QUESTIONNAIRE 2018 POUR L'ÉVALUATION DES NORMES MINIMALES:

ANNÉE CONTRÔLÉE 2017

Nom de l'institution (obligatoire)	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) (facultatif)	....
Prénom, nom et courriel du délégué à la protection des données (DPO) (facultatif)	....
Prénom, nom et courriel du délégué à la protection des données adjoint (DPO) (facultatif)	....
Prénom, nom et courriel de la personne chargée de la gestion journalière de l'institution (obligatoire)	....

Les normes minimales de sécurité publiées sur le site de la Banque Carrefour de la sécurité sociale s'appliquent en premier lieu aux institutions de sécurité sociale, visées à l'article 2, alinéa 1er, 2° de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*. Au fil du temps, le législateur a agrandi le champ d'application du réseau de la Banque Carrefour au travers de l'application de l'article 18 de cette dite loi. En plus des institutions de sécurité sociale, vient s'ajouter toute organisation ayant reçu un accord du Comité sectoriel de la sécurité sociale et de la santé pour l'accès, l'utilisation, et la fourniture de données sociales.
Afin de simplifier la lecture de ce document, le terme « organisation » couvre l'ensemble du champ d'application des normes minimales de sécurité tel que décrit dans le paragraphe précédent.

Les organisations doivent obligatoirement respecter ces normes minimales de sécurité si elles souhaitent accéder et maintenir l'accès au réseau de la Banque Carrefour. Les normes ont donc une valeur contraignante. Le contrôle du respect des normes est réalisé à partir d'un questionnaire qui est transmis par l'intermédiaire de la Banque Carrefour au Comité sectoriel de la sécurité sociale et de la santé pour évaluation. Il appartient à l'organisation de le remplir dûment et de veiller au respect des dites normes. Le comité sectoriel de la sécurité sociale et de la santé peut, le cas échéant, (faire) réaliser des contrôles sur place afin d'évaluer sur le terrain le respect de ces normes minimales de sécurité.

Ce questionnaire a pour **but** d'évaluer et de déterminer si les normes de sécurité en vigueur au sein de l'organisation sont en ligne avec les objectifs des normes minimales de sécurité, tout en tenant compte de leur situation spécifique et de l'importance des moyens de fonctionnement à protéger.

La mise en œuvre et le contrôle des normes minimales de sécurité auprès de tiers qui traitent[1] des données sociales à caractère personnel pour le compte d'une organisation, incombent en premier lieu à l'organisation qui a confié les travaux au tiers. (Art. 16 de la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel)

Les réponses sont évaluées par le Comité sectoriel de la sécurité sociale et de la santé.

[1] Par "traitement", on entend toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion.

Norme	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
5.1	**Principes de base**		
5.1.1	L'organisation a-t-elle intégré les principes clés dans sa sécurité de l'information?	☐ OUI ☐ NON	
5.2	**Politique de sécurité de l'information**		
5.2.1	L'organisation dispose-t-elle d'une politique de sécurité de l'information formelle et actualisée, approuvée par le responsable de la gestion journalière?	☐ OUI ☐ NON	
5.2.2a	L'organisation dispose-t-elle d'un processus d'évaluation des risques (utilisé dans le cadre des projets et des processus) qui tient compte de la sécurité de l'information et de la vie privée?	☐ OUI ☐ NON	
5.2.2b	L'organisation a-t-elle communiqué toutes les évaluations de risques contenant un risque résiduel majeur à la direction?	☐ OUI ☐ NON	
5.2.2c	L'organisation applique-t-elle pour son évaluation des risques les principes énumérés dans la « directive relative à l'évaluation des risques » (annexe C de la politique **«** Evaluation des risques »)?	☐ OUI ☐ NON	
5.3	**Organisation de la sécurité de l'information**		
5.3.1.1	L'organisation réalise-t-elle les activités obligatoires (si d'application) avant, pendant et lors de la cessation ou modification du contrat de travail telles que décrites dans les normes minimales 5.3.1.1?	☐ OUI ☐ NON	
5.3.1.2a	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? • confié l'organisation de la sécurité de l'information à un service de sécurité spécialisé agréé?	☐ OUI ☐ NON ☐ OUI ☐ NON ☐ OUI ☐ NON	
5.3.1.2b	L'organisation a-t-elle communiqué l'identité de son conseiller en sécurité et de ses adjoints éventuels au Comité sectoriel de la sécurité sociale et de la santé ou, en ce qui concerne les institutions du réseau secondaire, à son institution responsable de ce réseau?	☐ OUI ☐ NON	

Norme	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
5.3.1.2c	L'organisation dispose-t-elle d'un plan de sécurité de l'information approuvé par le responsable de la gestion journalière?	☐ OUI ☐ NON	
5.3.1.2d	L'organisation connectée au réseau de la Banque Carrefour dispose-t-elle des crédits de fonctionnement nécessaires, approuvés par le responsable de l'organisation concernée, en vue de l'exécution de son plan de sécurité et de l'exécution par le service de sécurité des tâches qui lui ont été confiées?	☐ OUI ☐ NON	
5.3.1.2e	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	
5.3.1.2f	L'organisation dispose-t-elle de procédures pour la communication d'informations au conseiller en sécurité de sorte qu'il dispose des données lui permettant d'exécuter la mission de sécurité qui lui a été confiée?	☐ OUI ☐ NON	
5.3.1.3	L'organisation dispose-t-elle d'une plateforme de décision pour valider et approuver les mesures de sécurité?	☐ OUI ☐ NON	
5.3.1.4	L'organisation gérant un « réseau secondaire » échange-t-elle au moins une fois par semestre des informations pertinentes avec son réseau secondaire en organisant une réunion du sous-groupe de travail « Sécurité de l'information » pour les organisations qui font partie de son réseau? Dans l'affirmative, veuillez noter dans la colonne de droite à côté de OUI - NON - N/A les dates des réunions organisées durant l'année auditée?	☐ OUI ☐ NON ☐ N/A	
5.3.1.5	L'organisation connectée au réseau de la Banque Carrefour dispose-t-elle 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 relatives à la sécurité de l'information et à la vie privée?	☐ OUI ☐ NON ☐ N/A	
	(sous-groupe 'Organisation de la sécurité de l'information')		

Norme	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
5.3.2.1a	L'organisation prend-elle les mesures adéquates afin que les données sensibles, confidentielles et professionnelles enregistrées sur des médias mobiles (tant médias qu'appareils d'enregistrement mobiles) ne soient accessibles qu'aux seules personnes autorisées?	☐ OUI ☐ NON	
5.3.2.1b	L'organisation prend-elle 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 l'organisation aux données sensibles, confidentielles et professionnelles de l'organisation?	☐ OUI ☐ NON	
5.3.2.1c	L'organisation impose-t-elle les conditions qui sont détaillées dans la politique « appareils mobiles » lors de l'utilisation d'appareils privés à des fins professionnelles?	☐ OUI ☐ NON	
5.3.2.1d	L'organisation impose-t-elle les règles qui sont détaillées dans la politique « appareils mobiles » lors de l'utilisation d'appareils mobiles à des fins professionnelles et à des fins privées?	☐ OUI ☐ NON	
5.3.2.1e	L'organisation dispose-t-elle d'un registre central contenant l'identification de ses appareils mobiles[2] et configure-t-elle la sécurité utile pour ces appareils (et les équipe-t-elle des logiciels antimalware nécessaires ainsi que des logiciels permettant la suppression à distance de l'ensemble des données sur l'appareil)?	☐ OUI ☐ NON	
5.3.2.1f	L'organisation prévoit-elle les contrôles appropriés afin de vérifier la conformité des appareils mobiles à la politique relative à la sécurité de l'information et à la vie privée (à distance au moyen d'un logiciel ou sur place au moyen d'un contrôle direct)?	☐ OUI ☐ NON	
5.3.2.1g	L'organisation sensibilise-t-elle régulièrement les utilisateurs concernant les bonnes pratiques d'utilisation et leurs responsabilités (en particulier en ce qui concerne la connexion à des réseaux sans fil publics)?	☐ OUI ☐ NON	
5.3.2.1h	La possibilité de bloquer directement l'accès aux informations de l'organisation (données ou applications présentes sur l'appareil mobile) et d'effacer des données existe-t-elle?	☐ OUI ☐ NON	
5.3.2.1i	L'organisation s'engage-t-elle à respecter la vie privée de l'utilisateur?	☐ OUI ☐ NON	
5.3.2.2a	L'organisation a-t-elle pris les mesures adéquates, en fonction du moyen d'accès[3], afin de garantir la sécurité de l'information de l'accès en ligne réalisé en dehors de l'organisation aux données sensibles, confidentielles et professionnelles de l'organisation?	☐ OUI ☐ NON	

[2] Appareils mobiles : voir BLD Mobile pour la description

3 Moyen d'accès: p.ex. Internet, ligne louée, réseau privé, réseau sans fil.

Norme	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
5.3.2.2b	L'organisation a-t-elle clairement mis au point des règles de bonne conduite ainsi qu'une mise en œuvre appropriée du télétravail, les a-t-elle validées, communiquées et tenues à jour? L'organisation doit aussi préciser quels systèmes peuvent et quels systèmes ne peuvent pas être consultés au départ du lieu de travail à domicile ou d'autres appareils?	☐ OUI ☐ NON	
5.3.2.2c	L'organisation a-t-elle organisé les dispositifs de télétravail de l'organisation de la sorte que sur le lieu du télétravail (à domicile, dans un bureau satellite ou à un autre endroit) aucune information relative à l'organisation ne soit enregistrée sur des appareils externes sans chiffrement et qu'aucune menace potentielle ne puisse atteindre l'infrastructure IT de l'institution au départ du lieu de télétravail?	☐ OUI ☐ NON	
5.4	**Sécurité liée aux collaborateurs (Clean desk & Clear desk)**		
5.4.1	L'organisation sensibilise-t-elle annuellement tout collaborateur à la sécurité de l'information et à la vie privée et réalise-t-elle annuellement une évaluation du respect de cette politique dans la pratique (au moyen d'une enquête interne)?	☐ OUI ☐ NON	
5.4.2a	L'organisation dispose-t-elle une politique indiquant que la collaboration de l'ensemble des collaborateurs est essentielle pour la sécurité de l'information et la vie privée?	☐ OUI ☐ NON	
5.4.2b	L'organisation dispose-t-elle une politique indiquant que l'utilisateur demeure responsable des informations, quelle que soit la forme sous laquelle ces informations sont enregistrées?	☐ OUI ☐ NON	
5.4.2c	L'organisation a-t-elle sécurisé l'accès par un dispositif d'accès précis et a-t-elle implémenté un système d'accès (physique ou logique) afin d'éviter tout accès non autorisé à l'organisation?	☐ OUI ☐ NON	
5.5	**Gestion des actifs**		
5.5.1a	L'organisation dispose-t-elle d'un schéma de classification interne qui est conforme à la législation spécifique en la matière et à la réglementation internationale éventuelle?	☐ OUI ☐ NON	
5.5.1b	L'organisation dispose-t-elle de procédures appropriées et de registres en vue de la labellisation (étiquetage) des traitements de l'ensemble des collectes de données, supports de données et systèmes d'information en cours de gestion, et ce conformément au schéma de classification interne?	☐ OUI ☐ NON	
5.5.1c	L'organisation dispose-t-elle et applique-t-elle la règle selon laquelle la classification qui est définie par le type d'information vaut également pour le niveau supérieur des systèmes d'information?	☐ OUI ☐ NON	

Norme	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
5.5.1d	Les classifications de tous les systèmes critiques sont-elles définies à un niveau central par leurs propriétaires?	☐ OUI ☐ NON	
5.5.1e	Les classifications de tous les systèmes critiques sont-elles contrôlées annuellement par le conseiller en sécurité de l'information (CISO) et/ou le délégué à la protection des données (DPO)?	☐ OUI ☐ NON	
5.5.1f	Les mesures de contrôle sont-elles conformes aux risques? Dans ce cadre, il y a lieu de tenir compte des possibilités techniques et du coût des mesures à prendre?	☐ OUI ☐ NON	
5.5.2	L'organisation dispose-t-elle d'un inventaire du matériel informatique et des logiciels actualisé en permanence?	☐ OUI ☐ NON	
5.5.4a	L'organisation a-t-elle intégré dans sa politique relative à la sécurité de l'information et à la vie privée les règles qui sont spécifiées à l'annexe C de la politique « E-mail, communication en ligne et utilisation d'internet »?	☐ OUI ☐ NON	
5.5.4b	L'organisation exerce-t-elle en permanence un contrôle sur l'e-mail, la communication en ligne et l'utilisation d'internet dans le cadre des objectifs suivants: • la protection de la réputation et des intérêts de l'organisation; • la prévention de faits illicites ou de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ; • la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'organisation, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'organisation ; • le respect des principes clés?	☐ OUI ☐ NON	
5.5.5	L'organisation a-t-elle pris les mesures nécessaires pour protéger, contre les accès non autorisés, les supports en transit, notamment les backups contenant des données sensibles?	☐ OUI ☐ NON	
5.6	**Protection de l'accès (logique)**		
5.6.1a	L'organisation a-t-elle désigné au moins un gestionnaire des accès lorsqu'elle utilise les services et applications du portail de la sécurité sociale pour les besoins de ses utilisateurs?	☐ OUI ☐ NON	
5.6.1b	L'organisation a-t-elle stimulé ses collaborateurs à lire et à appliquer les règlements relatifs à l'utilisation des systèmes d'information des portails?	☐ OUI ☐ NON	
5.6.1c	Lorsque l'organisation utilise les services et applications du portail de la sécurité sociale pour les besoins de ses utilisateurs, respecte-t-elle les obligations liées à l'exercice de la fonction de gestionnaire ou de co-gestionnaire qui sont décrites dans la politique « gestion des accès aux portails »?	☐ OUI ☐ NON	

Norme	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
5.6.2	Lorsque l'organisation souhaite utiliser l'internet comme moyen d'accès au réseau de la Banque Carrefour de la sécurité sociale (BCSS): • dispose-t-elle d'une autorisation et dérogation écrites du fonctionnaire dirigeant de la BCSS? • a-t-elle appliqué strictement les conditions énumérées à l'annexe D (Conditions d'accès à l'Extranet de la sécurité sociale via internet) de la politique?	☐ OUI ☐ NON ☐ OUI ☐ NON	
5.6.3	L'organisation a-t-elle sécurisé l'accès aux données nécessaires à l'application et à l'exécution de la sécurité sociale par un système d'identification, d'authentification et d'autorisation?	☐ OUI ☐ NON	
5.6.4	L'organisation dispose-t-elle des autorisations nécessaires du comité sectoriel compétent pour l'accès aux données (sociales) à caractère personnel gérées par une autre organisation?	☐ OUI ☐ NON	
5.6.5	L'organisation a-t-elle limité l'accès au(x) système(s) informatique(s) aux gestionnaires d'information identifiés, authentifiés et autorisés?	☐ OUI ☐ NON	
5.6.6	L'organisation a-t-elle pris les mesures adéquates afin que toute personne ait uniquement accès aux services pour lesquels elle a spécifiquement reçu une autorisation?	☐ OUI ☐ NON	
5.6.7	L'organisation utilise-t-elle l'Extranet de la sécurité sociale pour l'ensemble de ses connexions externes ou pour les connexions avec son réseau secondaire? Toute dérogation à cette mesure fait-elle l'objet d'une demande motivée introduite par l'intermédiaire du service de sécurité de la BCSS?	☐ OUI ☐ NON ☐ OUI ☐ NON	
5.7	**Chiffrement**		
5.7.1	Lorsque l'organisation souhaite appliquer la « cryptographie »: • dispose-t-elle d'une politique formelle pour l'utilisation de contrôles cryptographiques? • dispose-t-elle 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	
5.8	**Protection physique et protection de l'environnement**		
5.8.1	L'organisation prend-elle les mesures nécessaires permettant de limiter l'accès aux bâtiments et locaux aux personnes autorisées et effectue-t-elle un contrôle à ce sujet tant pendant qu'en dehors des heures de travail?	☐ OUI ☐ NON	
5.8.2	L'organisation prend-elle des mesures de prévention contre la perte, l'endommagement, le vol ou la compromission des actifs de l'entreprise et contre l'interruption des activités de l'entreprise?	☐ OUI ☐ NON	

Norme	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
5.8.3a	L'organisation prend-elle les mesures nécessaires en cas d'utilisation du chiffrement comme mesure de base préventive contre le vol, l'abus ou la perte du support d'information?	☐ OUI ☐ NON	
5.8.3b	En cas de réutilisation du support d'information, l'organisation réutilise-t-elle celui-ci dans un niveau de classification des données au moins comparable?	☐ OUI ☐ NON	
5.8.3c	L'organisation réalise-t-elle une évaluation des risques, afin de déterminer la méthode appropriée pour la suppression du support d'information?	☐ OUI ☐ NON	
5.8.3d	L'organisation détruit-elle physiquement le support d'information lorsqu'il existe un risque résiduel de retrouver des données consécutivement à la suppression qui n'est pas acceptable pour l'organisation?	☐ OUI ☐ NON ☐ N/A	
5.8.3e	L'organisation détermine-t-elle contractuellement les mesures appropriées pour la suppression de données lorsque: • l'organisation utilise des supports de données qui ne sont pas sa propriété (par exemple, dans le cadre du leasing ou du disaster recovery)? • l'organisation ne maîtrise pas la technologie d'accès à l'ensemble des niveaux du support d'information (par exemple, dans le cadre du cloud computing)?	☐ OUI ☐ NON ☐ N/A ☐ OUI ☐ NON ☐ N/A	
5.9	**Gestion opérationnelle**		
5.9.1	L'organisation s'est-elle assurée qu'aucun développement ou test n'a lieu au sein de l'environnement de production?	☐ OUI ☐ NON	
5.9.2	L'organisation dispose-t-elle de procédures pour la mise en production de nouvelles applications et la réalisation d'adaptations aux applications existantes? L'organisation a-t-elle pris les mesures nécessaires permettant d'éviter qu'une seule et même personne n'assure le contrôle de l'ensemble de ce processus?	☐ OUI ☐ NON ☐ OUI ☐ NON	
5.9.3	L'organisation dispose-t-elle de systèmes actualisés pour se protéger (prévention, détection et rétablissement) contre des codes nocifs?	☐ OUI ☐ NON	
5.9.4	L'organisation a-t-elle défini la politique et la stratégie organisant la mise en œuvre d'un système de sauvegarde en phase avec la gestion de la continuité? L'organisation a-t-elle régulièrement contrôlé les sauvegardes réalisées dans ce cadre?	☐ OUI ☐ NON ☐ OUI ☐ NON	

Norme	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
5.9.6	L'organisation (participant à la transmission de données au travers de la Banque Carrefour) est-elle en mesure d'assurer à son niveau la traçabilité des identifiants utilisés?	☐ OUI ☐ NON	
5.9.7	L'organisation a-t-elle installé un système et des procédures formelles et actualisées permettant la détection, le suivi et la réparation d'infractions au niveau de la sécurité proportionnellement au risque technique / opérationnel?	☐ OUI ☐ NON	
	(Sous-groupe 'Gestion opérationnelle')		

5.9.5	En ce qui concerne le logging des accès:
	• l'organisation dispose-t-elle d'une procédure de gestion des logs formelle?
	• l'organisation définit-elle, de manière structurée, dans des fichiers logs individuels, les transactions, les travaux de contrôle, les activités des utilisateurs, les exceptions et les événements liés à la sécurité de l'information et à la vie privée?
	• la gestion des logs est-elle prévue dès le début, dans le design lors du développement ou lors de la détermination des critères d'achat de systèmes ou d'applications, afin de réaliser un « security/privacy by design »?
	• tout accès à des données personnelles et confidentielles à caractère social ou médical fait-il l'objet d'une prise de logs, conformément à la législation et à la réglementation applicables?
	• les horloges internes de l'ensemble des systèmes d'information de l'organisation sont-elles synchronisées avec une source temporelle précise et déterminée, de sorte qu'une analyse fiable des fichiers logs sur les différents systèmes d'information soit toujours possible?
	• les outils nécessaires sont-ils disponibles ou développés que sorte que les données de logs puissent être analysées par les personnes autorisées?
	• l'utilisation du système fait-il l'objet d'une prise de logs?
	  ○ de manière automatique?
	  ○ ou en ayant recours à un journal manuel?
	• les fichiers logs sont-ils protégés contre toute consultation par des personnes non autorisées, toute modification ou toute suppression?
	• les fichiers logs sont-ils conservés pendant une période convenue, pour les investigations et contrôles futurs et ce en conformité avec la législation et la réglementation?
		☐ OUI ☐ NON
		☐ OUI ☐ NON
		☐ OUI ☐ NON
		☐ OUI ☐ NON
		☐ OUI ☐ NON
		☐ OUI ☐ NON
		☐ OUI ☐ NON
		☐ OUI ☐ NON	

Norme	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
	• existe-t-il une procédure organisée au sein de l'organisation qui tient à jour un historique des demandées approuvées/exécutées ou refusées pour la consultation des fichiers logs? • le résultat de la gestion des logs est-il analysé, rapporté et évalué à des intervalles réguliers?	☐ OUI ☐ NON ☐ OUI ☐ NON	
5.10	**Sécurité de communication**		
5.10.1a	L'organisation dispose-t-elle, pour l'ensemble des réseaux sans fil qu'elle a sous sa gestion et à tous les endroits, d'un processus permettant de mettre à jour un aperçu de l'ensemble des réseaux sans fil existants et autorisés, des protocoles de sécurité y afférents et de l'ensemble des mesures de sécurité de l'information y associées?	☐ OUI ☐ NON	
5.10.1b	L'organisation respecte-t-elle les directives qui sont décrites dans l'annexe C de la politique « réseaux sans fil sécurisés »?	☐ OUI ☐ NON	
5.10.2	L'organisation vérifie-t-elle que les réseaux sont gérés et contrôlés de manière adéquate afin de les protéger contre les menaces?	☐ OUI ☐ NON	
5.10.3	L'organisation a-t-elle mis en place les mesures techniques nécessaires, suffisantes, efficientes et adéquates en vue de garantir la plus haute disponibilité de connexion avec le réseau de la Banque Carrefour et ce afin d'assurer une accessibilité maximale aux données tant mises à disposition que consultées?	☐ OUI ☐ NON	
5.10.4	L'organisation dispose-t-elle d'une cartographie actualisée des flux techniques[4] mis en œuvre au travers de l'Extranet de la sécurité sociale?	☐ OUI ☐ NON	
5.10.5	L'organisation traite-t-elle toute transmission de données sociales au sein du réseau de la sécurité sociale dans les meilleurs délais, notamment en communiquant toute dérogation ou lacune dans la transmission électronique?	☐ OUI ☐ NON	
5.11	**Achat, conception, développement et maintenance d'applications**		
5.11.1	Tout projet d'acquisition, de développement ou de maintenance de systèmes a-t-il fait l'objet d'une communication constructive ente les différentes parties concernées par le projet et le(s) conseiller(s) en sécurité?	☐ OUI ☐ NON	
5.11.2a	L'ensemble des collaborateurs travaillent-ils avec des moyens TIC (mis à la disposition par l'organisation) sur la base d'une autorisation minimale pour l'exécution de leurs tâches?	☐ OUI ☐ NON	

4 Les flux techniques au niveau du réseau sont nécessaires à la gestion des firewalls dans les différentes zones de l'Extranet.

Norme	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
5.11.2b	Lors du développement des protections d'accès a-t-il été tenu compte des systèmes opérationnels actuels de gestion des accès (tels qu'UAM) et de leur évolution?	☐ OUI ☐ NON	
5.11.2c	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	
5.11.2e	L'organisation établit-elle la relation entre le numéro de programme et l'identité de la personne physique qui envoie le message lorsqu'un programme est développé dans lequel l'institution de sécurité sociale reprend un numéro de programme dans un message qu'elle adresse à la BCSS, bien qu'une personne physique soit à l'origine de ce message?	☐ OUI ☐ NON	
5.11.2d	A-t-on évité autant que possible la gestion des accès au niveau interne dans une application ?	☐ OUI ☐ NON	
	(Sous-groupe 'Achat, conception, développement et maintenance d'applications')		
5.11.3	Lors de la sous-traitance à des tiers, les conditions relatives à la sécurité et à la vie privée sont-elles fixées contractuellement et des clauses de confidentialité et de continuité sont-elles prévues?	☐ OUI ☐ NON	
5.11.4	L'organisation utilise-t-elle 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	
5.11.5	L'organisation s'assure-t-elle, 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? Les conditions de sécurité ont notamment trait à la confidentialité, à l'intégrité et à la disponibilité.	☐ OUI ☐ NON	
5.11.6	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 dans le cadre du projet qui en découle est-il réalisé?	☐ OUI ☐ NON	
5.11.7b1	Est-il précisé dans les spécifications d'un projet comment l'accès et l'utilisation des systèmes et des applications seront journalisés (« loggés »), 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	

Norme	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
5.11.7b2	La journalisation (le « logging ») satisfait-elle au cours d'un projet 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	
5.11.7c	A-t-on tenu compte des systèmes de gestion des logs actuels lors de l'évaluation des besoins de logs dans le cadre du présent projet?	☐ OUI ☐ NON	
5.11.7e	Les « privacy logs » sont-ils conservés pendant 10 ans au moins?	☐ OUI ☐ NON	
	(Sous-groupe 'Achat, conception, développement et maintenance d'applications')		
5.11.8	Les délivrables du projet (code source, programmes, documents techniques, ...) sont-ils intégrés dans le système de gestion des sauvegardes comme imposé dans les politiques?	☐ OUI ☐ NON	
5.11.9a	Au cours du développement du projet, les besoins relatifs à la continuité de la prestation de services sont-ils formalisés conformément aux attentes de l'organisation?	☐ OUI ☐ NON	
5.11.9b	Dans les systèmes logiciels, les points de reprise à définir afin de faire face à des problèmes opérationnels sont-ils clairement intégrés? Les informations relatives aux points de reprise font partie du dossier d'exploitation.	☐ OUI ☐ NON	
5.11.9c	Au cours du développement d'un projet, une attention spécifique est-elle accordée à une sauvegarde et à une restauration (« restore ») des informations?	☐ OUI ☐ NON	
5.11.9d	Dans l'environnement de production, est-il tenu compte des exigences de l'organisation en ce qui concerne la tolérance aux problèmes et la redondance de l'infrastructure?	☐ OUI ☐ NON	
5.11.9e	Le plan de continuité et les procédures y afférentes, en ce compris les tests de continuité, sont-ils actualisés en fonction de l'évolution du projet?	☐ OUI ☐ NON	
5.11.9f	Une analyse des risques est-elle réalisée au début du projet afin de définir les procédures d'urgence?	☐ OUI ☐ NON	
5.11.10a	Les procédures relatives à la gestion des incidents sont-elles formalisées et validées au cours du développement d'un projet?	☐ OUI ☐ NON	
5.11.10b	Le conseiller en sécurité est-il informé des incidents relatifs à la sécurité de l'information et à la vie privée au cours du développement d'un projet?	☐ OUI ☐ NON	

Norme	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
5.11.11	La documentation (technique, procédures, manuels, ...) est-elle actualisée au cours de la durée de vie du projet?	☐ OUI ☐ NON	
5.11.12	Tous les actifs, en ce compris les systèmes acquis ou développés, sont-ils ajoutés au système de gestion des moyens opérationnels (inventaire)?	☐ OUI ☐ NON	
5.11.13	La collaboration appropriée à des fins d'audit interne et externe 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	
5.11.14	Les aspects du « secure project lifecycle » sont-ils appliqués ? Pour plus d'informations, voir l'annexe C de la politique « Achat, conception, développement et maintenance d'applications »?	☐ OUI ☐ NON	
5.12	**Relations avec les fournisseurs**		
5.12.1a	Les obligations en matière de traitement de données à caractère personnel sont-elles fixées dans un contrat lorsque l'organisation sous-traite du travail à un fournisseur?	☐ OUI ☐ NON	
5.12.1b	Les conditions relatives à la sécurité de l'information et à la vie privée font-elles l'objet d'un accord avec les tiers et sont-elles documentées afin de réduire les risques relatifs à l'accès des tiers aux informations?	☐ OUI ☐ NON	
5.12.1c	Les fournisseurs (auxquels le travail est sous-traité et qui lisent, traitent, enregistrent, communiquent des informations de l'organisation ou qui fournissent des éléments d'infrastructure TIC) ont-ils répondu à toutes les questions du questionnaire « normes minimales fournisseurs »?	☐ OUI ☐ NON	
5.12.1d	Les contrats conclus avec les tiers (fournisseurs) comprennent-ils toutes les conditions permettant de traiter les risques liés à la sécurité de l'information et à la vie privée qui sont afférents aux services TIC?	☐ OUI ☐ NON	
5.12.1e	L'organisation effectue-t-elle régulièrement un monitoring de la prestation de service de tiers et évalue et audite-t-elle cette prestation de service?	☐ OUI ☐ NON	
5.12.1f	Les adaptations de la prestation de service sont-elles gérées par des tiers ? Par adaptations, on entend notamment l'actualisation et l'amélioration des politiques, procédures et mesures relatives à la sécurité de l'information et à la vie privée existantes?	☐ OUI ☐ NON	
5.12.1g	Les « directives relatives à la sécurité de la sous-traitance à des tiers » sont-elles appliquées telles que décrites dans l'annexe C de la politique « sécurité de la sous-traitance à des tiers »?	☐ OUI ☐ NON	

Norme	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
5.12.2a	Lorsque l'organisation fait appel aux services d'un cloud, le fait-elle en conformité avec les dispositions décrites au point 2.1 de la politique « Cloud computing »?	☐ OUI ☐ NON	
5.12.2b	Lorsque l'organisation souhaite traiter des données sensibles, confidentielles ou professionnelles dans un cloud, satisfait-elle 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	
5.13	**Gestion des incidents relatifs à la sécurité de l'information**		
5.13.1a	L'organisation dispose-t-elle 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 a-t-elle communiquées ces procédures à ses collaborateurs?	☐ OUI ☐ NON	
5.13.1b	L'organisation a-t-elle signé un contrat avec les collaborateurs dans lequel il est stipulé que tout collaborateur (fixe ou temporaire, interne ou externe) est obligé de signaler tout accès, utilisation, modification, publication, perte ou destruction non autorisés d'informations et de systèmes d'information?	☐ OUI ☐ NON	
5.13.1c	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 sont-ils rendus publics, de sorte que l'organisation puisse prendre, en temps utile, des mesures correctrices adéquates?	☐ OUI ☐ NON	
5.13.1d	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) et ce conformément aux procédures de gestion des incidents?	☐ OUI ☐ NON	
5.13.1e	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 (notamment la réglementation RGPD)?	☐ OUI ☐ NON	
5.13.1f	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 la direction de l'organisation, en vue de la validation et de l'approbation d'actions futures?	☐ OUI ☐ NON	
5.13.1g	La « directive relative à la gestion des incidents » est-elle appliquée telle que décrite dans l'annexe C de la politique « Gestion des incidents »?	☐ OUI ☐ NON	

Norme	*cochez (X) la case qui correspond à votre réponse*		Expliquez si la réponse est « non »
5.14	**Aspects de la sécurité de l'information dans la gestion de la continuité**		
5.14.1a	Existe-t-il un plan de continuité pour l'ensemble des processus critiques et systèmes d'information essentiels de l'organisation?	☐ OUI ☐ NON	
5.14.1b	La sécurité de l'information et la vie privée font-elles partie intégrante de la gestion de la continuité?	☐ OUI ☐ NON	
5.14.1c	L'organisation a-t-elle mis au point un plan de continuité contenant les informations minimales telles que décrites dans la politique « gestion de la continuité »?	☐ OUI ☐ NON	
5.14.1e	Le plan de continuité est-il régulièrement testé et adapté et fait-il l'objet de la communication utile à la direction en vue de sa validation et de son approbation?	☐ OUI ☐ NON	
5.15	**Respect**		
5.15.1a	L'organisation réalise-t-elle 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 politiques?	☐ OUI ☐ NON	
5.15.1d	L'organisation dispose-t-elle 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	
5.15.1e	La « directive relative au respect » telle que décrite dans l'annexe C de la politique « Gestion des incidents » est-elle appliquée?	☐ OUI ☐ NON	
5.15.2a	L'organisation dresse-t-elle régulièrement la carte des risques relatifs à la conformité au Règlement européen et exécute-t-elle les actions devenues nécessaires suite à un risque résiduel majeur de non-conformité?	☐ OUI ☐ NON	
5.15.2b	L'organisation dispose-t-elle des registres centraux nécessaires et mis à jour du responsable du traitement ou du sous-traitant et possède-t-elle 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 pour **le 20 mai 2018** au plus tard au Service Sécurité de l'information et Audit interne de la Banque Carrefour de la sécurité sociale.

Modalité à respecter par les institutions du réseau secondaire:
Les institutions du réseau secondaire remettent le questionnaire complété à l'institution de tutelle qui transmet les listes reçues au Service Sécurité de l'information et Audit interne de la Banque Carrefour pour la date mentionnée ci-dessus.

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

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