QUESTIONNAIRE POUR L'ORGANISATION TIERS QUI LIT, TRAITE, ENREGISTRE, COMMUNIQUE DES INFORMATIONS DES INSTITUTIONS PUBLIQUES DE LA SÉCURITÉ SOCIALE OU QUI FOURNIT DES ÉLÉMENTS D'INFRASTRUCTURE & DES SERVICES TIC

Nom de l'organisation (tiers)	Dénomination: ..... Adresse : .... Numéro d'entreprise (BCE) 0 | | | | | | | | | |
Prénom, nom et courriel du conseiller en sécurité (CISO) (obligatoire)	....
Prénom, nom et courriel du conseiller en sécurité adjoint (CISO adjoint) (obligatoire)	....
Prénom, nom et courriel du délégué à la protection des données (DPO) (obligatoire)	....
Prénom, nom et courriel du délégué à la protection des données adjoint (DPO adjoint) (obligatoire)	....
Prénom, nom et courriel de la personne chargée de la gestion journalière de l'organisation (tiers) (obligatoire)	.....

	.....

Question	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
1	Disposez vous d'une politique de sécurité de l'information formelle et actualisée, approuvée par le responsable de la gestion journalière?	☐ OUI ☐ NON	
2	Disposez vous d'une évaluation des risques pour tout processus et tout projet relatif à la sécurité de l'information et à la vie privée que vous utilisez pour la prestation de service?	☐ OUI ☐ NON	
3	L'organisation a-t-elle, en son sein: • organisé un service de sécurité placé sous la direction d'un conseiller en sécurité? • organisé un service chargé de la sécurité de l'information placé sous l'autorité fonctionnelle directe du responsable de la gestion journalière de l'organisation?	☐ OUI ☐ NON ☐ OUI ☐ NON	
4	Disposez vous d'un plan de sécurité de l'information approuvé par le responsable de la gestion journalière?	☐ OUI ☐ NON	
5	Combien d'heures ont été prestées par le conseiller en sécurité et son (ses) adjoint(s) éventuel(s) pour l'exécution des tâches de sécurité? 1) conseiller en sécurité 2) conseiller(s) en sécurité adjoint(s) Combien d'heures de formation relative à la sécurité de l'information le conseiller en sécurité et son (ses) adjoint(s) ont-ils suivi pendant l'année? 1) conseiller en sécurité 2) conseiller(s) en sécurité adjoint(s)	1) heures / mois 2) heures / mois 3) heures / année 4) heures / année	
6	Disposez vous de procédures pour le développement de nouveaux systèmes ou d'évolutions importantes dans les systèmes existants, de sorte que le responsable de projet puisse tenir compte des exigences de sécurité décrites dans les normes minimales?	☐ OUI ☐ NON ☐ N/A	
7	Avez-vous pris les mesures adéquates afin que les données sensibles, confidentielles et professionnelles enregistrées sur des médias mobiles ne soient accessibles qu'aux seules personnes autorisées?	☐ OUI ☐ NON	

Question	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
8	Avez-vous pris les mesures adéquates, en fonction du moyen d'accès, afin de garantir la sécurité de l'information de l'accès en ligne réalisé en dehors de votre organisation aux données sensibles, confidentielles et professionnelles?	☐ OUI ☐ NON	
9	Avez-vous organisé les dispositifs de télétravail de la sorte que sur le lieu du télétravail (à domicile, dans un bureau satellite ou à un autre endroit) aucune information ne soit enregistrée sur des appareils externes sans chiffrement et qu'aucune menace potentielle ne puisse atteindre l'infrastructure IT au départ du lieu de télétravail?	☐ OUI ☐ NON	
10	Est-ce que vous sensibilisez annuellement tous vos collaborateurs à la sécurité de l'information et à la vie privée et est-ce que vous réalisez annuellement une évaluation du respect de cette politique dans la pratique?	☐ OUI ☐ NON	
11	Avez-vous sécurisé l'accès par un dispositif d'accès précis et avez vous implémenté un système d'accès (physique ou logique) afin d'éviter tout accès non autorisé?	☐ OUI ☐ NON	
12	Disposez vous d'un schéma de classification interne pour laquelle vous fournissez des services et est-ce que vous appliquez les règles supplémentaires en fonction du schéma de classification?	☐ OUI ☐ NON	
13	Avez-vous intégré les règles dans une politique relative à la sécurité de l'information et à la vie privée qui sont spécifiées dans la ligne directrice « E-mail, communication en ligne et utilisation d'internet »?	☐ OUI ☐ NON	
14	Avez vous désigné au moins un gestionnaire des accès lorsque vous utilisez les services et applications du portail de la sécurité sociale pour les besoins de vos utilisateurs?	☐ OUI ☐ NON	
15	Avez vous stimulé vos collaborateurs à lire et à appliquer les règlements relatifs à l'utilisation des systèmes d'information des portails?	☐ OUI ☐ NON	
16	Lorsque vous souhaitez appliquer la « cryptographie »: • disposez vous d'une politique formelle pour l'utilisation de contrôles cryptographiques? • disposez vous d'une politique formelle pour l'utilisation, la protection et la durée de vie des clés cryptographiques pour le cycle de vie complet?	☐ OUI ☐ NON ☐ OUI ☐ NON	
17	Avez-vous pris les mesures nécessaires permettant de limiter l'accès aux bâtiments et locaux aux personnes autorisées et est-ce que vous effectuez des contrôle à ce sujet tant pendant qu'en dehors des heures de travail?	☐ OUI ☐ NON	

Question	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
18	Avez-vous pris les mesures de prévention nécessaires contre la perte, l'endommagement, le vol ou la compromission des actifs et contre l'interruption des activités?	☐ OUI ☐ NON	
19	En cas de réutilisation du support d'information, est-ce que vous réutilisez celui-ci dans un niveau de classification des données au moins comparable?	☐ OUI ☐ NON	
20	Avez-vous déterminé les mesures appropriées pour la suppression de données dans un contrat avec le mandant ?	☐ OUI ☐ NON	
21	Est-ce que vous appliquez les règles relatives à la journalisation des accès telles que fixées par le mandant?	☐ OUI ☐ NON	
22	Est-ce qu'il y a une communication constructive dans chaque projet d'acquisition, de développement ou de maintenance de systèmes entre les différentes parties concernées par le projet et le(s) conseiller(s) en sécurité?	☐ OUI ☐ NON	
23	L'ensemble de vos collaborateurs travaillent-ils avec des moyens TIC sur la base d'une autorisation minimale pour l'exécution de leurs tâches?	☐ OUI ☐ NON	
24	Les conditions de protection des accès (identification, authentification, autorisation) ont-elles été définies, documentées, validées et communiquées? Ces accès font-ils l'objet d'une prise de traces?	☐ OUI ☐ NON ☐ OUI ☐ NON	
25	Les risques relatifs à la sécurité et à la vie privée sont-ils fixés dans un contrat entre vous et le mandant et des clauses de confidentialité et de continuité sont-elles prévues?	☐ OUI ☐ NON	
26	Est-ce que vous utilisez une liste de contrôle pour le chef de projet de sorte que ce dernier puisse s'assurer que l'ensemble des directives relatives à la sécurité de l'information et à la vie privée sont correctement évaluées et sont, si nécessaire, mises en œuvre durant la phase de développement du projet?	☐ OUI ☐ NON	
27	Assurez vous lors de la mise en production du projet, que les conditions relatives à la sécurité et à la vie privée qui ont été fixées au début du projet sont effectivement mises en œuvre?	☐ OUI ☐ NON	
28	Les dispositifs de développement, de test et/ou d'acceptation, et de production sont-ils scindés sous la supervision du chef de projet et le partage des responsabilités qui en découle est-il réalisé dans le cadre du projet?	☐ OUI ☐ NON	
29	Tout accès à des données personnelles et confidentielles à caractère social ou médical fait-il l'objet d'une prise de traces, conformément à la politique « journalisation » et à la législation et à la réglementation applicables?	☐ OUI ☐ NON	

Question	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
30	Est-il précisé dans les spécifications d'un projet comment l'accès et l'utilisation des systèmes et des applications seront journalisés, afin de contribuer à la détection d'anomalies par rapport aux directives relatives à la sécurité de l'information et à la vie privée?	☐ OUI ☐ NON	
31	La journalisation satisfait-elle au moins aux objectifs suivants? • les informations permettant de déterminer qui a obtenu accès à quelles informations, à quel moment et de quelle manière • l'identification de la nature des informations consultées • l'identification précise de la personne	☐ OUI ☐ NON	
32	Les outils nécessaires sont-ils disponibles pour que les données de journalisation puissent être exploitées par les personnes autorisées?	☐ OUI ☐ NON	
33	Les données de journalisation fonctionnelles/transactionnelles sont-elles conservées pendant 10 ans au moins et les données de journalisation techniques/infrastructurelles pendant 2 ans au moins?	☐ OUI ☐ NON	
34	Les délivrables du projet (données traitées, la documentation (code source, programmes, documents techniques, ...)) sont-ils intégrés dans le système de gestion des sauvegardes comme imposé dans les politiques?	☐ OUI ☐ NON	
35	Au cours du développement du projet, les besoins relatifs à la continuité de la prestation de services sont-ils formalisés conformément à vos attentes?	☐ OUI ☐ NON	
36	Vos plans de continuité et vos procédures y afférentes, en ce compris les tests de continuité, sont-ils actualisés en fonction de l'évolution du projet?	☐ OUI ☐ NON	
37	Une analyse des risques est-elle réalisée au début du projet afin de définir les procédures d'urgence?	☐ OUI ☐ NON	
38	Les procédures relatives à la gestion des incidents sont-elles formalisées et validées au cours du développement d'un projet?	☐ OUI ☐ NON	
39	Le conseiller en sécurité est-il informé des incidents relatifs à la sécurité et à la vie privée?	☐ OUI ☐ NON	
40	La documentation (technique, procédures, manuels, ...) est-elle actualisée au cours de la durée de vie du projet?	☐ OUI ☐ NON	
41	Tous les actifs, en ce compris les systèmes acquis ou développés, sont-ils ajoutés au système de gestion des moyens opérationnels (inventaire)?	☐ OUI ☐ NON	
42	La collaboration appropriée pour l'audit est-elle apportée sous la forme de mise à la disposition du personnel, de la documentation, de la gestion des traces et des autres informations qui sont raisonnablement disponibles?	☐ OUI ☐ NON	

Question	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
43	Les conditions relatives à la sécurité de l'information et à la vie privée sont-elles documentées afin de réduire les risques relatifs à l'accès aux moyens d'information?	☐ OUI ☐ NON	
45	Toutes les conditions pertinentes relatives à la sécurité de l'information et à la vie privée sont-elles définies et font-elles l'objet d'un accord entre vous et les tiers / sous-traitants (qui lisent, traitent, enregistrent, communiquent les informations de l'organisation ou fournissent des éléments d'infrastructure TIC et des services TIC)?	☐ OUI ☐ NON	
46	Est-ce que vous effectuez régulièrement un monitoring, une évaluation et un audit de la prestation de service du tiers / du sous-traitant?	☐ OUI ☐ NON	
47	Les adaptations de la prestation de service sont-elles gérées par le tiers / sous-traitant, dont notamment l'actualisation des directives, procédures et mesures relatives à la sécurité de l'information et à la vie privée existantes?	☐ OUI ☐ NON	
48	Lorsque vous faites appel aux services d'un cloud, est-ce que vous êtes en conformité avec le point 2.1 de la politique « Cloud Computing »?	☐ OUI ☐ NON	
49	Lorsque vous souhaitez traiter des données sensibles, confidentielles ou professionnelles dans un cloud, est-ce que vous satisfait aux garanties contractuelles minimales et aux directives telles que décrites au point 2.2, 2.3 et 2.4 de la politique « Cloud computing »?	☐ OUI ☐ NON	
50	Disposez vous de procédures pour la détermination et la gestion d'incidents relatifs à la sécurité de l'information ou à la vie privée et des responsabilités y afférentes et est-ce que vous communiquez les procédures à vos collaborateurs?	☐ OUI ☐ NON	
51	Est-ce que vous avez signé un contrat avec les collaborateurs dans lequel il est stipulé que tous les collaborateurs (fixe ou temporaire, interne ou externe) sont obligés de signaler tout accès, utilisation, modification, publication, perte ou destruction non autorisés d'informations et de systèmes d'information?	☐ OUI ☐ NON	
52	Les événements et failles relatifs à la sécurité de l'information ou à la vie privée en rapport avec les informations et les systèmes d'information de l'organisation sont-ils communiqués à vous de sorte que vous pouvez prendre, en temps utile, des mesures correctrices adéquates?	☐ OUI ☐ NON	
53	Les incidents relatifs à la sécurité de l'information et à la vie privée sont-ils rapportés, dans les meilleurs délais, à l'intervention du supérieur hiérarchique, du helpdesk, du conseiller en sécurité de l'information (CISO) ou du délégué à la protection des données (DPO)?	☐ OUI ☐ NON	
54	En cas d'incidents relatifs à la sécurité de l'information ou à la vie privée, les preuves sont-elles collectées conformément aux prescriptions réglementaires et légales?	☐ OUI ☐ NON	

Question	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
55	Tout incident relatif à la sécurité de l'information et à la vie privée est-il validé de manière formelle, de sorte que les procédures et mesures de contrôle puissent être améliorées? Les leçons tirées d'un incident sont-elles communiquées à votre direction, en vue de la validation et de l'approbation d'actions futures?	☐ OUI ☐ NON	
56	Existe-t-il un plan de continuité pour l'ensemble des processus critiques et systèmes d'information essentiels?	☐ OUI ☐ NON	
57	La sécurité de l'information et la vie privée font-elles partie intégrante de la gestion de la continuité?	☐ OUI ☐ NON	
58	Est-ce que vous avez mis au point un plan de continuité contenant les informations minimales telles que décrites dans la directive « gestion de la continuité »? Est-ce que votre plan est-il régulièrement testé et adapté et fait-il l'objet de la communication utile à votre direction en vue de sa validation et de son approbation?	☐ OUI ☐ NON ☐ OUI ☐ NON	
59	Est-ce que vous réalisez périodiquement un audit de conformité de la situation relative à la sécurité de l'information et à la vie privée telle que décrite dans les directives?	☐ OUI ☐ NON	
60	Disposez vous d'une procédure disciplinaire formelle pour les travailleurs ayant commis une infraction à la sécurité de l'information ou à la vie privée?	☐ OUI ☐ NON	
61	Est-ce que vous rassemblez régulièrement les données pour construire la carte des risques relatifs à la conformité au Règlement Européen et est-ce que vous exécutez les actions nécessaires suite à un risque résiduel majeur de non-conformité?	☐ OUI ☐ NON	
62	Disposez vous des registres centraux nécessaires et mis à jour du responsable du traitement ou du sous-traitant et possèdez vous une justification formelle de la non-réalisation des mesures de contrôle axées sur le respect du Règlement Européen pour le traitement (ou groupe de traitements) spécifique(s)?	☐ OUI ☐ NON	

Veuillez renvoyer le questionnaire complété au Service Sécurité de l'information et Audit interne de la Banque Carrefour de la sécurité sociale.

Date et signature du conseiller en sécurité (CISO) ou du délégué à la protection des données (DPO) de l'organisation (tiers) (facultatif)	..... Date Signature
Date et signature de la personne chargée de la gestion journalière de l'organisation (tiers) **(obligatoire)**	..... Date Signature

***** FIN DU DOCUMENT *****