Questionnaire d'évaluation à la maturité en gestion de crise cyber

Guide d'utilisation

Le présent questionnaire est fondé sur le guide publié par l'ANSSI en partenariat avec le CDSE en décembre 2021, intitulé *Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique*.

Conditions d'évaluation

Afin de remplir le questionnaire dans les meilleures conditions, nous vous recommandons de procéder à son déroulé lors d'ateliers avec les parties prenantes impliquées dans les processus de gestion de crise cyber de votre organisation, tant du point de vue stratégique qu'opérationnel (ex. RSSI, membres de la cellule stratégique, SOC, équipes techniques etc.).

Pour chaque question, vérifiez si vous possédez des preuves attestant de votre réponse et n'hésitez pas à vous servir de la colonne « Commentaires » pour procéder à d'éventuels renvois.

Nous vous recommandons de réserver au moins 3 heures pour la complétion du questionnaire afin de vous assurer de la justesse des notes que vous vous attribuez.

Ce questionnaire reprend l'essentiel des recommandations du guide sous la forme de questions, auxquelles sont attachées quatre niveaux de maturité. Ces questions ont été regroupées en cinq thématiques générales :

- Gouvernance et interactions entre équipes mobilisées
- Processus et outillage
- Communication de crise et relations externes
- Détection et réponse à incidents
- Continuité d'activité et reconstruction

Ce questionnaire est composé de 3 onglets :

- **Onglet « Questionnaire d'évaluation »**

Dans cet onglet, l'utilisateur du questionnaire auto-évalue la maturité de son organisation. Pour l'aider dans sa notation, 4 niveaux de maturité (0-1-2-3) ont été définis et exemplifiés d'activités et/ou d'outils attendus à chacun de ces niveaux.

L'utilisateur s'attribue une note entière allant de 0 à 3 dans la colonne « Note » de la feuille, à l'aide de la colonne « Preuves » qui indique les documents pouvant justifier la réponse. La colonne « Commentaire » pourra servir à justifier les notes auto-évaluées en cas de relecture.

- **Onglet « Résultat global »**

Les notes sont consolidées et arrondies au dixième le plus proche dans la feuille « Résultat global ». Vous retrouvez :

- Une note globale, reprenant la moyenne de l'ensemble des notes attribuées par l'utilisateur pour toutes les questions ;
- Une note détaillée pour les différentes temporalités de la crise (en préparation et en réaction) ;
- Une note détaillée pour les 5 thématiques définis plus haut ;
- Une note détaillée pour chaque fiche du guide avec une appréciation selon la note.
- **Onglet « Recommandations »**

La feuille « Recommandations » reprend la note attribuée sur chaque question par l'utilisateur et propose les actions du niveau de maturité supérieur afin de donner des pistes d'amélioration. Pour certaines questions, vous trouverez des ressources supplémentaires pour vous accompagner dans la colonne « Outils / Accélérateurs », qui vous redirige vers des guides thématiques.

L'évaluation que vous allez réaliser vous permettra d'identifier les forces et points d'amélioration de vos processus de gestion de crise et d'avoir une vision directe et concrète des actions que vous pouvez mettre en place pour vous permettre de mieux vous préparer à l'éventualité d'une crise cyber.

Abréviations pertinentes		
Sigle FR	**Sigle EN**	**Signification**
AND	NDA	Accord de non-divulgation
ANSSI	/	Agence nationale de la sécurité des systèmes d'information
/	AD	Active Directory
BDGC	CMDB	Base de données de gestion de configuration
CNIL	/	Commission nationale de l'informatique et des libertés
/	CTI	Connaissance de la menace cyber (*Cyber Threat Intelligence)*
DMIA	RTO	Durée maximum d'interruption d'activité
/	DNS	Systèmes de noms de domaines
GDC	CM	Gestion de crise
IGC	PKI	Infrastructures de gestion des clés
PDMA	RPO	Perte de données maximale admissible
PCA	BCP	Plan de continuité d'activité
PRA	DRP	Plan de reprise d'activité
/	RACI	Matrice "Responsible, Accountable, Consulted, Informed"
RETEX	/	Retour d'expérience
RH	HR	Ressources humaines
RSSI	CISO	Responsable de la Sécurité des Systèmes d'Information
TAMT	MTD	Temps d'arrêt maximal tolérable
SI	IS	Système d'information
TI	IT	Technologies de l'information
TRD	WRT	Temps de récupération des données