



FORMULAIRE I : LISTE DE VÉRIFICATION SUR LA SITUATION EN MATIÈRE DE CYBERSÉCURITÉ

À remplir par le ou les services de TI de la ou des organisations du demandeur.

F. ORGANIZATION'S CURRENT CYBERSECURITY STRUCTURE		
Pour les demandes impliquant plusieurs partenaires, veuillez remplir une liste de vérification par organisation. Remplissez toutes les sections de la manière la plus précise et la plus complète possible.		
LA PERSONNE QUI REMPLIT CETTE LISTE DE VÉRIFICATION		
NOM:	TITRE	COURRIEL:
_____	_____	_____

QUESTIONNAIRE SUR LA CYBERSÉCURITÉ		
MESURES DE CYBERSÉCURITÉ	ÉTAT	
Parmi les mesures suivantes, lesquelles sont en place dans votre organisation :		
<ul style="list-style-type: none">a. Réseau privé virtuel (RPV) pour les employés qui travaillent à distanceb. Pare-feu fiable, système de détection et de prévention des intrusions, antivirus, anti-maliciels et logiciel de gestion des menaces liées aux appareils mobiles pour détecter et supprimer les virus, les maliciels, les logiciels de publicité et les logiciels espionsc. Protocole de gestion des courriels malveillants, de la messagerie instantanée et des messages textesd. Nettoyage à distance des ordinateurs portatifs et des téléphones intelligentse. Modèle à vérification systématiquef. Segmentation du réseau pour mettre en œuvre des contrôles et des services propres à chaque sous-réseaug. Système de gestion des informations et des événements de sécurité permettant de surveiller et de suivre en permanence toutes les activités du réseau pour l'ensemble des utilisateurs, des appareils et des applicationsh. Plan d'intervention en cas d'incident pour récupérer rapidement et rétablir les fonctions essentiellesi. Processus de détection et d'atténuation des menaces internes		
VÉRIFICATIONS, PLANIFICATION ET MESURES DE PROTECTION DES SYSTÈMES	ÉTAT	
<ul style="list-style-type: none">1. Votre organisation suit-elle un ensemble de règles et de procédures de cybersécurité dans le cadre de ses activités, en vue de protéger son personnel, ses biens, ses PI et ses données sensibles, et de garantir la confidentialité, l'intégrité et la disponibilité de ses systèmes?2. Votre organisation utilise-t-elle un outil de prise de décision automatisée pour mettre en œuvre ses protocoles de gouvernance, de droits et de confidentialité des données?3. Votre organisation a-t-elle mis en place un mécanisme de contrôle d'accès solide pour contrôler et surveiller les privilèges d'accès des utilisateurs?		



FORMULAIRE I : LISTE DE VÉRIFICATION SUR LA SITUATION EN MATIÈRE DE CYBERSÉCURITÉ

À remplir par le ou les services de TI de la ou des organisations du demandeur.

4. Votre organisation utilise-t-elle régulièrement des outils et des contrôles de vérification pour déceler les enjeux et les problèmes?
5. Votre organisation applique-t-elle des mises à niveau et des correctifs automatiques aux micrologiciels, au matériel, aux logiciels et aux systèmes d'exploitation?
6. Votre organisation impose-t-elle l'authentification multifacteur (AMF) pour les comptes et les systèmes?
7. Votre organisation classe-t-elle ses biens par catégories afin d'identifier ceux qui sont les plus importants pour ses fonctions opérationnelles?
8. Votre organisation examine-t-elle régulièrement la position de ses fournisseurs tiers et des membres de sa chaîne d'approvisionnement en matière de cybersécurité (services infonuagiques et services clés externalisés pour s'assurer que des mesures de sécurité appropriées sont en place)?
9. Votre organisation a-t-elle adopté un système de secours bien pensé?
10. Votre organisation informe-t-elle ses employés sur les meilleures pratiques en matière de cybersécurité et leur donne-t-elle des conseils dans ce domaine?
11. Votre organisation organise-t-elle régulièrement des formations de sensibilisation à la sécurité à l'intention des employés et du personnel tiers affecté aux projets?
12. Votre organisation a-t-elle mis en place un plan de reprise bien conçu en cas d'interruption ou de violation, en particulier pour les biens indispensables?
13. En ce qui concerne la conformité, votre organisation veille-t-elle à ce que tous les biens soient configurés de manière à optimiser leur sécurité et conformément aux pratiques exemplaires de l'industrie?
14. Ce projet de recherche implique-t-il l'utilisation de données personnelles pouvant être de nature sensible?

BIENS INFORMATIQUES

1. Veuillez dresser la liste des biens de TI du projet.
 - a. Veuillez dresser la liste des biens matériels du projet (ordinateurs, serveurs, appareils mobiles) et des mesures mises en place dans votre organisation pour les sécuriser. Par exemple, les mesures pourraient inclure un contrôle de l'accès physique, des pare-feux, des systèmes de détection d'intrusions sur réseau, des systèmes de détection d'intrusion au niveau des hôtes et des systèmes de gestion des informations et des événements de sécurité.

