Le Fournisseur doit intégrer des contrôles de sécurité des informations dans ses processus et procédures de sélection, de développement et de mise en œuvre d'applications, de produits et de services.
3. Le Fournisseur doit disposer d'une procédure de conception sécurisée pour tous les systèmes sur lesquels les informations de Citi sont stockées, traitées et/ou transmises.
4. Le Fournisseur doit conserver une image ou un modèle sécurisé pour tous les systèmes.
5. Tous les comptes et mots de passe par défaut doivent être supprimés et/ou modifiés au niveau des systèmes, des périphériques réseau et des applications pris en charge par le Fournisseur.

6. Tout système ou service compromis doit être reconstruit et reconfiguré à l'aide d'une image ou d'un modèle dont l'intégrité est avérée.
7. Tout changement à apporter à une configuration sécurisée doit être validé par la direction via le processus de gestion des modifications du Fournisseur.
8. Le Fournisseur devra informer Citi de tout changement apporté à la configuration sécurisée.
9. La procédure de génération sécurisée doit inclure des outils pour prendre en charge les vérifications de configuration automatisées des paramètres de sécurité/de génération standard au moment du déploiement de la production, et un contrôle permanent de la conformité à la configuration de base et des écarts par rapport à celle-ci.

17.9 Exigences en matière de chiffrement

Le Fournisseur ne doit pas transmettre d'Informations classées Confidentielles ou de niveau supérieur sans les crypter. Les Informations classées Confidentielles ou de niveau supérieur doivent être chiffrées **de bout en bout** avec des outils ou solutions approuvés par Citi. Les protocoles approuvés et leurs numéros de version respectifs pour la transmission cryptée des données sont les suivants :

1. Lors de l'échange d'informations d'authentification et d'autorisation : SAML v2.0, OAuth v2.0 (autorisation uniquement),
2. Pour protéger les canaux de communication et l'échange de clés associé, seuls les protocoles de sécurité réseau suivants sont autorisés :
 - a) La version TLS v1.3 est privilégiée et toutes les suites TLS v1.3 sont autorisées. Si le protocole TLS v1.3 est le seul protocole activé, aucun examen supplémentaire n'est nécessaire.
 - b) Si la version TLS v1.3 n'est pas techniquement réalisable et que la version TLS 1.2 est utilisée, une note égale ou supérieure à B attribuée par SSL Labs est actuellement acceptable et aucun examen supplémentaire n'est nécessaire.

Les données stockées de manière persistante dans l'environnement du Tiers de Citi ou lorsqu'elles sont échangées doivent être entièrement chiffrées à l'aide d'outils ou de solutions approuvés par Citi. Les algorithmes approuvés et les longueurs de clés pour le chiffrement des données sont les suivants :

1. **Norme de chiffrement avancé (AES)** : Longueur de clé approuvée : 256 bits ou plus. Modes restreints : Le mode Electronic Codebook (ECB) est interdit sauf lorsque la quantité de texte en clair est inférieure ou égale à la taille du bloc. Chiffrement du disque : AES avec une clé de 256 bits obligatoirement. L'utilisation de l'AES avec une clé de 128 bits est autorisé comme option de chiffrement TLS ; toutefois, son utilisation sera interdite au profit d'une clé de 256 bits ou plus d'ici le 31 décembre 2028, afin de permettre à Citi de s'aligner sur les échéances internationales (réf. NIST 8547 IPD).
2. **ChaCha20 (un chiffrement par flux pour les cas d'utilisation associés)** : Longueur de clé approuvée : 128 ou 256 bits, avec un nonce de 96 bits et

un compteur de blocs de 32 bits, ou un nonce de 64 bits et un compteur de blocs de 64 bits. Taille maximale des données : 16 pétaoctets.

Les cryptosystèmes de clés publiques approuvés, l'échange de clés, les mécanismes d'accord, les fonctions de hachage de messages et de dérivation de clés sont les suivants :

Avis lié à la préparation quantique du Fournisseur : Les Fournisseurs sont tenus de présenter leur plan de conformité aux *tableaux 2 et 4* de la norme NIST IR 8547 (ipd) à l'équipe du programme Citi Quantum Readiness via ([lien d'enquête](#)).

1. **Cryptosystèmes à clé publique et tailles minimales de longueur de clé :**
 - a) Rivest–Shamir–Adleman (RSA) : 2048 bits.
 - b) Digital Signature Algorithm (DSA) : 2048 bits. Le DSA ne doit pas être utilisé pour sécuriser les données Citi traitées ou stockées en dehors de Citi.
 - c) Elliptic Curve Digital Signature Algorithm (ECDSA) : 256 bits, et tel qu'indiqué dans ANSI X9.62 avec les courbes recommandées par le NIST.
2. **Mécanismes d'échange et de reconnaissance des clés et taille minimale des clés :**
 - a) Diffie-Hellman (DH) / Ephemeral Diffie-Hellman (DHE) : 2048 bits.
 - b) Elliptic-curve Diffie–Hellman (ECDH) / Ephemeral Elliptic-curve Diffie–Hellman (ECDHE) : 256 bits, et tel qu'indiqué dans ANSI X9.63 avec les courbes recommandées par le NIST¹.
3. **Fonctions de hachage de messages :** La création d'une clé de chiffrement d'une taille supérieure au nombre de bits aléatoires dans le matériel utilisé pour générer le hachage est interdite.
 - a) SHA-1 acceptable uniquement pour les applications de signature non numériques. Famille SHA-2, famille SHA-3 et POLY-1305 : Acceptable pour toutes les applications de fonction de hachage cryptographique.
4. **Fonctions de dérivation de clés fondées sur le mot de passe et exigences minimales :**
 - a) PBKDF2 : Compte d'itération minimum de 10 000 avec un sel d'au moins 16 octets.
 - b) HKDF : Doit être salé et la valeur d'entrée d'informations doit être incluse.
 - c) SCRYPT : Nombre minimum de tours/facteur de coût d'au moins 10.
 - d) L'utilisation de NIST SP800-108 KDF pour le chiffrement de flux est interdite. Les modes de dérivation de clés (KDF) définis dans la norme NIST SP 800-108, à savoir les modes Counter, Feedback et Double-Pipeline Iteration, sont acceptables.
 - e) Argon2 est recommandé.

¹ ECDHE est le mécanisme à privilégier.

5. Fonctions de hachage des mots de passe et exigences minimales :

- a) Bcrypt (pour le stockage en local du matériel d'authentification) :
Nombre minimum de tours/facteur de coût d'au moins 10.
- b) Argon2 ou PBKDF2 est recommandé pour le hachage des mots de passe lors du stockage local des mots de passe sur tout environnement ou système déployé par le Fournisseur.

17.10 Courrier électronique externe :

L'exigence de chiffrement pour les courriers électroniques individuels contenant des Informations de Citi avec une classification d'Informations Confidentielles ou de niveau supérieur, lorsque le Fournisseur n'est pas autorisé à utiliser un logiciel ou des outils de chiffrement de bout en bout approuvés par Citi conformément à la réglementation et/ou à la politique du Fournisseur, peut être entièrement satisfaite par le chiffrement de transport (par exemple, le chiffrement de passerelle à passerelle via Transport Layer Security (TLS)). Les protocoles de courrier électronique sécurisé approuvés sont les suivants :

- 1. L'**Identity-Based Encryption (IBE)** inclut le chiffrement des e-mails et doit être utilisé uniquement dans les solutions client de Citi et les systèmes sécurisés de courrier électronique et d'eDelivery.
- 2. Le **Mandatory TLS (MTLS)** inclut le chiffrement de session (ne chiffre pas la charge utile des e-mails) et est destiné aux Fournisseurs, partenaires et clients qui ont des accords prédéfinis quant à son utilisation.
- 3. Le **Domain Keys Identified Mail (DKIM)** comprend l'authentification de la source et la gestion des clés et est destiné à être utilisé par les Fournisseurs, les partenaires et les clients.

17.11 Réseaux privés

Les réseaux privés qui sont réglementés de façon indépendante par une autorité reconnue et qui satisfont aux normes du secteur des services financiers pour les transactions entre contreparties autorisées ou accréditées (SWIFT ou réseau de banque centrale par exemple) pourront être considérés comme exemptés de l'exigence de chiffrement en transit des données PII confidentielles jusqu'à ce que ces réseaux soient à même de fournir l'infrastructure permettant de prendre en charge les transmissions chiffrées.

17.12 Téléphonie et télécopie

Les informations dont la classification par Citi est Confidentielle ou de niveau supérieur, envoyées par fax ou évoquées lors d'appels vocaux (y compris la voix sur IP [VOIP]) peuvent être envoyées sans être chiffrées. Le Fournisseur doit, le cas échéant, élaborer des procédures et des directives spécifiques pour protéger les informations classées Confidentielles ou de niveau supérieur envoyées par ces canaux.

17.13 Gestion des clés cryptographiques et des certificats

Le terme « périmètre de sécurité » utilisé dans cette section fait référence à un périmètre validé par un Cryptographic Module Validation Program (CMVP), tel que la norme Federal Information Protection Standard (FIPS) (le niveau 2 de FIPS 140-2/3 constitue le niveau de sécurité minimal acceptable). Les enclaves de calcul confidentiel

telles que les AWS Nitro Enclaves sont acceptables. D'autres cas uniques de périmètres de sécurité doivent être approuvés par Citi).

1. Le Fournisseur doit mettre en œuvre les algorithmes cryptographiques standard actuels du secteur et observer des longueurs minimales de clés pour le chiffrement et la signature (y compris les clés SSH). Lorsque ces algorithmes et ces longueurs clés sont mis à jour, le Fournisseur doit fournir l'assurance, via son processus de gestion des changements, que les normes du secteur ont été observées.
2. Les Fournisseurs doivent disposer d'un processus formel documenté pour la gestion du cycle de vie des clés, des secrets et des certificats, avec des contrôles en place pour protéger les données sensibles contre toute utilisation ou exposition non autorisée. Tous les secrets cryptographiques et tous les événements liés au cycle de vie des clés doivent se dérouler exclusivement au sein d'un périmètre sécurisé. Tout accès à des périmètres privilégiés et sûrs doit être correctement documenté. Le Fournisseur doit fournir un schéma de séquence pour tous les événements du cycle de vie des clés soulignant les acteurs, entités et périmètres impliqués.
3. Les clés cryptographiques doivent avoir une finalité unique et ne doivent jamais être utilisées à d'autres fins, telles que l'utilisation de la même clé de chiffrement pour le chiffrement sur disque et le chiffrement des données, ou la même clé de chiffrement pour le chiffrement de la charge et le chiffrement de la base de données. La réutilisation de clés cryptographiques entre plusieurs clients par un fournisseur SaaS est interdite par défaut et ne peut être autorisée que pour des cas d'utilisation non critiques et à faible risque impliquant des informations personnelles identifiables de Citi classées à un niveau inférieur à « Informations personnelles confidentielles », « Informations personnelles sensibles » et « À accès restreint », sous réserve de l'accord explicite du Security Architecture Council.
4. Pour toutes les clés cryptographiques (asymétriques ou asymétriques), la clé privée ou les éléments de clé privée (tel que les phrases de récupération, ou une partie d'une clé privée) ne doivent être affichés en texte clair à aucun moment. La clé privée ou les éléments de clé privée (tel que la phrase de récupération ou une partie d'une clé privée) ne doivent jamais quitter le périmètre de sécurité à l'exception des clés éphémères telles que les clés de session dynamiques. Si la conception nécessite une clé symétrique ou une clé privée ou un élément de clé privée à transmettre entre enclaves sécurisées/périmètres d'accès privilégiés, la transmission doit se faire sous forme chiffrée uniquement à l'aide d'une clé de chiffrement de clé symétrique ou d'une clé de transport de clé publique via des tunnels chiffrés TLS mutuels uniquement, et cette transmission doit être approuvée par Citi par écrit. Dans ce cas-là, la clé de transport de clé privée ne doit jamais quitter le périmètre de sécurité d'accès privilégié où elle a été générée.
5. La clé de chiffrement de clé symétrique doit être divisée en deux ou plusieurs composants de clé et être « XORée » avant d'être distribuée et lors de la saisie/du chargement manuel de la clé. La clé de chiffrement de clé symétrique doit disposer d'Access Controls Lists (ACLs) associées à

l'intérieur du périmètre de sécurité, telles que des modules validés CMVP et la clé de chiffrement de clé symétrique ne doit jamais être rangée hors du périmètre de sécurité.

6. L'accès par des personnes, des services ou des agents automatisés à des dépôts de clés ou à des paramètres de sécurité contenant des clés privées ou des secrets ou des éléments de clé privée (comme des phrases de récupération, ou une partie d'une clé privée) doit être correctement séparé par des contrôles limitant l'accès au personnel ou aux systèmes autorisés uniquement.
7. Chaque demande d'accès aux dépôts de clés contenant des clés privées ou symétriques doit être enregistrée et documentée à des fins d'audit en consignait les détails comme le nom de la personne, la date et le but de l'accès.
8. Le Fournisseur ne doit pas utiliser de certificats auto-signés et de certificats génériques ou de certificats SSL par défaut.
9. Toutes les clés cryptographiques doivent comporter une cryptopériode définie, comme le suggère le document NIST SP800-57 partie 1, révision 6. Les clés doivent être actualisées ou permutées avant leur expiration pour tenir compte des périodes de changement, des conflits de planification et des blocages du système.
 - a) Lors du remplacement d'un certificat expiré, la réutilisation de l'ancienne paire de clés asymétriques est interdite.
10. Les clés cryptographiques doivent être considérées comme compromises dès lors que l'intégrité de la clé, du support sur lequel elle est stockée ou partagée, ou la confidentialité de la clé symétrique ou privée est suspectée d'avoir été compromise. Toutes les clés compromises doivent être retirées du cadre d'utilisation opérationnelle et tous les certificats correspondants doivent être révoqués.
11. Les réseaux sans fil doivent être chiffrés à l'aide d'algorithmes de chiffrement standard de l'industrie.
12. Les Fournisseurs utilisant une forme quelconque de mécanisme cryptographique doivent utiliser les techniques et les outils de gestion des clés préconisés par les normes sectorielles. Le rôle de gestion des clés doit être distinct de celui de la gestion opérationnelle.
13. Les Fournisseurs ne peuvent recourir à des systèmes KMS et PKI natifs du cloud que si l'interopérabilité avec les services PKI et KMS fournis par Citi Data Security Services est garantie et si le contrôle cryptographique n'est pas délégué en dehors du cadre de la gouvernance cryptographique de Citi.

17.14 Responsabilité du contrôle d'accès

Pour protéger tous les systèmes d'information contrôlés utilisés pour stocker, consulter, traiter ou transmettre des informations de Citi classées confidentielles ou de niveau supérieur contre un accès non autorisé, le Fournisseur est responsable de l'application du principe du moindre privilège, en restreignant les droits des utilisateurs au niveau d'accès le plus faible nécessaire pour chaque fonction et en gérant le provisionnement d'un accès logique pour tous les systèmes et applications. Les contrôles doivent être

entièrement documentés et vérifiables. La création et la suppression des droits d'accès, y compris la réinitialisation et l'activation des mots de passe, doivent être effectuées, dans la mesure du possible, via un processus automatisé afin de limiter les risques liés à d'éventuelles erreurs humaines pouvant entraîner l'octroi de droits excessifs, et de se conformer aux normes du secteur.

1. Le Fournisseur est responsable des droits d'accès de tous les utilisateurs de son organisation.
2. Le Fournisseur doit mettre en place des contrôles d'accès garantissant que les utilisateurs ne reçoivent que les privilèges et droits strictement nécessaires à l'exécution de leur fonction.
3. Le Fournisseur devra implémenter un processus assurant que toutes les fonctionnalités d'accès par défaut sont supprimées, désactivées ou protégées afin d'empêcher toute utilisation non autorisée.

17.15 Gestion de l'accès utilisateur

Le Fournisseur doit prendre en charge la fourniture d'un accès logique aux systèmes et applications traitant, stockant et/ou transmettant des informations de Citi classées Confidentielles ou de niveau supérieur. Cela comprend :

1. Identification et inventaire des systèmes d'authentification approuvés.
2. L'obligation que tout accès aux données de Citi doit nécessiter une validation de la part d'un responsable ou de son représentant et du propriétaire du système. Le Fournisseur doit veiller à ce que les membres de son personnel ayant accès aux données de Citi bénéficient d'un tel accès sur la base du « besoin de savoir ».
3. L'obligation selon laquelle toute combinaison de privilèges/fonctions pour un utilisateur individuel ne peut être octroyée si elle présente un conflit d'intérêts ou une violation des règles du « maker-checker » (créateur-contrôleur).
4. Un processus de surveillance pour superviser et gérer les droits d'accès accordés/révisés pour chaque utilisateur du système.
5. Les demandes d'accès ne doivent pas reposer sur la reproduction ou le clonage des droits d'un autre utilisateur. Elles doivent préciser explicitement les rôles et les droits concernés, accompagnés d'une justification métier, afin d'éviter toute dérive liée aux privilèges et de respecter le principe du privilège minimal.

17.16 Identification et authentification de l'utilisateur

Tous les systèmes d'information contrôlés par le Fournisseur doivent authentifier l'identité des utilisateurs ou des systèmes accédant à ces plateformes avant d'entamer une session ou une transaction dans laquelle des informations de Citi peuvent être consultées.

1. Les utilisateurs doivent être identifiés ou faire l'objet d'un traçage sur la plateforme technologique par un Identifiant utilisateur qui leur est propre.
2. Les utilisateurs doivent être authentifiés sur la plateforme technologique à l'aide d'une méthode d'authentification approuvée. Le Fournisseur doit

contacter son contact commercial principal (le BAO) pour connaître les méthodes actuellement approuvées.

3. Toute utilisation d'une infrastructure d'authentification partagée (authentification SSO, authentification RSO et autres services d'authentification partagée) doit être conforme aux exigences d'authentification de Citi. Le Fournisseur devra s'informer sur les méthodes actuellement approuvées auprès de son contact (le BAO) principal.
4. Les Identity Verification Data (IVD) utilisées pour authentifier un utilisateur auprès d'un système d'information doivent être chiffrées en transmission et en stockage. Voir la section 17.9 pour connaître les exigences en matière de chiffrement.
5. Chaque compte utilisé par le personnel du Fournisseur pour accéder aux systèmes de Citi doit être associé à un identifiant unique attribué par Citi (p. ex., un GEID) ; l'utilisation d'identifiants génériques ou partagés pour les utilisateurs humains est interdite afin de garantir la traçabilité, le respect du principe de Segregation of Duties (SOD) et la préparation aux audits.

17.17 Identification des accès privilégiés et accès privilégiés temporaires

Le Fournisseur doit tenir à jour un registre de toutes les identités et recenser celles qui disposent d'un accès privilégié ou d'un accès à des référentiels électroniques (ensembles de données ou bases de données alimentant des applications métier) contenant des informations personnelles identifiables classées « Informations personnelles confidentielles » ou d'un niveau de confidentialité supérieur. Le Fournisseur doit mettre en œuvre des contrôles qui protègent contre l'utilisation non autorisée de ces identités. Si un employé a besoin d'accéder à un identifiant privilégié ou aux référentiels électroniques mentionnés précédemment, l'accès doit être accordé par le biais d'un processus temporaire de gestion de l'accès qui :

1. Impose que le demandeur figure sur la liste des utilisateurs autorisés préapprouvés ou qu'il bénéficie d'une approbation valide au moment de l'utilisation.
2. Nécessite un justificatif pour toute demande de modification ou de résolution de problème avant que l'accès ne soit accordé ;
3. Inclut un examen indépendant de la transaction exécutée avec l'accès ;
4. Inclut une procédure permettant de lancer la révocation ou la suppression de l'accès à l'issue de la période de validité de l'accès temporaire.
5. Permet de prolonger l'accès de sept (7) jours maximum, en cas de production et de stabilisation post-implémentation après une mise à jour majeure ou une intervention de dépannage.

17.18 Examen des droits d'accès utilisateur

1. Le Fournisseur doit mettre en œuvre un processus documenté pour examiner, vérifier et supprimer les droits d'accès utilisateur inutiles aux Systèmes informatiques contrôlés utilisés pour stocker, traiter, gérer ou transmettre les Informations de Citi au moins une fois par semestre.

2. Les utilisateurs ne doivent pas réviser ou approuver leurs propres droits ou les droits d'une personne qui leur a délégué la responsabilité de révision.
3. À la suite d'un changement de fonction d'un employé du Fournisseur de Citi, le Fournisseur dispose de 14 jours civils pour effectuer un examen des accès et des droits et supprimer l'accès aux données de Citi si cet accès n'est plus nécessaire pour la nouvelle fonction de l'employé.

17.19 Procédures de connexion sécurisée

1. Les Identifiants de connexion qui ont été bloqués devront être réactivés via un service de réinitialisation conforme aux normes sectorielles ou par toute autre fonction autorisée. Lorsque cela est pris en charge par le système d'exploitation ou l'application, un texte de bannière doit être affiché à tous les points d'entrée du réseau auquel un utilisateur se connecte ou s'authentifie initialement.

17.20 Système de gestion des mots de passe

1. Les mots de passe statiques de l'utilisateur ne doivent jamais être affichés à l'écran en texte clair. La fonctionnalité permettant d'afficher ou de masquer le mot de passe est exemptée de cette exigence, à condition que :
 - (1) La saisie du mot de passe soit masquée par défaut,
 - (2) L'affichage du mot de passe ne puisse être déclenché que par une action explicite de l'utilisateur,
 - (3) Le mot de passe soit automatiquement masqué à nouveau dans un délai maximal de 15 secondes une fois que l'action de l'utilisateur a pris fin.
2. Les mots de passe d'identification fonctionnelle privilégiée ne doivent pas être codés en dur en texte clair.
3. Les mots de passe statiques doivent contenir au moins dix (10) caractères, qui doivent être un mélange de lettres et de chiffres, et être sensibles à la casse. La distinction entre majuscules et minuscules des mots de passe statiques doit être vérifiée à chaque point d'authentification. Les mots de passe statiques des Identifiants fonctionnels (FID) doivent comporter au moins 15 caractères pour les applications déployées après le 31 août 2026.
4. Les codes PIN ne peuvent être utilisés comme seule méthode d'authentification pour accéder aux Systèmes informatiques que si les contraintes physiques de l'appareil (clavier, téléphone, carte à puce) imposent d'utiliser des codes PIN.
5. Chaque mot de passe statique doit être changé tous les 90 jours minimum.
6. Tous les mots de passe statiques doivent être bloqués après six (6) tentatives consécutives d'accès infructueuses au maximum, ou après six (6) tentatives consécutives de réinitialisation du mot de passe. Les mots de passe doivent être débloqués via une fonction d'administrateur des identifiants ou automatiquement débloqués au bout de 30 minutes au minimum.
7. Tous les systèmes d'authentification doivent appliquer un contrôle de l'inactivité/de la non-utilisation de la connexion qui ne peut pas dépasser 100 jours civils. Si cela est techniquement faisable, les connexions désactivées pourront être réactivées par l'utilisateur ou par une autre fonction autorisée.

8. Le processus d'authentification doit faire en sorte que le même mot de passe ne soit pas réutilisé avant au minimum six (6) changements consécutifs.

17.21 Utilisation des utilitaires du système

Le Fournisseur doit s'assurer que l'utilisation de programmes utilitaires ayant priorité sur les contrôles du système et des applications (par exemple, le démarrage à partir de périphériques) est restreinte et contrôlée.

17.22 Expiration de session

1. Une nouvelle authentification de la connexion est obligatoire pour tous les utilisateurs d'un système informatique contrôlé permettant de stocker, traiter et/ou transmettre des informations de Citi.
2. Les Utilisateurs seront tenus de procéder à une nouvelle authentification après une période d'inactivité ne dépassant pas 30 minutes. L'activité comprend toute entrée effectuée au point d'extrémité (souris, clavier, écran tactile, etc.). Lorsque le respect de cette règle est assuré par un économiseur d'écran protégé par mot de passe, il n'est pas nécessaire de la faire respecter au niveau de l'Application ou de recourir à une authentification par Single Sign-on (SSO).

17.23 Résiliation de l'accès des utilisateurs

1. En cas de résiliation ou de démission, l'accès utilisateur ou les droits permettant d'accéder aux données de Citi classées Confidentielles ou de niveau supérieur (identifiant utilisateur à Desktop/Active Directory, Single Sign-on (SSO), courrier électronique, jetons de mots de passe à usage unique (OTP) et accès distant) devront être supprimés immédiatement.
2. Si un employé a accès à des systèmes détenus et administrés par Citi, le Citi Business Relationship Manager, le BAO ou le délégué du BAO doivent être notifiés immédiatement lors du changement de poste ou de la fin de contrat de cet employé pour veiller à ce que le Citi Business Manager amorce le processus de suppression de l'accès pour les employés concernés avant la date de leur fin de contrat.
3. Le Fournisseur dispose d'un processus documenté pour récupérer l'accès à tous les actifs conformément aux délais prévus à la section 17.23.2 lorsqu'un employé ou un non-employé est licencié ou démissionne.
4. Si une anomalie est découverte par le Fournisseur conformément aux sections 17.23.1-17.23.3, le Fournisseur doit en informer immédiatement le Citi Business Manager, le BAO ou le délégué du BAO, en fournissant une justification et des contrôles solides.

17.24 Accès à distance

Le Fournisseur doit disposer de contrôles d'accès à distance pour protéger l'accès aux réseaux capables de stocker, traiter ou transmettre les données de Citi classées Confidentielles ou de niveau supérieur, notamment :

1. L'accès à distance aux Systèmes informatiques permettant de stocker, gérer, traiter ou transmettre des Informations de Citi doit être protégé contre toute utilisation non autorisée.
2. Tous les ordinateurs portables et tous les ordinateurs de bureau gérés par le Fournisseur permettant de stocker, traiter et/ou transmettre des informations de Citi, utilisant un accès distant donnant lieu à un stockage ou traitement local d'informations classées comme informations confidentielles ou de niveau supérieur par Citi, devront être chiffrés via un outil de chiffrement conforme aux normes sectorielles.
3. Les connexions à distance ne peuvent être établies que via des solutions d'accès à distance utilisant une authentification multifacteur (MFA).
4. Les appareils gérés par le Fournisseur doivent être équipés d'un pare-feu personnel actif lorsqu'ils sont directement reliés à Internet (c.-à-d. que le pare-feu ne doit pas être géré par le Fournisseur ou par un mandataire).
5. Les appareils gérés par le Fournisseur doivent être connectés régulièrement au réseau du Fournisseur pour recevoir et installer des mises à jour régulières des logiciels/antivirus afin de pouvoir profiter d'un accès complet au réseau. Un accès limité peut être autorisé dans le but exprès de mettre à jour l'appareil.
6. Si des appareils non gérés et détenus par le Fournisseur sont utilisés pour accéder aux Informations de Citi classées Confidentielles ou de niveau supérieur, ils doivent être configurés de façon à disposer d'une solution agréée n'autorisant pas de téléchargements sur l'appareil local. Les contrôles suivants doivent être en place :
 - a) Les Données de Citi ne peuvent être téléchargées sur un appareil en dehors d'une solution gérée par l'entreprise.
 - b) Le Fournisseur doit s'assurer que cet accès est sécurisé par une authentification basée sur des jetons ou sur des certificats à l'aide de technologies d'accès à distance standard (p. ex., Virtual Desktop Interface (VDI)).
 - c) Les solutions d'accès à distance telles que Terminal Services et VMware Horizon doivent être configurées de façon à désactiver le partage du presse-papiers et le mappage des lecteurs sur les protocoles Blast, PCoIP et RDP, et à désactiver les protocoles RDP et SSH.
7. Si des jetons logiciels sont utilisés pour l'authentification MFA, dans le but d'accéder à une application sur un appareil mobile, le programme d'authentification par jeton logiciel doit authentifier l'utilisateur (par exemple, par mot de passe, par des moyens biométriques, etc.) et empêcher son utilisation si le téléphone mobile est « débridé » ou « enraciné » (utilisation d'un système d'exploitation autre que ceux certifiés et fournis par le Fournisseur de l'appareil mobile).
8. Tout le personnel du Fournisseur, y compris, mais sans s'y limiter, les employés permanents/temporaires et les sous-traitants nécessitant un accès spécial, privilégié et/ou administratif aux systèmes, référentiels de données, applications et/ou infrastructure, y compris, mais sans s'y limiter, les administrateurs système, les administrateurs de base de données, les

administrateurs de contrôle d'accès, les administrateurs de pare-feu, les administrateurs de site Web, etc., qui sont liés directement ou indirectement aux services fournis pour Citi doivent être authentifiés exclusivement par le biais d'une MFA et cet accès sera enregistré et surveillé de manière indépendante par le Fournisseur en ce qui concerne l'activité suspecte et/ou l'accès non autorisé, conformément à ces exigences.

9. Pour les appareils appartenant à des particuliers et les appareils appartenant à un tiers, le Fournisseur doit disposer d'une méthode ou d'une solution efficace pour s'assurer que ces appareils ont une version approuvée du système d'exploitation, des niveaux de correctifs et des logiciels antivirus et antimalware, avant que ces appareils ne soient autorisés à se connecter au réseau.
10. Le Fournisseur doit s'assurer que tout son personnel :
 - a) Maintiendra un espace de travail à distance privé et dédié qui ne contient aucun dispositif d'assistance vocale (par exemple, Siri, Alexa), dispositif d'enregistrement vidéo et/ou tout autre dispositif d'écoute/d'enregistrement photo, vidéo ou audio. Aucun membre du personnel non agréé ne sera autorisé à consulter des données, des systèmes ou des applications qui peuvent apparaître sur l'écran des systèmes informatiques à distance.
 - b) Verrouillera l'appareil informatique lorsqu'il le laissera sans surveillance afin de garantir que tout risque d'accès non autorisé à l'écran est adéquatement atténué.

17.25 Politique du « Clear desk » (bureau rangé)

Le personnel du Fournisseur est tenu de protéger les informations de Citi sous toutes les formes, y compris les informations physiques utilisées ou stockées dans son espace de travail. Les Fournisseurs sont tenus de communiquer cette exigence à l'ensemble de leur personnel au moins une fois par an par le biais d'une formation IS ou d'autres canaux.

17.26 Sécurité incendie

1. Le Fournisseur doit se conformer aux exigences légales et réglementaires applicables régissant la sécurité physique et l'établissement d'un environnement de travail sûr, notamment les codes locaux relatifs aux incendies.
2. Le Fournisseur doit utiliser un ou plusieurs systèmes de détection, d'alarme et d'extinction des incendies. Ces systèmes doivent être inspectés chaque semestre et testés chaque année.

17.27 Sécurité physique

1. Les informations de Citi doivent être stockées dans des zones sécurisées disposant de contrôles qui limitent l'accès au personnel autorisé uniquement.
2. Le Fournisseur doit disposer d'un système de contrôle des accès physiques opérationnel, dûment documenté et auditable.

3. Le Fournisseur est tenu de mettre en œuvre une combinaison de dispositifs de sécurité incluant un système d'alarme anti-intrusion supervisé par un opérateur agréé, ainsi que, selon la nature de l'environnement et des services fournis, des agents de sécurité et un système de vidéosurveillance.
4. Le Fournisseur doit disposer d'une politique documentée en matière de visiteurs, exigeant de tous les visiteurs qu'ils fournissent une identification vérifiable à leur arrivée, à leur entrée et à leur sortie.

17.28 Procédures et responsabilité opérationnelles de sécurité

1. Le processus de gestion des changements du Fournisseur doit impérativement intégrer des contrôles clés aux étapes de l'enregistrement du changement, de la révision, des tests, de l'approbation, de la mise en œuvre et de la clôture. Le Fournisseur doit également disposer d'un processus de modification d'urgence qui nécessite toutes les étapes énumérées ci-dessus, y compris une hiérarchie des approbations obligatoires.
2. Le Fournisseur doit disposer d'un processus vérifiable de gestion des capacités qui comprenne (entre autres) des indicateurs de disponibilité, de capacité et de performance ; une évaluation de l'impact commercial ; et un suivi proactif, une analyse et une correction des problèmes de performance et de capacité.
3. Le cas échéant, le Fournisseur doit s'assurer que les environnements de Laboratoire, de Développement, de Test et de Production sont tous séparés les uns des autres, tant sur le plan physique que logique.

17.29 Exigences en matière de développement logiciel

Applicable aux Fournisseurs livrant des logiciels développés exclusivement pour l'usage de Citi. Les Fournisseurs doivent se conformer à ces exigences ou démontrer qu'ils disposent d'un processus de Software Development Lifecycle (« SDLC ») documenté et approuvé, reposant sur une approche similaire et garantissant un niveau de qualité équivalent.

17.30 Lancement et planification

Le Fournisseur doit définir le périmètre et les objectifs de la solution conformément aux exigences de Citi et à ses obligations contractuelles. Cela comprend :

1. La documentation des exigences fonctionnelles et non fonctionnelles ;
2. La fourniture d'estimations de l'effort nécessaire et des délais ; et
3. L'identification de tous les composants ou dépendances tiers.

Les mesures de mise en conformité, dont les évaluations des risques de sécurité, doivent être mises en œuvre dès le lancement du projet. Les rôles, les responsabilités et les étapes de validation doivent être clairement communiqués.

Tous les environnements doivent être classés en tant que Développement (DEV), Test (TEST) ou Production (PROD) et doivent rester strictement segmentés tout au long du cycle de vie. La classification de l'environnement détermine les droits d'accès et le type de données pouvant être traitées. Le Fournisseur doit restreindre l'accès en fonction de la classification de l'environnement et faire coïncider les déploiements avec

l'achèvement de la phase correspondante du SDLC afin d'empêcher tout accès non autorisé ou toute exposition des données.

17.31 Conception

Le Fournisseur doit documenter une approche de conception garantissant que la solution fournie répond à toutes les exigences énoncées (un « Plan de test »). Un Plan de test doit au minimum inclure et décrire les éléments suivants :

1. 1.Tous les tests devant être réalisés par l'équipe de développement, y compris les tests unitaires, les tests fonctionnels et non fonctionnels, ainsi que les tests de performances, avec traçabilité des exigences ;
2. 2.L'identification du ou des responsables chargés de valider son exécution ;
3. 3.Les exigences en matière de tests de sécurité, telles que les évaluations de vulnérabilité et la modélisation des menaces ; et
4. 4.L'environnement de test, l'approche, le processus et le parcours de validation.

Une stratégie de mise en production doit être élaborée afin de définir les conditions préalables et le processus de mise en production dans les environnements TEST et PROD, notamment les critères de préparation à la mise en production, le contenu et la fréquence des livraisons tout au long du cycle de vie du projet.

Lorsque le Contrat le prévoit, les distributions de logiciels doivent être conditionnées dans un format approuvé par Citi, à l'aide d'outils et de processus approuvés par Citi.

17.32 Tests

Les tests doivent être planifiés et réalisés dans un environnement contrôlé pour confirmer que la solution répond aux exigences et aux critères de réussite définis. Les cas de test doivent pouvoir être rattachés aux exigences et aux modifications apportées au code.

Le Fournisseur doit rédiger un rapport résumant les résultats (réussite/échec), les essais supplémentaires effectués au cours du développement, ainsi que les essais non menés à bien (en précisant les raisons) (un « Rapport de clôture des tests »). Les défauts et les fonctionnalités reportées doivent être consignés, accompagnés de plans d'atténuation pour les problèmes non résolus.

À la demande de Citi, le Fournisseur doit fournir les éléments suivants :

1. Un Plan de test détaillé ;
2. La confirmation de la réalisation des tests et leurs résultats, consignés dans un Rapport de clôture des tests ;
3. La traçabilité des résultats des tests par rapport aux exigences et aux modifications apportées au code.

17.33 Déploiement

Avant le déploiement, le Fournisseur doit effectuer tous les tests de sécurité requis, y compris les analyses de vulnérabilité et la modélisation des menaces. Le processus de mise en production doit être structuré et s'appuyer sur des registres de modifications documentés, des stratégies de restauration et les autorisations requises. Les plans de

mise en œuvre et les guides de déploiement doivent inclure des protocoles de surveillance et de remontée.

Après le déploiement, le Fournisseur doit finaliser les identifiants du système et mettre à jour tous les éléments associés afin de garantir la conformité aux exigences d'audit.

17.34 Sécurité

1. Une évaluation structurée menée au cours de la phase de conception du SDLC pour identifier et traiter les risques de sécurité, les vulnérabilités et les faiblesses architecturales potentiels avant l'écriture du code (un « Examen de la conception de la sécurité ») doit être intégrée au SDLC, avec des contrôles préventifs et de détection conformes aux normes du secteur telles que celles de l'OWASP.
2. Des pratiques de codage sûres doivent être appliquées.
3. Le Fournisseur doit intégrer des contrôles de sécurité des informations dans ses processus et procédures de sélection, de développement et de mise en œuvre d'applications, de produits et de services.
4. Le Fournisseur doit disposer d'une procédure de déploiement sécurisée pour tous les systèmes sur lesquels des informations de Citi sont stockées, traitées et/ou transmises, et doit maintenir une image ou un modèle sécurisé pour tous ces systèmes.

17.35 Lutte contre les logiciels malveillants

Le Fournisseur doit s'assurer que les précautions nécessaires soient prises pour prévenir et détecter l'introduction de tout code malveillant (par exemple, virus, vers, chevaux de Troie, logiciels publicitaires, logiciels espions, rançongiciels ou autres cyberattaques similaires dans lesquelles des données peuvent se trouver compromises). Le Fournisseur doit :

1. Mettre en œuvre, mettre à jour et maintenir des technologies antivirus et antispyware sur tous les ordinateurs personnels et technologies sur tous les Serveurs de réseau local (LAN), les serveurs de courrier électronique et tous les autres dispositifs à même de stocker, traiter et/ou transmettre des données de Citi.
2. Mettre en place des paramètres de sécurité visant à empêcher les utilisateurs finaux de désactiver les outils antivirus/antimalware et les analyses planifiées.
3. Disposer de procédures automatisées gérées de manière centralisée pour la configuration et la mise à jour des logiciels antivirus et anti-malware.
4. Veiller à mettre en œuvre des processus pour identifier et procéder à des corrections au niveau des ordinateurs non conformes, sur lesquels les signatures antivirus ou les moteurs d'analyse sont obsolètes.
5. Contrôler l'accès aux ports de communication/interfaces qui permettent la connexion à des appareils externes, y compris, mais sans s'y limiter, les supports de stockage.

17.36 Lutte contre le code mobile

Les Fournisseurs doivent veiller à la mise en œuvre de contrôles concernant les pratiques sûres en matière de code mobile. Lorsque l'utilisation d'un code mobile est

autorisée, la configuration doit, au minimum, satisfaire à toutes les normes sectorielles concernées et à toutes les obligations contractuelles à l'égard de Citi, et le Fournisseur doit veiller à ce que le code mobile autorisé fonctionne selon une politique de sécurité clairement définie et documentée, et empêcher l'exécution de codes mobiles non autorisés.

Dans le cas d'un code mobile susceptible d'affecter le système d'exploitation sous-jacent ou la plateforme (c'est-à-dire, en dehors du « bac à sable »), le Fournisseur doit faire en sorte que :

1. Le code mobile publié par le Fournisseur soit visé par une autorité de certification agréée par Citi et que le cycle de vie du certificat soit géré par le Fournisseur en cas d'expiration ou de renouvellement du certificat.
2. Un code mobile signé dont les certificats sont arrivés à expiration doit être retiré de la production.

17.37 Journalisation aux fins d'audits

Le Fournisseur devra veiller à ce que tous les Systèmes informatiques contrôlés permettant de consulter, stocker, traiter, gérer et/ou transmettre des données de Citi conservent des pistes d'audit au niveau de l'infrastructure ou de l'application pour enregistrer les éléments suivants :

1. Les actions relevant de la sécurité des infrastructures pour la plateforme associée
2. Toutes les alarmes système associées à un événement de sécurité généré au niveau du pare-feu ou de l'IDS/IPS
3. Toutes les tentatives de violation des sécurités du système (par exemple échecs des tentatives de connexion par un Utilisateur)
4. Les tentatives non autorisées d'accès aux ressources (logiciels, données, processus, etc.)
5. Les actions de l'administrateur
6. Les informations liées à la réception de données spécifiques d'un utilisateur ou d'un autre système
7. Tous les événements importants liés aux transactions financières et aux informations de Citi qui comprennent spécifiquement les éléments suivants :
 - a. Mises à jour des transactions financières
 - b. Mises à jour des données PII confidentielles ou sensibles
 - c. Mises à jour des données à accès restreint
 - d. Mises à jour des données d'authentification
8. La création de toutes les sessions
9. Les attributs de session, tels que les identifiants uniques d'appareil, doivent être récupérés, si cela est techniquement faisable, et consignés pour toutes les applications connectées à Citi (sites Web et applications mobiles), en cas d'enquêtes sur des fraudes. Ces attributs doivent au minimum contenir les adresses IP. Ces artefacts doivent être saisis pour les transactions de Citi et pour l'activité d'ouverture de compte de Citi. Les informations doivent

être saisies afin que l'artefact de la session puisse être lié à la transaction ou à l'ouverture du compte.

10. Les pistes d'audit doivent documenter l'attribution d'une activité spécifique à une personne particulière afin d'empêcher la répudiation.
11. Les événements d'Information Security Administration (ISA) significatifs doivent être consignés, en indiquant notamment les éléments suivants :
 - a) Création d'utilisateurs
 - b) Modification des droits d'accès utilisateur
 - c) Suppression, création et modification de profils sur les Systèmes informatiques contrôlés.
 - d) Réinitialisation des mots de passe
 - e) Changements dans la configuration de sécurité du système
 - f) Toutes les interactions afférentes à des Identifiants fonctionnels privilégiés
 - g) Les journaux de sécurité doivent contenir au minimum les données indiquées ci-dessous, quel que soit le système générant le journal à moins que cela ne soit pas techniquement faisable :
 - I. Date et heure de l'événement (format UTC)
 - II. ID d'utilisateur de la personne effectuant l'action
 - III. Type d'événement
 - IV. Nom de l'actif ou de la ressource concerné(e)
 - V. Type d'accès (suppression, modification, etc.)
 - VI. Réussite ou échec de l'événement
 - VII. Source (terminal, port, emplacement, IP, nom de l'hôte, etc.)

17.38 Protection des informations journalisées

Le Fournisseur doit s'assurer de la mise en œuvre de contrôles d'accès afin de préserver l'intégrité des pistes de vérification pendant l'ouverture, l'arrêt, l'entreposage et la transmission.

1. Afin d'empêcher toute modification non autorisée des journaux d'audit, le Fournisseur doit s'assurer que les journaux ne peuvent être ni écrasés ni modifiés par les utilisateurs du système dont ils suivent l'activité.
2. Le Fournisseur doit fournir à Citi une procédure de conservation des données de journal qui définisse les modalités de conservation de ces données et qui inclue des mesures de conformité faisant référence à l'ensemble des exigences légales et réglementaires applicables.
3. Les horloges de tous les systèmes de traitement de l'information pertinents au sein d'une organisation ou d'un domaine de sécurité doivent être synchronisées avec une source horaire précise.

17.39 Utilisation du système de surveillance

Les Fournisseurs doivent s'assurer que les événements suivants sont saisis, enregistrés et examinés directement ou par le biais d'un processus d'examen automatisé :

1. Toutes les alarmes système associées à un événement de sécurité généré par un pare-feu ou un système de détection des intrusions (IDS)/un système de prévention des intrusions (IPS).
2. Toutes les mises à jour des ressources critiques telles que définies dans la version standard sécurisée.
3. Toute activité interactive effectuée par tout identifiant (fonctionnel, privilégié, système, temporaire, etc.) ayant accès à des informations classées comme PII confidentielles ou de niveau supérieur.
4. Les événements ISA importants indiqués dans la section Journalisation aux fins d'audit ci-dessus, à l'exception suivante :
 - a) Suppression des droits d'un utilisateur, d'un rôle ou d'un profil lorsque l'opération relevant de l'Administration de la sécurité des informations est exécutée par un système de flux de travaux ou un système d'optimisation automatique avec des contrôles d'intégrité de bout en bout.

17.40 Corrélation et examen des journaux

1. Lorsqu'un événement consigné déclenche une alerte et que celui-ci fait l'objet d'un examen, le Fournisseur est tenu de mettre en œuvre des mesures de suivi et de mener une enquête s'il existe des indices laissant supposer qu'un incident de sécurité de l'information potentiellement préjudiciable a pu se produire.
2. Le Fournisseur doit veiller à ce que les journaux d'audit soient centralisés au sein d'un système de gestion des journaux, tel qu'un système de Security Information and Event Management (SIEM) ou tout autre outil d'analyse des journaux, afin de permettre leur corrélation et leur examen.
3. Les Fournisseurs doivent périodiquement revoir et ajuster la configuration de leur outil SIEM ou d'analyse des journaux pour améliorer l'identification des événements exploitables.

17.41 Contrôle des logiciels opérationnels

Le Fournisseur doit s'assurer d'utiliser exclusivement des systèmes d'exploitation et des logiciels bénéficiant d'un support actif de la part d'un Fournisseur commercial reconnu par le secteur, ou faisant l'objet de mises à jour correctives et de configuration appropriées visant à remédier aux vulnérabilités de sécurité.

Le Fournisseur doit veiller à la mise en œuvre d'un processus documenté précisant les délais de correction dans lesquels tous les correctifs de sécurité et toutes les configurations approuvés sont appliqués.

Indépendamment de tout accord de maintenance distinct entre le Fournisseur et Citi, le Fournisseur doit s'assurer que les logiciels développés pour Citi et régis par un accord de licence ne permettent pas l'utilisation de versions de logiciels non pris en charge présentant des vulnérabilités connues, et que ces logiciels sont mis à jour et corrigés selon les besoins en temps opportun.

Les logiciels d'application utilisés pour traiter les Informations de Citi doivent être acquis auprès de Fournisseurs établis et doivent être agréés, catalogués et pris en charge.

17.42 Vulnérabilité et gestion des menaces

1. Le Fournisseur doit mettre en œuvre un processus de gestion des vulnérabilités et des menaces qui traite de manière exhaustive et/ou inclut tous les éléments suivants :
 - a. Des outils et des procédures d'identification et de gestion des vulnérabilités au niveau de l'ensemble des actifs qui peuvent être utilisés pour traiter, stocker, accéder ou transmettre des données de Citi classées Confidentielles ou plus sensibles encore.
 - b. L'obligation de réaliser des analyses au moins une fois par semaine à l'aide d'outils de détection des vulnérabilités et d'une méthodologie de rapport reconnus par le secteur.
 - c. Un classement des vulnérabilités conformément à la version la plus récente du « Common Vulnerability Scoring System (CVSS) » (voir <https://www.first.org/cvss>), avec des délais de correction qui sont fonction de la gravité.
 - d. L'obligation de tester les correctifs de vulnérabilité avant le déploiement complet en production.
 - e. Un processus opérationnel documenté et reproductible pour accélérer la résolution des vulnérabilités critiques.
 - f. Le Fournisseur doit assurer le suivi des actifs tout au long de leur cycle de vie pour se préparer aux statuts End of Life (EOL) ou End of Vendor Support (EOVS), et mettre en place des processus permettant de mettre à niveau ou de remplacer ces actifs de manière proactive.
 - g. Toute vulnérabilité présentant un score CVSS critique, identifiée dans le cadre de la collecte de renseignements, d'analyses de vulnérabilité ou de tests d'intrusion, doit être classée par ordre de priorité et corrigée dans un délai clairement défini et proportionné au risque qu'elle représente.

17.43 Applications hébergées par des tiers

Si le Fournisseur conserve ou stocke des informations confidentielles de Citi ou des données encore plus sensibles sur un site Web ou un système accessible par Internet, ou encore un site Web portant la marque Citi, il devra alors, afin de se protéger contre une vulnérabilité ou une menace qui implique des produits ou des services affectant Citi (chacune étant une « vulnérabilité »), se conformer aux exigences suivantes :

1. Désigner un employé du Fournisseur chargé de répondre aux demandes de Citi concernant la sécurité des informations.
2. Mettre à profit les bonnes pratiques reconnues dans le secteur pour surveiller au moins une fois par semaine les sources fiables d'informations sur les vulnérabilités de sécurité informatique telles que FIRST, CERT/CC, CISA Known Exploited Vulnerabilities Catalog et les listes de diffusion des Fournisseurs, et prendre les mesures appropriées pour obtenir, tester

minutieusement, appliquer et fournir à Citi les packs de service, les correctifs, les mises à niveau et solutions de contournement qui s'appliquent.

3. Tester, au moins une fois par trimestre, la mise en œuvre de ses mesures de sécurité de l'information à l'aide d'outils d'analyse des vulnérabilités du réseau, du système et des applications et/ou de tests d'intrusion.
4. Permettre à Citi ou à une tierce partie approuvée par Citi d'effectuer, à intervalles raisonnables, des évaluations de vulnérabilité, de piratage éthique ou d'autres évaluations de sécurité, pour vérifier la conformité du Fournisseur avec ses obligations en vertu de tout contrat et des présentes exigences, y compris, mais sans s'y limiter, l'examen des politiques, processus et procédures, les évaluations sur site des dispositifs de sécurité physique, l'analyse des vulnérabilités du réseau, du système et des applications et les tests d'intrusion, en utilisant des outils disponibles dans le commerce et/ou des pratiques standard du secteur pour effectuer ces inspections.
5. Tout prestataire qui fournit au Fournisseur des services d'évaluation des vulnérabilités doit figurer sur la liste approuvée par Citi des prestataires d'évaluation des vulnérabilités. Lorsque le Fournisseur fait appel à des prestataires ou à des sous-traitants pour la prestation des services, le Fournisseur doit, à ses propres frais, s'assurer que toutes les évaluations de vulnérabilité requises sont réalisées dans les mêmes délais que si le Fournisseur dispensait directement ces services et doit s'assurer que l'obligation pour tout prestataire ou sous-traitant de faciliter ces évaluations est consignée dans le contrat conclu entre le Fournisseur et le prestataire/sous-traitant concernant le service, y compris les termes autorisant Citi à effectuer ces évaluations.
6. **Notification.**
 - a) Si le Fournisseur identifie une vulnérabilité qui implique un produit ou un service affectant Citi, le Fournisseur en avisera Citi par écrit dans les 24 heures qui suivent l'identification et inclura une description des mesures correctives prises par le Fournisseur.
 - b) Lorsque le Fournisseur prend connaissance d'une vulnérabilité impliquant un produit ou un service affectant Citi suite à une divulgation publique responsable des canaux de processus (publication de la vulnérabilité dans la National Vulnerability Database (NVD) ou via un catalogue de menaces transmis aux Fournisseurs de sécurité externes), le Fournisseur en informera Citi par écrit dans les 24 heures qui suivent cette publication. Chaque notification comprendra des informations sur la vulnérabilité, l'utilité du système pour les services liés à Citi (c'est-à-dire s'il héberge des informations Citi ou est utilisé dans la fourniture de services, ou les deux), si elle peut être exploitée à distance ; et le score Common Vulnerabilities and Exposures (CVE). Le Fournisseur continuera de

fournir des mises à jour à Citi tant que la vulnérabilité n'aura pas été corrigée. Dans les cas où Citi identifie une vulnérabilité, Citi peut en informer le Fournisseur, et le Fournisseur devra remédier rapidement à la vulnérabilité conformément à la présente section.

7. **Actions correctives.** Pour chaque Vulnérabilité notifiée en vertu de la présente Section, la partie notifiante évaluera le niveau de risque et l'impact de cette vulnérabilité en fonction de la gravité et du risque pour Citi et attribuera un niveau de priorité de risque basé sur le Common Vulnerability Scoring System (CVSS) comme indiqué dans l'Annexe A (voir <https://www.first.org/cvss>). Une fois qu'un niveau de risque aura été attribué et convenu par les parties, le Fournisseur remédiera à toute vulnérabilité moyenne, élevée ou critique identifiée. Dans la mesure du possible, la correction de la vulnérabilité devra être mise à disposition dans un paquet de sécurité pour la version actuellement déployée.

Si le Fournisseur n'est pas en mesure ou ne veut pas remédier à la vulnérabilité à la satisfaction de Citi dans le délai imparti, alors Citi pourra résilier la licence applicable sans autre responsabilité ou obligation financière (pour la partie résiliée) et le Fournisseur devra rembourser rapidement à Citi la partie au prorata des droits de licence acquittés.

17.44 Contrôles du réseau de sécurité des communications

1. Les réseaux des Fournisseurs utilisés pour consulter, stocker, gérer, traiter et/ou transmettre les Informations de Citi doivent être protégés contre les menaces et la sécurité doit être maintenue pour les Systèmes informatiques utilisant des points d'application du réseau.
 - a. Les Informations classées Confidentielles ou de niveau supérieur par Citi ne devront pas être stockées de façon permanente sur un système situé dans une Zone démilitarisée (DMZ) connectée à Internet. Les réseaux utilisés pour accéder, stocker, gérer, traiter et/ou transmettre des Informations de Citi au moyen de réseaux locaux sans fil (WLAN) ou d'autres solutions de dispositifs sans fil qui incluent des contrôles raisonnables pour interdire l'accès non autorisé (PEAP-TLS, PAE-TTLS, etc.) peuvent être connectés à des réseaux qui contiennent des Informations de Citi.
 - b. Toutes les connexions IP externes au réseau global du Fournisseur sont protégées par un pare-feu géré par le Fournisseur.
 - c. Un système de détection des intrusions (IDS) et un système de prévention des intrusions (IPS) en temps réel est en place pour surveiller et protéger les connexions Internet au réseau du Fournisseur où sont consultées, gérées, stockées, traitées ou transmises les Informations Citi.
2. Pour toutes les applications Internet portant la marque Citi, le Fournisseur devra s'assurer du respect des points suivants :

- a. Les services hébergés sur les sites du Fournisseur doivent être protégés par des services anti-DDoS (dénial de service distribué) approuvés par Citi ou des contrôles comparables validés par Citi.
- b. Les pare-feu externes doivent être configurés avec une règle de refus d'accès par défaut. Les règles de pare-feu doivent être configurées sur la base du principe du moindre privilège et toutes les tentatives de connexion refusées par le pare-feu (par exemple, abandon de paquets) doivent être consignées/enregistrées.
- c. Le trafic des communications réseau doit, par défaut, être refusé et ne peut être autorisé qu'à titre exceptionnel au niveau des interfaces gérées. Les exceptions doivent être très limitées à des sources, des destinations et des services spécifiques.
- d. Le trafic des applications Web doit faire l'objet de contrôles appropriés et être filtré, notamment à l'aide de pare-feu d'applications Web.

17.45 Séparation au niveau des réseaux

Le Fournisseur doit s'assurer que tous les Systèmes informatiques et applications utilisés pour consulter, stocker, traiter, gérer et/ou transmettre les Informations de Citi et accessibles via Internet ne sont accessibles que via la zone démilitarisée (DMZ) du Fournisseur.

En cas d'urgence, le Fournisseur doit être en mesure de filtrer les accès entre les différentes parties du réseau afin d'atténuer l'impact des incidents liés à la sécurité du réseau (par exemple, le filtrage des ports en cas de virus).

Les mécanismes d'accès à distance et de sécurité des hôtes doivent intégrer des contrôles d'accès fondés sur des groupes (par exemple, le personnel, les sous-traitants) afin de restreindre l'accès aux ressources réseau du Fournisseur. Au niveau de l'hôte, le contrôle d'accès peut être effectué à l'échelle du groupe ou à l'échelle individuelle.

17.46 Identification des équipements dans les réseaux

Les plateformes technologiques doivent identifier et authentifier les plateformes technologiques homologues en fonction des niveaux de risque liés à la sécurité de l'information de l'interaction et d'autres contrôles d'atténuation.

1. Les appareils exclusifs au Fournisseur (c'est-à-dire le matériel informatique, à savoir, entre autres, les ordinateurs de bureau et les ordinateurs portables) conformes aux présentes Exigences et autorisés par le Fournisseur peuvent accéder au réseau du Fournisseur où les Informations de Citi sont stockées, traitées ou transmises.
2. Les appareils exclusifs au Fournisseur (c'est-à-dire le matériel informatique, à savoir, entre autres, les ordinateurs de bureau, les ordinateurs portables et les supports de stockage de données amovibles) qui sont conformes aux présentes Exigences et autorisés par Citi peuvent accéder au réseau de Citi.

17.47 Analyse et spécification des exigences de sécurité

Le Fournisseur doit intégrer des procédures de sécurité des informations dans ses processus et procédures de sélection, de développement et de mise en œuvre d'applications, de produits et de services.

17.48 Transactions en ligne

1. Le cas échéant, le Fournisseur devra disposer de Systèmes informatiques utilisant des mots de passe dynamiques ou des certificats numériques pour valider les informations d'identification.
2. Tous les certificats d'entité finale devront être remplacés au moins une fois tous les 13 mois.
3. Les applications du Fournisseur qui stockent, traitent, gèrent ou accèdent aux Informations de Citi, hébergent des applications Internet de marque Citi ou sont connectées aux ressources réseau de Citi doivent :
 - a. Tirer parti d'une méthode d'authentification basée sur les types de données/fonctions accessibles ;
 - b. Effectuer une évaluation de conformité de l'Authentification multifacteur (MFA) et mettre en œuvre les recommandations, le cas échéant ;
 - c. Effectuer une évaluation de la surveillance des activités suspectes (SAM) lors de l'intégration et mettre en œuvre des recommandations si nécessaire ;
 - d. Dans tous ces cas, le Fournisseur doit contacter son contact commercial principal pour connaître les exigences actuelles de Citi.

17.49 Procédures de contrôle des modifications

1. Le Fournisseur doit s'assurer que les modifications de configuration des pare-feu, des systèmes de détection des intrusions (IDS) et des systèmes de prévention des intrusions (IPS) sont acheminées via le processus de gestion des changements du Fournisseur.
2. L'accès accordé à la production par le biais d'identifiants temporaires doit être enregistré et surveillé pour suivre les changements apportés à l'environnement.
3. Dans le cas de systèmes d'information contrôlés contenant des informations client classées Confidentielles ou de niveau supérieur par Citi, ou dont la valeur de la composante de risque IS pour l'« intégrité » ou la « disponibilité » est élevée, les données récupérées et consignées conformément à la section 17.32 (Journalisation aux fins d'audit) devront être examinées par le Fournisseur. Ces examens peuvent reposer sur une méthode d'échantillonnage appropriée fondée sur les risques.
4. L'examen doit valider que les modifications apportées dans le cadre de l'accès privilégié temporaire ont été effectuées comme prévu.
5. Le Fournisseur doit documenter tous les changements, y compris en consignait les preuves du processus d'examen.

17.50 Fuite d'informations

Le Fournisseur doit avoir en place une norme de codage sécurisé documentée qui empêche la fuite d'informations, notamment :

1. Les informations système détaillées (type de serveur, technologie, etc.) ;
2. Les traces de pile et les messages d'erreur d'exception ne doivent pas divulguer la structure des répertoires ni le type de base de données sous-jacent.

17.51 Données de test

Les informations classées Confidentielles ou de niveau supérieur, telles que définies par Citi, ne devront pas être utilisées ou stockées par le Fournisseur dans des environnements ou laboratoires de développement ou de test d'applications logicielles, à moins que ces informations ne soient dépersonnalisées, masquées et/ou autrement dissimulées à l'aide d'outils et de méthodes conformes aux normes du secteur, de sorte que ces données ne soient plus sensibles, ou le Fournisseur devra mettre en œuvre des contrôles de la production en direct au sein des environnements de développement ou de test.

17.52 Acceptation du système

Le Fournisseur devra avoir mis en place des processus de Gestion de l'étendue des projets (« Project Scope Management ») et de Réception des systèmes (« System Acceptance ») documentés et respectant les normes sectorielles applicables.

17.53 Signalement des faiblesses de la sécurité des informations

Le Fournisseur doit avoir un processus garantissant que les vulnérabilités au niveau des applications ou des infrastructures à même d'affecter les actifs informationnels de Citi **soient signalées immédiatement à Citi.**

17.54 Responsabilités et procédures en cas d'incident de sécurité

1. Un SIRT désigne un événement de sécurité qui compromet l'un des éléments suivants, quels que soient le mode et le lieu de survenue de l'incident de sécurité, ou l'identité de la personne à l'origine de cette compromission :
 - La confidentialité, l'intégrité ou la disponibilité des données de Citi.
 - La confidentialité, l'intégrité ou la disponibilité de toute donnée (y compris les informations à caractère personnel) pour laquelle Citi est soumise à des obligations contractuelles, légales ou réglementaires.
 - L'intégrité ou la disponibilité des systèmes d'information de Citi qui stockent, traitent ou transmettent des données de Citi.
2. Dans le cadre de la présente politique, une atteinte à la confidentialité désigne la divulgation de données à une personne non autorisée, ou toute situation dans laquelle Citi perd la maîtrise et le contrôle de ces données. Tous les incidents de sécurité doivent être signalés immédiatement.

3. Si le Fournisseur a subi un SIRT, il doit coopérer avec Citi en fournissant les informations demandées par Citi conformément à ses propres procédures de réponse aux incidents, et en analysant les données compromises de manière à permettre à Citi de satisfaire aux exigences légales, réglementaires et/ou de gouvernance interne ; effectuer toutes les notifications requises par la loi, les règles ou la réglementation, ou souhaitées par Citi à sa discrétion, à la demande de Citi et aux frais du Fournisseur, et uniquement après que Citi a eu la possibilité d'examiner et de modifier le libellé du modèle de notification proposé ; et le Fournisseur ne doit pas mentionner Citi dans ces notifications, sauf si Citi en fait la demande expresse par écrit.

17.55 Data Leakage Protection (DLP)

Le Fournisseur doit mettre en œuvre des contrôles de prévention des fuites de données (Data Leakage Protection, DLP), y compris la surveillance du contenu et des terminaux qui couvre tout le personnel ayant accès aux données Confidentielles ou de niveau supérieur de Citi.

Le Fournisseur doit mettre en place des contrôles pour détecter et éviter des situations où des données de Citi confidentielles ou de niveau supérieur sortent de son réseau via les canaux suivants :

- a. E-mails non chiffrés
- b. Pièces jointes d'e-mails non chiffrés
- c. Impression de données Citi
- d. Transferts de données Citi vers des sites hors du réseau (par ex. via FTP)
- e. Les tentatives de copie de données Confidentielles ou supérieures de Citi vers un support amovible tel qu'une clé USB, un disque dur externe et d'autres périphériques portables disposant de capacités de stockage de données. Ce privilège doit être évité par défaut.
- f. La solution DLP doit enregistrer et signaler au Fournisseur tout événement correspondant à une tentative (réussie ou interceptée) de déplacer, transporter ou copier des données de Citi confidentielles ou de niveau supérieur de son réseau vers d'autres destinations. Ce privilège doit être évité par défaut.
- g. Transfert de données de Citi vers des sites Web externes, y compris des sites SaaS/de partage de fichiers. Ce privilège doit être évité par défaut.

17.56 Navigation sur Internet

1. Le Fournisseur doit mettre en place des contrôles d'accès Internet pour les employés ayant accès aux données de Citi, afin d'empêcher le partage d'Informations de Citi classées Confidentielles ou de niveau supérieur et l'exposition à des logiciels malveillants ou à des attaques.
2. Pour les Fournisseurs qui ont accès aux données de Citi classées Confidentielles ou de niveau supérieur :
 - a. Toutes les requêtes d'URL doivent être consignées.
 - b. Les tentatives d'accès à des sites pouvant être utilisés pour le partage non autorisé de données Citi (par exemple, messagerie Web, chat, réseaux sociaux, stockage en ligne, etc.) doivent être bloquées.
 - c. L'accès aux sites qui peuvent exposer l'environnement aux logiciels malveillants ou aux attaques doit être bloqué.
 - d. Les tentatives d'accès à des sites considérés comme non liés à l'entreprise doivent être bloquées.
 - e. Le Fournisseur doit s'abonner à un service de catégorisation des URL régulièrement mis à jour ; toutes les URL non catégorisées doivent être bloquées par défaut, ou toutes les URL doivent être bloquées par défaut et approuvées au cas par cas.
 - f. Les navigateurs Web utilisés par le Fournisseur doivent être intégralement pris en charge et mis à jour avec les versions de sécurité les plus récentes fournies par le Fournisseur du logiciel.

17.57 Messagerie électronique

Les messageries instantanées, les réseaux peer-to-peer ou d'autres outils collaboratifs d'Internet ne peuvent pas être utilisés pour transmettre ou stocker des informations Citi en dehors du réseau du Fournisseur ou à partir de réseaux contenant des informations Citi, sauf si un cryptage approprié est en place pour toutes les données Citi conformément à la section 17.9 (Politique relative à l'utilisation de contrôles cryptographiques).

17.58 E-mails

Le Fournisseur doit disposer de mécanismes de contrôle des e-mails pour éviter le partage d'informations de Citi et l'exposition aux logiciels malveillants ou aux attaques. Cela comprend :

1. Les pièces jointes entrantes arrivant au niveau de la passerelle de messagerie sont analysées et bloquées si elles présentent un risque pour le système.
2. Le logiciel de filtrage des e-mails (antispam, antihameçonnage) est actif et à jour.
3. Toutes les données de Citi confidentielles ou de niveau supérieur doivent être chiffrées en cas d'envoi à l'extérieur de l'organisation.
4. Les clients de messagerie utilisés par le Fournisseur sont intégralement pris en charge et mis à jour avec les versions de sécurité les plus récentes fournies par le Fournisseur du logiciel.

17.59 Supports amovibles

1. Le Fournisseur devra protéger les Informations de Citi quel que soit le support sur lequel elles sont conservées. Cette norme s'applique, sans toutefois s'y limiter, aux types de supports stockant des informations tels que : carte, cassette, disque compact (CD), disquette ou autre support de stockage amovible, impression papier, disque magnétique, bande magnétique, microfilm, microfiche, disque optique ou document papier.
2. Le paramètre par défaut pour l'accès aux supports/dispositifs de stockage portables pour les systèmes où les informations Citi sont stockées doit être : Aucun accès. Si des exceptions sont accordées et que l'accès en lecture-écriture est ainsi autorisé, les données doivent être chiffrées sur le dispositif multimédia portable.
3. Si l'utilisation d'un support amovible est autorisée, elle doit être soumise à la validation de la direction, en justifiant notamment la nécessité d'utiliser ce média amovible. Les supports amovibles doivent être répertoriés. Les supports amovibles contenant des données de Citi Confidentielles ou de niveau supérieur doivent être automatiquement chiffrés sans qu'aucune intervention de la part de l'utilisateur ne soit nécessaire.

17.60 Élimination des supports

1. Lorsque les informations de Citi classées Confidentielles ou de niveau supérieur sont éligibles à être détruites conformément aux instructions données par Citi (c'est-à-dire à un stade où l'information n'est plus nécessaire ou utile à Citi, et que les délais de conservation supplémentaires légaux, réglementaires et/ou imposés par les politiques de Citi sont respectés), le Fournisseur devra détruire ces Informations afin qu'elles soient inutilisables et irrécupérables.
2. Un outil agréé, capable de réécrire aléatoirement les secteurs du disque à l'aide de caractères spécifiques et distincts, doit être utilisé afin d'effacer de manière sécurisée tout support installable, conformément aux règles suivantes :
 - a. Pour les supports stockant des Informations classées Confidentielles ou de niveau supérieur, l'outil doit effectuer trois passages sur le support.
 - b. Démagnétisation des supports (le cas échéant).

3. Destruction physique des supports pour les rendre illisibles (c.-à-d. déchiquetage, écrasement des disques).
4. Le papier et les autres supports de stockage non électroniques contenant des Informations classées Confidentielles ou de niveau supérieur doivent être collectés et stockés de manière sécurisée dans une « Corbeille Confidentielle » avant leur destruction finale. Les Corbeilles confidentielles doivent toujours être verrouillées et accessibles uniquement au personnel autorisé.
 - a. Les photocopieuses, imprimantes, fax et autres appareils disposant d'une mémoire/capacité de stockage, susceptibles de contenir des Informations classées Confidentielles ou de niveau supérieur doivent également être « nettoyés ».

17.61 Gestion de la sécurité des informations et formations sur le sujet

1. Tenir à jour un programme approprié de sensibilisation et de formation à la cybersécurité et à la sécurité de l'information, qui comprenne, entre autres, la prévention des attaques par hameçonnage et autres attaques d'ingénierie sociale, le traitement approprié des informations confidentielles ou de niveau supérieur, ainsi que la gestion des rapports et des réponses aux incidents de sécurité.
2. Le Fournisseur devra veiller à ce que tous les employés, y compris les sous-traitants et le personnel temporaire, reçoivent une formation et une sensibilisation appropriées sur les politiques et procédures organisationnelles, selon leur pertinence par rapport à leurs fonctions professionnelles.
3. Le Fournisseur doit veiller à ce que le programme de formation et de sensibilisation soit révisé et mis à jour chaque année afin de tenir compte des risques et menaces émergents, des bonnes pratiques actuelles et des nouvelles technologies dans le domaine de la cybersécurité.
4. Les thèmes suivants devront impérativement être abordés :
 - b. Classification et traitement des informations
 - c. Transmission sécurisée (e-mails sécurisés, stockage SharePoint sécurisé, pas d'envoi de données appartenant à Citi vers des adresses e-mail personnelles)
 - d. Signalement des incidents de sécurité des informations
 - e. Lieu de travail sécurisé (p. ex., utilisation appropriée d'Internet, logiciels non autorisés, interdiction de télécharger des logiciels non approuvés)
 - f. Gestion des mots de passe (p. ex., mots de passe forts, interdiction de partage des mots de passe)
 - g. Ingénierie sociale (p. ex., phishing, spear fishing, vishing, SMishing)
 - h. Télétravail (p. ex., connexion sécurisée/sécurité, sécurité des appareils personnels)

5. Les employés des Fournisseurs doivent suivre la formation avant ou au moment où ils obtiennent l'accès aux systèmes hébergeant les données de Citi et l'avoir terminée avant la date limite indiquée dans la notification de mission.
 - a. Une formation IS devra être dispensée à l'ensemble du personnel au moins une fois par an, sauf si la loi l'interdit.
6. La formation doit inclure un outil permettant d'évaluer son efficacité (p. ex., un questionnaire à la fin de la formation avec un seuil de réussite/échec), lorsque la législation locale le permet.

17.62 Programme de gestion du risque cybernétique

Le Fournisseur devra également, au minimum, avoir un programme approprié de gestion des risques cybernétiques comprenant au moins les éléments suivants :

1. Un programme de gestion des risques de sécurité des informations bien défini et documenté, et/ou un programme de gestion des risques opérationnels comportant une composante de gestion des risques de cyber information clairement définie, qui définit l'appétence du Fournisseur au risque cybernétique et garantit que son risque cybernétique résiduel s'aligne sur cette appétence.
2. Un programme robuste de gouvernance de la gestion des risques de sécurité qui comprend, sans s'y limiter, la collecte et/ou la réalisation d'audits et d'examens de sécurité qui évaluent l'état général de la sécurité au sein de l'organisation, et qui rend compte au moins une fois par an à la direction générale pour examen et assurance que l'appétence du Fournisseur au risque cybernétique n'a pas été enfreinte.
3. Le respect de la conformité avec toutes les normes PCI Data Security Standards (PCI-DSS) applicables au Fournisseur lorsque celui-ci traite, stocke et/ou transmet des transactions par carte de crédit/débit, des paiements et/ou des informations.
4. Un plan et un guide de gestion des crises, ainsi qu'un plan d'intervention en cas d'incident de sécurité conforme aux normes du secteur, afin de garantir que le Fournisseur dispose des capacités suffisantes et adéquates pour détecter, contenir, enquêter, réagir et se remettre de toute tentative, suspicion et/ou incident réel de cybersécurité.

17.63 Sécurité des applications, des API, du code, du système et de l'infrastructure

Lorsque le Fournisseur héberge, développe, co-développe, procure des environnements de développement et/ou fournit une ou plusieurs applications logicielles, le Fournisseur doit effectuer des examens de code dudit logiciel et/ou des correctifs au logiciel pour les failles de sécurité, la prévention de l'accès non autorisé, la modification et/ou l'insertion de logiciels malveillants ou d'autres formes de code malveillant, et des tests de vulnérabilité pour s'assurer que l'application (y compris les API), ainsi que les services système sous-jacents, les systèmes d'exploitation et les réseaux sont exempts de vulnérabilités et de défauts connus qui pourraient entraîner un incident de sécurité, une violation de la vie privée, une fraude, un accès et/ou une divulgation non autorisés d'informations confidentielles, une perte d'intégrité des informations traitées, stockées ou transmises par la ou les applications et/ou une perte

de disponibilité qui pourrait affecter la qualité des produits et/ou services que le Fournisseur procure à Citi.

17.64 Sécurité mobile

Lorsque le Fournisseur fournit une application mobile, il doit se conformer aux exigences suivantes :

1. L'application mobile ne doit prendre en charge que la ou les version(s) généralement disponible(s) (GA) / stable(s) et non-EOL² du système Google Android (à l'exclusion d'Android Go) et/ou des plateformes Apple iOS / iPadOS. Si la solution mobile est dotée d'une prise en charge de solutions supplémentaires, les systèmes/versions d'exploitation pris en charge doivent être configurables par Citi.
2. La solution mobile ne doit pas prendre en charge des plateformes ou appareils mobiles qui ne sont pas équipés d'ensembles d'instructions régulières permettant de prendre en charge des algorithmes cryptographiques, y compris, entre autres, le chiffrement tel que spécifié à la section 17.9 (Exigences de chiffrement) du présent document.
3. Les versions des systèmes d'exploitation antérieures à la production, y compris, mais sans s'y limiter, les versions bêta, l'accès anticipé et les versions de prévisualisation, ne sont pas autorisées dans l'environnement de production.
4. Le Fournisseur devra être en mesure de fournir la liste des composants tiers intégrés, y compris, mais sans s'y limiter, les bibliothèques logicielles libres et en open source qui sont regroupées/exploitées par la solution mobile.
5. L'application mobile doit respecter les exigences et les bonnes pratiques qui permettent la publication des applications mobiles sur les magasins d'applications publics, tels que l'App Store d'Apple ou le Google Play Store. Les plateformes d'applications publiques énumérées doivent constituer le moyen privilégié et principal de distribution et de publication de l'application mobile.
6. Les applications mobiles Android doivent exploiter le système de signature APK v2+. La version 1 du schéma APK Signature (également connue sous le nom de signature JAR) ne doit pas être utilisée.
7. Le type et la longueur de la clé de signature de l'application mobile doivent respecter ce qui est indiqué à la section 17.9 - **Exigences en matière de chiffrement** du présent document.
8. Chaque clé de signature de l'application et le certificat X.509v3 associé doivent être gérés individuellement et dédiés à un seul identifiant

² Les versions du produit qui sont activement prises en charge et reçoivent régulièrement des mises à jour de sécurité et d'entretien de la part du propriétaire de la plateforme ou du Fournisseur.

d'application/identifiant de groupe d'applications. La ou les clés de signature ne doivent pas être échangées entre les différentes applications.

9. Si une application mobile nécessite la conservation des données sur l'appareil mobile, elle ne doit conserver sur l'appareil que les données les plus récentes nécessaires aux fins de l'application/du service, ou aussi longtemps que nécessaire conformément aux exigences légales/ou réglementaires.
 - a. La collecte, le traitement et/ou le stockage des données des utilisateurs doivent être conformes aux lois locales, y compris, entre autres, aux réglementations en matière de confidentialité, telles que le Règlement général sur la protection des données (RGPD) et la directive 2002/58/CE (ePrivacy) ou leurs équivalents régionaux.
 - b. Les composants tiers intégrés (par exemple, les bibliothèques) ne doivent pas recueillir, traiter et/ou stocker les données des utilisateurs.
10. Les applications mobiles ne doivent rendre aucune donnée d'application accessible dans le monde entier.
 - a. Si le partage de données avec d'autres applications est nécessaire, les applications doivent exploiter des techniques, méthodes et contrôles raisonnables sur le plan commercial pour que les systèmes d'exploitation respectifs ne communiquent que la quantité nécessaire de données au nombre minimum d'autres applications, et un tel partage de données devra être dûment justifié et documenté.
11. Les applications mobiles doivent uniquement s'appuyer sur des moyens de communication sûrs fournis par leurs systèmes d'exploitation mobiles respectifs. Par exemple :
 - a. Les applications Android doivent déclarer explicitement dans le manifeste de l'application et/ou dans son fichier de configuration réseau que le trafic réseau non sécurisé n'est autorisé vers aucun domaine de réseau.
 - b. Les applications iOS/iPadOS doivent tirer parti de la Application Transport Security (ATS) sans aucune exception.
12. Les documents cryptographiques doivent être liés à un magasin de clés sécurisé adossé au matériel.
13. Les applications mobiles doivent être construites en mode « release » et ne doivent contenir :
 - a. Aucune fonctionnalité ou méthode susceptible de contourner les contrôles de sécurité ;
 - b. Aucune information de débogage, telle que les noms des fichiers de code source, les noms des variables, les noms des symboles, etc., susceptibles de faciliter la rétro-ingénierie.
14. Les applications mobiles doivent être équipées de mécanismes efficaces anti-crochetage ou anti-manipulation pour empêcher l'injection de code

malveillant susceptible de modifier ou de surveiller le comportement de l'application au moment de son exécution.

15. Les applications mobiles doivent mettre en œuvre des techniques complètes d'anti-débogage ou d'anti-rétro-ingénierie/dissimulation afin d'empêcher les attaques par rétro-ingénierie.
16. Les progiciels d'application mobile doivent être dotés de la capacité de vérifier l'authenticité et l'intégrité de leur contenu (par exemple, à l'aide d'une somme de contrôle cryptographique et/ou d'une signature numérique).
17. Si l'application mobile nécessite une authentification de l'utilisateur, les contrôles d'intégrité de l'application et/ou de l'appareil doivent être effectués avant le début de l'authentification d'utilisateur.
18. Les applications mobiles qui accèdent à, traitent ou stockent des informations appartenant à Citi classées Confidentielles ou de niveau supérieur et/ou dont le niveau de risque IS est moyen ou plus élevé doivent utiliser uniquement des modalités biométriques robustes (par exemple, respecter ou dépasser la catégorie de classe 3 / robuste telle que définie dans le [Android Compatibility Definition Document](#) correspondant).
19. Les applications mobiles doivent mettre en œuvre des contre-mesures pour protéger contre les attaques de type « Man-in-the-middle » (MitM).
20. Les applications mobiles doivent être en mesure de détecter les appareils compromis (entre autres, les appareils mobiles « débridés » ou « enracinés ») et de réagir conformément à l'évaluation des risques et aux exigences réglementaires de l'entreprise.
21. Les applications mobiles doivent mettre en œuvre une liaison forte avec l'appareil afin d'empêcher le clonage du jeton logiciel (par exemple, la preuve de détention).
22. Les applications mobiles doivent utiliser des applications/solutions de clavier sécurisées (p. ex., celles intégrées/préinstallées par les systèmes d'exploitation mobiles).
23. Les notifications push ne doivent contenir aucune information sensible (p. ex., des Informations de Citi classées Confidentielles ou de niveau supérieur). Toutefois, un mot de passe à usage unique (OTP) peut être distribué par notification push.
24. Les solutions d'applications mobiles doivent être équipées d'une capacité de rejeter/d'ignorer les tentatives de communication avec les clients mobiles qui utilisent des versions d'applications présentant des vulnérabilités connues/exploitable.
25. Les applications mobiles doivent respecter les bonnes pratiques du secteur, y compris, entre autres, les techniques de prévention publiées dans l'[OWASP Mobile Top 10](#).
26. Les applications mobiles qui exploitent les techniques d'intelligence artificielle et d'apprentissage automatique (IA/AA) doivent le faire de manière éthique et conformément à la Section 19 – Erreur : source de la référence non trouvée (y compris l'IA générative et l'IA agentique).

27. L'application mobile doit exploiter la ou les autorisations minimales des appareils requis pour effectuer la ou les fins/fonctions exploitées par Citi.
28. Les applications mobiles ne doivent pas stocker d'informations non publiques sur un stockage externe/amovible, comme des cartes SD. Erreur : source de la référence non trouvée **Error! Reference source not found.**

17.65 Divulcation des logiciels

Le Fournisseur est tenu de divulguer l'ensemble des composants logiciels, y compris, sans s'y limiter, les logiciels open source contenus dans les produits ou services fournis à Citi (collectivement dénommés « Composants logiciels »). Le Fournisseur ne procédera, par le biais d'une mise à jour, d'une mise à niveau ou de toute autre manière, à l'intégration d'aucun Composant logiciel dans aucune version des produits ou services destinés à être installés sur les Systèmes de Citi sans en avoir préalablement informé Citi dans chaque cas. En outre, le Fournisseur devra s'assurer que ses produits ou services ne comprennent pas de Composants logiciels dont la licence est soumise à des conditions qui imposeraient à Citi ou à ses Filiales des obligations non expressément mentionnées et acceptées par Citi dans un Contrat. Le Fournisseur est tenu de signaler à Citi tout composant logiciel malveillant détecté au sein de son organisation, de ses produits ou de ses services, dans un délai de 30 jours à compter de sa découverte. Plus précisément, le Fournisseur devra divulguer son utilisation de Composants logiciels à chaque publication et version des produits ou services en fournissant à Citi une nomenclature logicielle (Software Bill of Materials, « SBOM ») soit au format de fichier OWASP CycloneDX, soit au format de fichier de spécification ISO/CEI 5962:2021 Software Package Data Exchange (« SPDX »). Cette divulgation doit préciser l'origine des Composants logiciels (p. ex., fournisseur commercial, base de données intégrée, gestionnaire de paquets binaires public, compilation à partir du code source, ou tout logiciel embarqué ou fournisseur de Composants logiciels sélectionnés), et si le Fournisseur ou l'un de ses fournisseurs en amont dans la chaîne d'approvisionnement logicielle a réalisé une copie des Composants logiciels (ce que l'on appelle un « fork ») et l'a ensuite intégrée à ses produits ou services, soit en tant que dépendance de paquet, soit sous forme de code source intégré au code source du Fournisseur à partir duquel les produits et services sont compilés.

17.66 Modélisation des menaces

Le Fournisseur doit mettre en œuvre un processus de modélisation des menaces qui traite de manière exhaustive et/ou inclut tous les éléments suivants :

1. Définition du champ d'application : Le Fournisseur doit définir clairement le périmètre du modèle de menace, en mettant l'accent sur les composants logiciels et les flux de données qui traitent, stockent ou transmettent des informations classées « Citi Confidential » ou d'un niveau de confidentialité supérieur.
2. Identification des menaces : Le Fournisseur doit identifier systématiquement les menaces et vulnérabilités potentielles liées à la conception, à l'architecture et à l'utilisation prévue du logiciel, en tenant compte dès les

premières étapes du cycle de vie de la conception des différents vecteurs d'attaque et acteurs malveillants.

3. Analyse des risques : Le Fournisseur doit analyser les menaces identifiées pour évaluer leur impact potentiel et leur probabilité, ce qui permettra de hiérarchiser les risques de sécurité.
4. Intégration des contrôles : Le Fournisseur doit définir et intégrer des mesures de sécurité et des stratégies d'atténuation appropriées dans la conception et le développement du logiciel afin de faire face à ces risques classés par ordre de priorité.
5. Documentation : Le Fournisseur doit documenter le modèle de menaces, y compris les menaces identifiées, les risques associés et les mesures d'atténuation correspondantes mises en œuvre.
6. Contrôle périodique : Le Fournisseur doit régulièrement examiner et mettre à jour les modèles de menaces, en particulier lorsque des changements importants sont apportés à la conception, aux fonctionnalités ou à l'environnement de déploiement du logiciel.

17.67 Intelligence artificielle

1. Les Fournisseurs doivent mettre en œuvre et respecter un Secure Software Development Lifecycle (SSDLC) rigoureux pour tous les systèmes et composants d'IA/AA fournis à Citi ou intégrés à ses systèmes. Cela inclut la conception, le développement, les tests, le déploiement et la maintenance continue sécurisés.
2. Les systèmes d'IA fournis par les fournisseurs doivent faire preuve d'intégrité dans leur fonctionnement et présenter une résistance solide aux attaques adversaires. Cela implique notamment la mise en place de mécanismes permettant de détecter rapidement les injections, de valider les données d'entrée et d'assurer l'isolation des données.
3. Les agents et composants d'IA fournis par les fournisseurs doivent interagir de manière sécurisée avec les systèmes de Citi et ses autres outils. Cela nécessite une gestion rigoureuse des identités et des accès, une validation stricte des arguments d'exécution des outils, ainsi que l'isolation des opérations à haut risque effectuées par ces outils. Des mécanismes Human-in-the-Loop (HITL) doivent être intégrés pour les actions sensibles ou à haut risque.
4. Les systèmes d'IA des Fournisseurs doivent générer des journaux complets, immuables et vérifiables pour tous les événements importants. Ces journaux doivent être protégés contre toute altération, agrégés et conservés conformément aux politiques de Citi. Des capacités de surveillance continue et de détection des anomalies sont nécessaires pour identifier les incidents liés à la sécurité et les activités suspectes, et pour signaler leur présence.
5. Les systèmes d'IA des Fournisseurs doivent permettre un contrôle humain fondé sur les risques, afin de faciliter une intervention appropriée, et être conçus de manière à garantir une responsabilité claire quant aux résultats et aux actions de l'IA. Cela implique notamment de classer les résultats générés par l'IA en fonction de leur niveau de risque et de permettre aux utilisateurs de passer outre les décisions de l'IA.

6. Tous les agents, composants et systèmes d'IA fournis par les fournisseurs doivent intégrer des contrôles rigoureux en matière de gestion des identités et des accès. Chaque interaction avec l'IA doit pouvoir être attribuée à une identité identifiable (humaine ou non humaine), et tout accès doit faire l'objet d'une authentification. Les agents d'IA doivent utiliser des identités gérées et respecter les principes du privilège minimal lorsqu'ils accèdent aux ressources de Citi.
 - a. Les Fournisseurs doivent mettre en place et s'assurer que tous les agents d'IA se voient attribuer des identités d'agent Citi Object Identity Network COIN, fédérées avec les systèmes Identity and Access Management (IAM) de Citi, afin de permettre l'application des politiques de sécurité de Citi, la gestion centralisée des identités et la traçabilité.
 - b. Les Fournisseurs doivent intégrer des agents tiers à COIN à l'aide des mécanismes d'intégration approuvés par Citi, notamment l'API COIN mise à disposition via des passerelles sécurisées (telles que SSG Gateway ou Apigee), et doivent veiller à ce que cette intégration soit effectuée de manière sécurisée, conformément aux exigences de sécurité applicables de Citi.
 - c. Les Fournisseurs, s'ils sont hébergés en interne, doivent générer leur propre jeton compatible avec COIN ; les Fournisseurs hébergés en externe et s'authentifiant en entrée à l'aide de leur propre jeton fédéré doivent disposer d'un jeton d'échange pris en charge pour les jetons Citi, p. ex., pour échanger des jetons MSFT contre des jetons COIN. Tout nouveau type de jeton qui n'est actuellement pas pris en charge par la plateforme d'échange doit faire l'objet d'un examen par l'équipe IAM de Citi en vue de son approbation.
7. Lorsque les fournisseurs utilisent ou fournissent des serveurs ou des clients MCP (Model Context Protocol), ils doivent mettre en œuvre la spécification MCP RFC 7591, y compris toutes les fonctionnalités optionnelles.
8. Les systèmes d'IA des Fournisseurs doivent empêcher toute divulgation ou manipulation des invites et des mécanismes internes du système. La gestion du contexte doit imposer des limites strictes afin d'empêcher toute fuite de données entre les locataires, les utilisateurs ou les environnements.
9. Les Fournisseurs doivent disposer de procédures documentées permettant de détecter, de traiter et de signaler les incidents de sécurité spécifiques à l'IA, notamment les attaques malveillantes, la manipulation de modèles, les actions non autorisées liées à l'IA ou les violations de données impliquant des systèmes d'IA. Tout incident de ce type doit être signalé immédiatement à Citi.

18 DIRECTIVES RELATIVES A LA SECURITE SUR LE LIEU DE TRAVAIL

Applicable aux Fournisseurs qui accèdent/traitent/gèrent/stockent des Informations de Citi ET/OU hébergent des applications Internet de marque Citi ET/OU sont connectés aux ressources réseau de Citi ET/OU nécessitent un accès sans escorte aux locaux de Citi.

Les Fournisseurs devront protéger les actifs corporels et incorporels de Citi et de ses clients. Les actifs de Citi et du Client pourront être utilisés uniquement à des fins approuvées et de manière approuvée (p. ex., conformément aux licences, termes et conditions applicables) et uniquement en lien avec les objectifs commerciaux de Citi et des Fournisseurs de Citi. Les actifs comprennent les espèces, les valeurs mobilières, les biens matériels, les services, les plans commerciaux, les informations Citi, les informations sur les Fournisseurs, les informations sur les distributeurs, la propriété intellectuelle (programmes informatiques, modèles et autres éléments) et toutes les autres informations personnelles, exclusives et confidentielles. Le détournement ou la divulgation non autorisée des actifs de Citi constitue une violation de votre obligation envers Citi et peut constituer un acte de fraude à l'encontre de Citi. De même, la négligence, le gaspillage ou l'utilisation non autorisée des actifs de Citi constitue également une violation de votre obligation envers Citi.

Élément	Exigences
Informations de Citi (documents électroniques et physiques)	Verrouiller et sécuriser les informations de Citi après les heures de travail normales et chaque fois que le Fournisseur s'éloigne de l'espace de travail désigné.
Ordinateur personnel de bureau (PC) et ordinateurs portables	Les PC et ordinateurs portables utilisés pour accéder à ou consulter des informations Citi doivent être sécurisés par mot de passe sur l'écran de veille après une période d'inactivité. Chaque fois qu'un Fournisseur s'absente de son espace de travail, il doit verrouiller son PC ou ordinateur portable en appuyant simultanément sur CTRL-ALT-SUPPR et en sélectionnant « Verrouiller ». Si un Fournisseur utilise un ordinateur portable pour consulter les informations de Citi, il doit s'assurer que cet ordinateur portable est sécurisé par câble ou par des verrous de sécurité à l'unité de base pendant les heures de travail et verrouillé de manière sécurisée après les heures de travail normales.
Verrouillage	Les classeurs et les tiroirs qui stockent les Informations Citi doivent être verrouillés après les heures normales de travail.
Bureaux en open space	Les espaces de bureaux en open space ne doivent pas être utilisés comme serveurs de fichiers/mini centres de données pour stocker les Informations de Citi, à moins qu'ils ne soient spécifiquement conçus pour une telle utilisation et documentés à cette fin en collaboration avec Citi.

Élément	Exigences
Bacs d'imprimantes, de photocopieuses et de télécopieuses	Tous les documents liés à Citi doivent être retirés des bacs d'imprimantes, de photocopieuses et de télécopieuses.
Élimination	Éliminer les informations de Citi qui ne sont plus requises (suivre des calendriers de conservation spécifiques). Les documents doivent être déchiquetés ou placés dans un bac de recyclage sécurisé ou verrouillé. Les supports magnétiques doivent être éliminés de manière sûre après que les procédures d'effacement appropriées ont été suivies.

19 INTELLIGENCE ARTIFICIELLE/APPRENTISSAGE AUTOMATIQUE (Y COMPRIS L'IA GENERATIVE/L'IA AGENTIQUE)

Applicable aux Fournisseurs qui utilisent l'Intelligence artificielle/Apprentissage automatique (AI/AA), y compris l'IA générative et l'IA agentique, tel que défini par Citi dans ces Exigences à l'égard des Fournisseurs, dans toute partie du produit/service qu'ils fournissent.

19.1 Le Fournisseur s'engage à ne pas utiliser, et à veiller à ce qu'aucun sous-traitant n'utilise, les technologies d'IA/AA décrites ci-dessous, à moins qu'une telle utilisation n'ait été convenue entre les Parties dans l'annexe ou le bon de commande applicable au titre du Contrat :

- a. Utilisé(e), contenu(e) ou autrement incorporé(e) dans tout produit ou service pour lequel il est sous Contrat pour fournir directement ou indirectement à Citi, ou dans toute partie de celui-ci, y compris tout produit ou service tiers contenu ou intégré dans celui-ci ; ou
2. Utilisé(e) de quelque manière que ce soit dans l'exécution de tout Contrat par le Fournisseur, que cet(te) IA/AA soit ou non utilisé(e), contenu(e) ou autrement incorporé(e) dans le produit ou service réel fourni à Citi ; ou
3. Utilisé(e) par le Fournisseur d'une manière susceptible d'exposer les Informations de Citi à un(e) tel(le) IA/AA, y compris, mais sans s'y limiter, tout(e) IA/AA utilisé(e) par le Fournisseur dans ses opérations non commerciales (par exemple, tenue de registres commerciaux, améliorations de processus, recherche et développement, conformité et audit interne).

19.2 Le non-respect par le Fournisseur de ces obligations sera considéré comme une violation substantielle des conditions du présent Accord.

19.3 À la demande d'un régulateur, dans le cadre d'une inspection réglementaire ou d'une enquête forensique sur l'utilisation de cet(te) IA/AA dans toute partie du produit/service, le Fournisseur doit aider Citi à répondre à la demande du régulateur, y compris en menant et/ou en facilitant la réalisation d'audits

d'algorithmes nécessaires pour découvrir les opérations réelles des algorithmes compris dans les modèles IA/AA.

19.4 Les principes suivants doivent également être respectés :

Légalité. Le Fournisseur d'IA/AA doit se conformer au droit applicable.

Objectif et proportionnalité. Le Fournisseur ne doit pas fusionner les contenus ou les informations de Citi avec ceux du Fournisseur ou avec des données de tiers. Le Fournisseur ne doit pas utiliser de contenus ou d'informations de Citi pour former l'IA/AA sans l'approbation écrite de Citi. Le Fournisseur d'IA/AA ne doit pas utiliser de contenus ou d'informations de Citi, sauf dans la mesure nécessaire à la fourniture des services.

20 PLAINTES DE CLIENTS

20.1 Une plainte est une communication orale ou écrite, qui peut être reçue oralement (en personne ou par téléphone) ou par écrit (par courrier ou par communications électroniques telles que courriers électroniques, messages instantanés ou messages sur les réseaux sociaux, etc.), qui exprime le mécontentement d'un client, d'un non-client ou d'un client potentiel de Citi, ou encore d'un représentant autorisé d'un client (collectivement, un « client ») au sujet d'une politique de Citi, d'un produit ou d'un service proposé par ou par l'intermédiaire de Citi, d'un employé de Citi, d'un sous-traitant de Citi ou d'un prestataire de services tiers agissant au nom de Citi, ou de toute combinaison de ce qui précède.

20.2 Les Fournisseurs doivent respecter la politique de traitement des plaintes des clients de Citi, ainsi que toutes les normes et procédures applicables de Citi en matière de plaintes. Le Fournisseur informera par écrit son interlocuteur principal chez Citi (ou la personne désignée par celui-ci) dans un délai de vingt-quatre (24) heures de toute manifestation écrite ou orale d'insatisfaction ou de préoccupation (ci-après dénommée « plainte » reçue par le Fournisseur de la part d'un Client (ou d'un non-client ou d'un client potentiel, conformément à la définition de « plainte » de Citi) ou d'une autorité de régulation, concernant les Services fournis par le Fournisseur pour le compte de Citi, ou liés de quelque manière que ce soit à Citi. À moins que Citi ne mette un tel système à la disposition du Fournisseur, ce dernier élaborera, mettra en œuvre et maintiendra également un système (« système de suivi ») raisonnablement satisfaisant pour Citi afin d'effectuer un suivi des plaintes et de fournir à Citi, à sa discrétion, une copie des rapports ou un accès au système. Le système de suivi :

- a. catégorisera les plaintes par type, date de réception et date à laquelle un avis de plainte a été fourni à Citi,
- b. effectuera le suivi du traitement de la plainte jusqu'à sa conclusion/résolution, et
- c. répondra à toutes les autres questions susceptibles d'être raisonnablement posées par Citi. Le système de suivi devra être conçu pour permettre au

Fournisseur de déterminer s'il reçoit un nombre excessif de plaintes concernant une question particulière afin que le Fournisseur (en consultation avec Citi) puisse déterminer s'il existe un problème systémique concernant l'activité du Fournisseur ou sa prestation de services et corriger rapidement les problèmes.

21 POLITIQUE RELATIVE AUX OPÉRATIONS PERSONNELLES ET AUX INVESTISSEMENTS

La Personal Trading and Investment Policy (Politique de négociation et de placement à des fins personnelles, PTIP) de Citi définit les activités de négociation et de placement autorisées et interdites, les exigences en matière d'autorisation préalable et les exigences concernant le maintien, la divulgation et la surveillance des comptes de courtage ou de négociation d'une personne couverte. Elle définit des normes minimales pour promouvoir le respect des lois et réglementations afin d'empêcher l'utilisation inappropriée de la position ou de la relation d'une personne avec Citi, notamment ses connaissances (1) de Material Non-Public Information ou d'informations privilégiées (collectivement, appelées « MNPI ») concernant Citi ou un tiers ; ou (2) d'informations concernant les positions, les transactions et les stratégies des clients en matière de titres, de produits dérivés et de matières premières.

Tout le personnel du Fournisseur qui a besoin d'un accès régulier aux MNPI dans le cadre de ses responsabilités professionnelles chez Citi et qui est désigné comme personne couverte et/ou personne bénéficiant d'un accès à Citi doit respecter les exigences de la PTIP. Le personnel du Fournisseur devra se conformer aux demandes de l'ICRM liées à la divulgation des comptes personnels, à l'autorisation préalable des activités de négociation à titre personnel, les restrictions applicables à ces opérations ainsi que la remise de déclarations périodiques.

22 NORMES EN MATIÈRE DE FACTURATION

Dans le cadre des efforts de Citi pour améliorer la ponctualité des services et renforcer les contrôles, tous les Fournisseurs doivent soutenir les méthodes privilégiées de soumission de facture de Citi, ainsi que les options de paiement de facture, telles que détaillées ci-dessous :

- Le Fournisseur créera des fichiers électroniques à transmettre à Citi dans le format communiqué par Citi au Fournisseur et/ou utilisera l'outil Citi iSupplier pour saisir les données de facturation requises en vue d'une transmission numérique ultérieure à Citi.
- Le Fournisseur transmettra à Citi toutes les informations bancaires requises et tous les documents à l'appui pour faciliter le paiement électronique au Fournisseur et/ou utilisera l'offre de paiements par carte virtuelle proposée par Citi (le cas échéant).

Remarque : Les conditions de paiement sont calculées à partir de la date à laquelle la facture est reçue par Citi.

Pour le paiement en temps voulu et le respect des engagements contractuels, Citi exige que tous les Fournisseurs incluent les données de facturation suivantes et respectent les lignes directrices connexes lorsqu'ils facturent Citi pour des biens ou des services :

1. La bonne entité commerciale de Citi, l'adresse de facturation et le nom du contact commercial associé à Citi.
2. Numéro de facture, date de facture et numéro de bon de commande.
3. Les factures doivent être envoyées à l'adresse de Citi ou à l'adresse e-mail détaillée sur le bon de commande de Citi.
4. Les biens ou services facturés doivent être décrits de manière claire et détaillée dans la facture.
5. Inclure uniquement les frais courants pour la facture spécifique (n'incluez pas les soldes impayés d'autres factures en attente).
6. Les factures doivent être rédigées en anglais, y compris les pièces justificatives.

23 POLITIQUE D'ABSENCE OBLIGATOIRE

La Politique d'Absence Obligatoire de Citi impose aux personnes exerçant des fonctions sensibles ou à haut risque, en particulier celles ayant une incidence sur la comptabilité et les registres de l'entreprise, de se retirer périodiquement de ces fonctions. Cette séparation imposée vise à renforcer les contrôles internes en permettant de détecter d'éventuels cas de fraude, de vol ou d'autres fautes professionnelles qui, sans cela, pourraient passer inaperçus. Cette politique est conforme aux attentes prudentielles définies par le U.S. Federal Reserve Board concernant les absences obligatoires du personnel occupant des postes sensibles.

Tout le personnel des Fournisseurs ayant accès à des données sensibles dans le cadre de ses fonctions chez Citi **et** désigné comme personne « Sensible » doit se conformer aux exigences de la MA policy. Les personnes Sensibles sont tenues, chaque année, de planifier et d'effectuer intégralement une période d'absence obligatoire, en respectant l'ensemble des règles et restrictions prévues par la politique en vigueur. Pendant cette période, ils ne doivent ni mener, ni donner de consignes, ni autoriser, ni approuver aucune activité sensible, ni répondre de manière approfondie à aucune communication, y compris les échanges avec les clients, sauf pour rediriger les demandes de renseignements vers le service compétent. Si la période d'absence doit être interrompue après son début, les responsables ou les interlocuteurs professionnels de Citi doivent l'annuler dans les systèmes de conformité pour que l'accès au système soit rétabli. Le salarié devra ensuite programmer une nouvelle période d'absence.

ANNEXE - DÉFINITIONS

L'**Air – Gap** est une mesure de sécurité dans laquelle un ordinateur, un système ou un réseau est physiquement séparé des autres ordinateurs, systèmes ou réseaux. Une architecture de sauvegarde des données Air-Gap limite l'exposition à une cyberattaque et permet la restauration des données à un moment donné avant le début de l'attaque.

Le **Droit applicable** comprend : (a) les lois et règlements des États en matière de forclusion et (b) les règles, directives et autres communiqués publiés par diverses agences fédérales des États-Unis, notamment l'Office of the Comptroller of the Currency (parfois dénommés Red Flag Guidelines and Regulations) mettant en œuvre la section 114 du Fair and Accurate Credit Transactions Act de 2003

La **Zone de disponibilité** est l'endroit où le Fournisseur de services cloud dispose d'un groupe de centres de données logiques. Une Zone de disponibilité correspond à un ou plusieurs centres de données discrets avec une alimentation, une mise en réseau et des télécommunications redondantes dans une Région cloud.

L'**Intelligence artificielle (IA)** fait référence à une méthode, un système ou une approche quantitative (« techniques ») qui imite l'intelligence humaine via des programmes informatiques pour faire des estimations, des prédictions, des recommandations ou prendre des décisions d'une manière qui va au-delà des approches statistiques, mathématiques, économétriques ou financières classiques. Cela inclut toutes les catégories d'IA énumérées ci-dessous ainsi que les variations de l'IA, par exemple : IA générative, IA agentique, grands modèles de langage, modèles d'IA à usage général (GPAI), etc.

Les catégories d'IA incluent :

- o **IA statique** : Techniques d'IA formées manuellement hors ligne ou dont les paramètres sont explicitement programmés, puis utilisés pour faire des estimations, des prédictions, des recommandations ou prendre des décisions.
- o **IA dynamique** : Techniques qui, contrairement à « l'IA statique » peuvent réentraîner automatiquement les paramètres de manière périodique, en production.
- o **IA automatique** : Techniques d'« IA dynamique » qui sont en outre capables de modifier automatiquement leur structure de base (par exemple, hyperparamètres, variables d'entrée).
- o **IA cognitive** : Techniques qui peuvent prendre des décisions et agir de manière autonome en conséquence, même sur des questions pour lesquelles elles n'ont pas été spécifiquement formées.

L'**Apprentissage automatique (AA)** est le sous-ensemble d'une IA qui établit des représentations ou des déductions à partir de données sans programmation explicite de chaque paramètre de représentation ou étape informatique, par exemple les forêts aléatoires, les approches basées sur les réseaux neuronaux. À l'inverse, les techniques d'IA qui ne sont pas membres du sous-ensemble d'AA incluent des techniques telles que la logique floue, les techniques complexes d'analyse syntaxique pour le traitement du langage naturel.

Le **Business Activity Owner (BA)** est un employé de Citi responsable de l'exécution et de la gestion active de certaines activités associées aux relations avec le Fournisseur.

L'**Apporteur d'affaires** est un Fournisseur engagé par Citi à agir au nom de Citi pour identifier de nouvelles opportunités commerciales ou gérer les relations existantes avec les clients.

Un **cadeau d'entreprise** désigne tout article de valeur (autre que des divertissements professionnels) donné ou reçu par un employé de Citi dans le cadre de l'activité de Citi ou de l'activité de la partie externe, à l'exclusion généralement des articles évalués à 25 \$US ou moins.

Les **informations de Citi** sont des informations que Citi détient ou est tenu de protéger pendant le stockage, le traitement, la transmission ou l'élimination dans des formats numériques et non numériques.

Les classifications des Informations de Citi sont les suivantes :

Les Informations **Confidentielles** sont des Informations sur les unités d'activités de Citi et/ou les parties liées qui ne font pas référence à des personnes et qui nécessitent un niveau de protection élevé. Une atteinte à la confidentialité, à l'intégrité ou à la disponibilité de ces informations pourrait avoir un impact sérieux sur les opérations, le statut financier, la franchise ou les entreprises clientes de Citi.

Les **Informations Personnelles Identifiables (PII) Confidentielles** sont des informations personnelles sur une personne qui peuvent faciliter des activités illégales telles que l'usurpation d'identité, la fraude au crédit ou d'autres fraudes financières à l'encontre de ladite personne. Une atteinte à la confidentialité, à l'intégrité ou à la disponibilité de ces informations peut avoir un impact important sur la ou les personnes, y compris, entre autres, une perte financière ou une fraude.

- o Les éléments de données personnelles qui, lorsqu'ils sont combinés à d'autres données personnelles, constituent des PII Confidentielles comprennent le nom de la personne ou ses coordonnées (adresse, téléphone ou adresse e-mail) en combinaison avec :
 - Des éléments de données de transaction susceptibles d'entraîner des mouvements de fonds ou pouvant être utilisés pour commettre un vol d'identité ou une fraude, tels que :
 - Numéro de carte de crédit/débit.
 - Valeur de vérification de carte (CVV) ou PIN
 - Données du rapport de crédit (note de crédit)
 - Date de naissance complète
 - Performance des collaborateurs (appréciations/retours), ou informations sur la rémunération
 - Enregistrements vidéo, y compris les enregistrements de vidéosurveillance et des guichets automatiques
- Certains éléments de données personnelles prises isolément vont constituer des PII Confidentielles :
 - o Un numéro de sécurité sociale américain ou un numéro d'identification émis par un gouvernement (dont l'utilisation et/ou le statut de protection juridique sont équivalents au numéro de sécurité sociale américain), un numéro de passeport, un numéro de permis de conduire ou le numéro d'identification fiscale d'un particulier

Les **informations internes** sont des informations qui ne concernent pas une personne, sont destinées à des fins commerciales et nécessitent un niveau de protection modéré.

Une atteinte à la confidentialité, à l'intégrité ou à la disponibilité de ces informations pourrait avoir un **impact limité** sur une équipe ou un groupe de travail.

- o Les **Informations Personnelles Identifiables (PII)** sont des informations qui :
 - Identifient ou peuvent être utilisées pour identifier un individu ou un foyer (comme le nom, la signature, l'adresse, un identifiant national unique tel que le numéro de sécurité sociale, le numéro d'enregistrement de résident, la date de naissance, le numéro de permis de conduire).
 - Concernent, décrivent, peuvent être associées ou pourraient raisonnablement être associées (directement ou indirectement) à un individu ou un foyer.
 - Peuvent être utilisées pour authentifier un individu ou fournir l'accès à un compte (par exemple :
 - Un nom d'utilisateur, une adresse électronique, un mot de passe, un code PIN, un numéro d'identification, des réponses à des questions de sécurité) ; ou qui se rapportent à une personne et qui pourraient être sensibles (comme des informations médicales ou de santé personnelles, un numéro de compte, une valeur de compte).
 - Les Informations Personnelles comprennent aussi les données protégées concernant la santé (au sens de l'U.S. Health Insurance Portability and Accountability Act), les Informations Personnelles Sensibles et les informations relatives au crédit (telles que définies par les diverses législations sur la protection des données et sur le secret bancaire).

Les **informations publiques** désignent des Informations librement disponibles en dehors de Citi ou qui sont destinées à un usage public, comme les communiqués de presse de Citi ou les articles qui apparaissent dans les actualités à propos de Citi.

Les **informations restreintes** sont des informations dont l'utilisation est limitée à des personnes ou des groupes spécifiques et qui sont les plus sensibles pour Citi ou ses sociétés affiliées et à ce titre nécessitent le niveau de protection le plus élevé. Les atteintes à la confidentialité, à l'intégrité ou à la disponibilité de ces informations pourraient avoir un **impact considérable (à l'échelle de l'entreprise, de plusieurs zones géographiques, de plusieurs secteurs)** sur les opérations, le statut financier, la franchise ou les entreprises clientes de Citi.

- o Les **PII Sensibles** sont des Informations Personnelles qui, en vertu de lois spécifiques, nécessitent une protection supplémentaire et pourraient être utilisées pour faire preuve de discrimination illégale envers une personne ou lui causer du tort ou un traitement injuste. Une atteinte à la confidentialité, à l'intégrité ou à la disponibilité de ces informations pourrait avoir un impact important sur la personne (y compris, entre autres, une perte financière, une fraude ou un impact discriminatoire).
- Des données portant spécifiquement sur : la couleur de peau, la religion, les convictions religieuses ou philosophiques, l'appartenance ethnique, l'appartenance politique, l'appartenance syndicale, le casier judiciaire ou les informations sur les infractions pénales, les données génétiques, les données biométriques ou les données relatives à l'orientation ou l'activité sexuelle d'un individu.
- o Des informations personnelles sur la santé (PHI), comprenant des informations sur les antécédents médicaux ou l'état mental ou physique de la personne.

Le **Client** désigne tout client de Citi et pourra inclure des particuliers (c'est-à-dire, des personnes physiques) aussi bien que des entreprises, institutions, organisations et entités juridiques (personnes morales).

Une **Région cloud** est un emplacement physique où le Fournisseur de services cloud regroupe son ou ses centres de données.

Les **Équipements, systèmes et services de communication** sont les éléments matériels, logiciels ou les applications utilisés pour la transmission des communications électroniques écrites liées à l'activité de Citi. Les canaux de communications électroniques incluent, mais sans s'y limiter : les ordinateurs, les ordinateurs portables, les tablettes, les appareils mobiles ou les téléphones portables, y compris les appareils « Bring Your Own Device » (BYOD), les BlackBerry, les téléphones, les télécopieurs (services de fax), l'accès à l'Intranet et à Internet, les services Wi-Fi, les services de courrier électronique, les services de messagerie instantanée tels que Microsoft Lync, Skype et les messages Bloomberg, les sites Web et les applications avec des fonctions de communication intégrées, les plateformes de réunion ou de collaboration vidéo telles que Zoom ou Microsoft Teams, et les services de réseaux sociaux, les services de partage d'informations interactives, les salons de discussion de tiers, les tableaux d'affichage électroniques et les blogs.

Le **Contenu** désigne les Informations Confidentielles de Citi et les données, rapports, statistiques ou informations de toute nature (a) fournis ou mis à disposition directement ou indirectement au Fournisseur par ou pour le compte de Citi ou de ses Sociétés affiliées ou par ou pour le compte de ses ou de leurs clients ou prestataires de services, (b) créés, produits via les Services, ou (c) dérivés de l'un des éléments précédents.

Un **Contrat** désigne un document juridique signé par deux parties ou plus qui inclut une offre, une acceptation, une contrepartie, les obligations des parties et la légalité de l'objet. Les exemples de Contrats peuvent inclure des Accords-cadres portant sur des produits et services, des énoncés de travaux/bons de travail, des modifications ou des avenants, des échéanciers, des bons de commande ou tout autre document écrit signé par une entité de Citi et un Fournisseur. Un Accord de non-divulgence (NDA) est également considéré comme un Contrat aux fins de ces Normes

Un **test de Déni d'accès (DOA)** permet de vérifier que les effectifs et le soutien fournis par le Fournisseur pour les processus métier de Citi permettent une reprise dans le cadre du RTO défini.

Un **test de Déni de service (DOS)** permet de vérifier que l'application du Fournisseur et les composants de l'infrastructure sous-jacente prenant en charge les activités de Citi peuvent être restaurés dans le cadre du RTO défini.

« **Supports déposés** » désigne collectivement les sous-sections (i) à (vi) suivantes concernant, le cas échéant, les logiciels concédés sous licence à Citi en vue de leur exploitation au sein de l'environnement Citi ou les éléments utilisés par le Fournisseur dans le cadre des services hébergés fournis à Citi.

- (i) Une version exacte et en double du Code source du logiciel utilisé pour le développement, l'exploitation, la maintenance et le support du logiciel sous licence ou des services hébergés énoncés dans l'accord applicable avec Citi (et toutes les versions ultérieures de ce logiciel ou de ces services hébergés), et toute la

- documentation pour ce logiciel (qu'il soit ou non possible que Citi dispose d'une copie de certaines parties de ce Code source) (« **Dépôt de code source** ») ;
- (ii) Le Code source de tout logiciel tiers dont le Fournisseur détient les droits en matière de développement, d'exploitation, de maintenance et d'assistance du logiciel sous licence ou des services hébergés ;
 - (iii) Une copie autorisée de tous les outils logiciels, tels que les débogueurs, les assembleurs et les compilateurs nécessaires pour convertir le code source inclus dans les supports déposés en un format exécutable, tel que nécessaire pour exploiter, maintenir et prendre en charge le logiciel ou les services hébergés ;
 - (iv) Dans la mesure où cela n'a pas déjà été prévu ci-dessus, toute documentation qui fournit ce qui suit : (A) descriptions générales et utilisations de supports déposés ; (B) architecture et fonctions de base du programme ; (C) informations sur le flux de données ; (D) carte mémoire détaillée et listings ; (E) cartes des ports d'entrée/sortie ; et (F) tout autre détail permettant à un programmeur ayant des compétences normales dans le ou les langages de programmation applicables d'utiliser et de modifier le Code source inclus dans les Supports déposés ;
 - (v) Toutes les autres informations techniques liées aux logiciels ou aux services hébergés qui seraient raisonnablement requises pour permettre à Citi, ou à un tiers compétent pour le compte de Citi, d'utiliser, d'exploiter, de modifier et d'améliorer les logiciels ou les services hébergés ; et
 - (vi) Une liste de tous les logiciels et technologies tiers utilisés en relation avec les logiciels ou les services hébergés, y compris des détails raisonnables concernant leur utilisation dans le logiciel et les coordonnées du Fournisseur de ces logiciels ou technologies. Citi reconnaît et accepte que les supports déposés ne contiennent pas de code source provenant de tiers autre que celui indiqué au paragraphe (ii) ; et
 - (vii) en ce qui concerne les services hébergés :
 - a. une réplique à échelle réduite de l'environnement de production hébergé dans le cloud ou des éléments spécifiques à cet environnement liés au cloud, ainsi que toute autre information nécessaire à la reproduction de l'environnement de production de Citi, y compris (sans s'y limiter) : l'infrastructure telle que le code, les scripts Terraform, les ressources cloud, les modèles CloudFormation, les fichiers de configuration, les locataires cloud, les abonnements cloud, les images de machine, les images Docker et l'infrastructure sous forme de code source du logiciel ; et
 - b. une copie des données de Citi stockées dans le logiciel.

Les **communications électroniques** sont des messages ou des informations envoyés, reçus ou utilisés par le personnel à l'aide de moyens électroniques, transmis par des signaux filaires ou sans fil. Les communications électroniques comprennent, sans s'y limiter, les messages texte, les e-mails, les messages pair à pair ou instantanés, les publications sur blog, les publications sur les réseaux sociaux, les messages envoyés par le biais d'applications de messagerie telles que WhatsApp, WeChat, Line, Signal ou Viber, et comprennent des pièces jointes, des captures d'écran, des fichiers vocaux ou vidéo enregistrés, vocaux ou vidéo en direct, et des fichiers créés, reçus, téléchargés, stockés, transmis, supprimés ou utilisés via l'équipement, les systèmes et les services de communications électroniques.

Les **identifiants fonctionnels** représentent un identifiant générique, tel que ADMIN ou ROOT, utilisé par une personne ou un processus pour accéder à un système de sécurité. Une initiative essentielle dans le processus Identity and Access Management (IAM) consiste à s'assurer que

Citi dispose des contrôles spécifiques définis en vue de la protection contre les risques associés à l'utilisation d'Identifiants fonctionnels.

Les **processus/applications critiques pour la franchise (FCA)** sont ceux identifiés par Citi comme essentiels à la réussite de l'exécution de ses fonctions commerciales critiques pour la franchise.

La **Fraude** est un acte intentionnel, une fausse déclaration ou une omission visant à tromper autrui, entraînant soit une perte pour la victime, soit un bénéfice pour l'auteur.

Les **Services hébergés** incluent toute application installée, ainsi que toute installation et tout environnement géré ou utilisé par le Fournisseur pour fournir les services hébergés, toutes les applications et autres logiciels, bases de données, sites Web, serveurs, matériel, réseaux, télécommunications et autres équipements, et toute autre technologie installée ou utilisée dans l'environnement des services hébergés, et, dans chaque cas, toutes les mises à jour et tous les services de soutien, mais à l'exclusion de tous les contenus et des systèmes de Citi.

Les **Identity Verification Data (IVD)** sont définies comme des questions de sécurité (SQ) ou des questions d'authentification basée sur les connaissances (KBA). Les questions de sécurité sont généralement définies par l'application et c'est l'utilisateur final qui y répond. On peut citer comme exemples le nom de jeune fille de la mère, le lieu de naissance, le parfum de glace préféré, etc. Ces deux types de questions doivent être traités comme des données d'authentification.

L'**Information Security** ou « **IS** » désigne l'état dans lequel un ordinateur ou un système informatique est protégé contre un accès ou une attaque non autorisé, et en raison de cet état : a) l'ordinateur ou le système informatique continue d'être disponible et opérationnel ; b) l'intégrité de l'ordinateur ou du système informatique est maintenue ; et c) l'intégrité et la confidentialité des informations stockées, traitées ou transmises par l'ordinateur ou le système informatique sont conservées.

Une **Menace IS** désigne un acte ou une activité (connu(e) ou présumé(e)) commis(e) sur ou via un ordinateur ou un système informatique, susceptible de compromettre ou d'affecter de manière négative la sécurité des informations de cet ordinateur ou d'un autre ordinateur ou système.

Une **Vulnérabilité IS** désigne toute vulnérabilité dans un ordinateur ou un système informatique pouvant être exploitée par une ou plusieurs menaces IS.

Le terme « **non-client** »/« **ne générant pas de revenu** » est défini comme une activité critique pour l'entreprise qui n'est pas associée aux activités génératrices de revenus, notamment les activités juridiques, de supervision, réglementaires et de continuité des activités.

Un **Accord de non-divulgence (NDA)** est un accord entre Citi et un Fournisseur selon lequel l'échange, l'utilisation et la divulgation d'informations sont régies par les conditions de l'accord.

Un **Logiciel open source** désigne du code source ou un programme informatique compilé dans lequel le code source est mis à disposition du grand public et dont la conception initiale peut être utilisée ou modifiée par celui-ci.

Le **Personnel** désigne, que cela soit déclaré directement ou déduit du contexte, le Fournisseur et ses sociétés affiliées, administrateurs, dirigeants, employés, agents, auditeurs, consultants, prestataires de services et sous-traitants (à l'exclusion du personnel de Citi). Le personnel du

Fournisseur comprend également les administrateurs, dirigeants, employés, agents, auditeurs, consultants ou autres représentants de tout Sous-traitant.*

L'**Inventaire des enregistrements** est une liste détaillée qui comprend les types d'enregistrement, l'emplacement, les dates, etc., des enregistrements de Citi et qui est nécessaire pour qu'une entreprise gère correctement ses dossiers tout au long du cycle de vie des informations.

Une **Mesure de conservation des informations** désigne l'obligation juridique de surseoir à la modification ou à la destruction de Documents ou d'Informations jusqu'à ce que cette obligation soit levée par l'autorité ayant ordonné le sursis.

La **Capacité de reprise** correspond au volume, à la quantité ou à la vitesse de livraison des produits et services du Fournisseur, exprimé en pourcentage de la livraison normale de produits et de services.

La **Durée de récupération** est le temps maximal, en jours civils, pendant lequel le Fournisseur est capable de maintenir les opérations en mode de récupération.

La **Perte de données maximale admissible (RPO ou PDMA)** est le moment dans le passé, indiqué en heures, auquel les données doivent être récupérées après une interruption de l'activité. Il s'agit de la période maximale visée au cours de laquelle des données pourraient être perdues dans un service informatique en raison d'un incident majeur. Le RPO n'est qu'une mesure de la période maximale pendant laquelle les données pourraient être perdues s'il y avait un incident majeur affectant un service informatique. Il ne s'agit pas d'une mesure directe du volume de données qui pourraient être perdues, par exemple, jusqu'à la fin du traitement du jour précédent.

La **Durée maximale d'interruption admissible (RTO ou DMIA)** désigne la durée en heures entre le moment où un service est interrompu et la restauration des produits et services.

« **Événement de déliement** » désigne l'un ou plusieurs des éléments suivants :

- (i) Le Fournisseur (A) devient insolvable ou reconnaît son incapacité à régler ses dettes de manière générale à leur échéance ; (B) fait l'objet, volontairement ou non, de toute procédure relevant du droit national ou étranger en matière de faillite ou d'insolvabilité, laquelle n'est pas intégralement suspendue dans un délai de sept (7) jours ouvrables ou n'est pas rejetée ou annulée dans un délai de quarante-cinq (45) jours suivant son dépôt ; (C) procède à une cession générale au bénéfice de ses créanciers ; ou (D) voit la désignation, par ordonnance d'un tribunal compétent, d'un administrateur judiciaire, fiduciaire, séquestre ou autre mandataire similaire, chargé de prendre le contrôle ou de procéder à la vente d'une partie substantielle de ses biens ou de son activité.

La **Resource Management Organization (RMO)** est responsable de la gestion globale des ressources de bout en bout pour Citi, y compris l'approvisionnement stratégique, les opérations d'achat et de paiement, le bureau de dotation en personnel et le cadre de gestion des Fournisseurs.

Le **RMO Sourcing Manager** désigne un individu intervenant au sein de la Resource Management Organization (RMO), en charge de la négociation des conditions économiques, des obligations et des tarifs des Contrats, y compris les demandes de proposition, ainsi que de la sélection des Fournisseurs, de l'administration au regard des conditions des Contrats et des exigences d'accréditation relatives aux évaluations financières.

Un **Effet néfaste grave ou catastrophique** sur une personne signifie que l'impact pourrait raisonnablement entraîner des effets négatifs importants, notamment une perte financière, une perte d'emploi ou la difficulté à obtenir un emploi, la perte de jouissance d'un droit humain, une humiliation personnelle ou publique ou un emprisonnement injustifié.

Sous-traitant : Un sous-traitant est une quatrième partie (personne ou entité), qui a été engagée par un tiers pour effectuer une partie ou la totalité des services ou activités que Citi a confiés au tiers dans le cadre d'un contrat.

Conseils :

Q1 : Tous les sous-traitants du Tiers doivent-ils être déclarés ?

R1 : Seuls les sous-traitants liés au service effectué doivent être déclarés. Exemples de services ou d'activités effectués par un sous-traitant, entre autres :

*Un sous-traitant effectuant des services technologiques ou logiciels qui soutiennent directement ou indirectement le service/les activités que Citi a confiés au Tiers ; ou

*Un sous-traitant dont les services incluent l'accès à des Informations de Citi classées Confidentielles ou de niveau supérieur ; ou

*Un sous-traitant qui a une interaction directe ou indirecte avec tout Client Citi existant/potentiel ; ou

*Un sous-traitant qui n'a pas besoin d'être escorté et qui effectue des services de déchiquetage ou d'archivage de documents de Citi dans ou en dehors de tout local de Citi ; ou

*Un sous-traitant soutenant des fonctions ou services bancaires clés tels que les paiements, l'encaissement, l'octroi de prêts, etc.

Fournisseurs : Aux fins du présent document intitulé « Exigences de Citi envers ses Fournisseurs », le terme « Fournisseur » désigne exclusivement un tiers externe qui a conclu un accord commercial afin de fournir des produits ou des services directement à une entité Citi ou d'aider une entité Citi à atteindre ses objectifs commerciaux. Un tiers externe est défini comme une entité ne relevant pas de Citi. Les Fournisseurs peuvent également être des clients d'une entité Citi ou faciliter les interactions avec les clients de Citi ; toutefois, les accords fondés exclusivement sur leur statut de client de Citi ne sont pas considérés comme des relations de « fournisseur » au sens du présent document.

Informations transitoires : Un dossier désigne la version définitive la plus complète des informations que Citi est tenu de conserver pour des raisons commerciales légales, réglementaires ou approuvées. Toutes les autres informations sont classées comme des « Informations transitoires ».