



**RÉPUBLIQUE  
FRANÇAISE**

*Liberté  
Égalité  
Fraternité*



# **EXERCICE DE CRISE CYBER JOP 2024**

## **Guide d'utilisation du pack documentaire**



# SOMMAIRE

1

OBJECTIFS DU PACK  
DOCUMENTAIRE

---

2

DÉMARCHE – ÉTAPES PAR ÉTAPES

---

3

TUTORIEL D'ORGANISATION D'UN  
EXERCICE DANS LE CADRE DES  
JOP2024

---



# 1. OBJECTIFS DU PACK



Sensibiliser à la gestion de crise  
cyber



Fournir une marche à suivre pour organiser un  
exercice



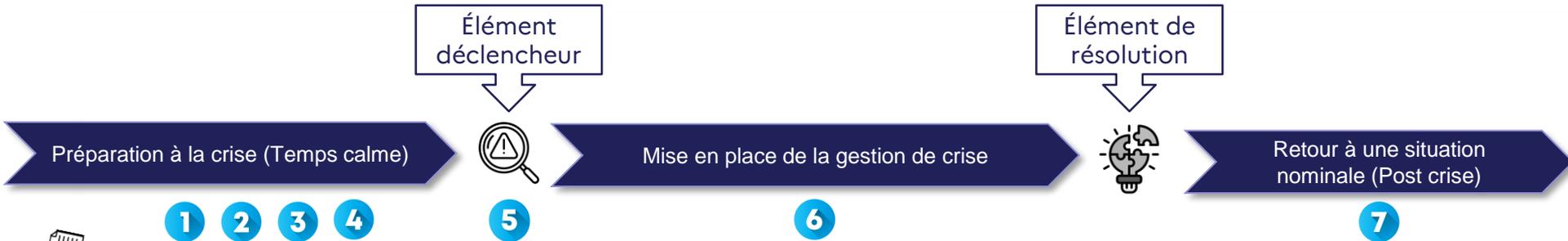
Répondre aux questions que l'organisation d'un exercice pourraient  
susciter



Fournir des modèles qu'il ne reste plus qu'à  
adapter



## 2. MARCHE A SUIVRE



Documents Supports



### Guides méthodologiques :

- Support de présentation des enjeux, des objectifs et la méthodologie
- Organisation-type de cellules de crise
- Cahier des charges



### Modèles à adapter :

- Chronogramme
- Support de briefing des joueurs
- Annuaire des joueurs
- Annuaire des animateurs



### Guides méthodologiques :

- Méthodologie d'observation



### Modèles à adapter :

- Main courante
- Grille d'observation



### Guides méthodologiques :

- Méthodologie de RETEX à chaud
- Méthodologie de RETEX à froid



### Modèles à adapter :

- Support de RETEX à chaud
- Support de RETEX à froid
- Questionnaire de RETEX à froid



# 3. TUTORIEL D'ORGANISATION D'EXERCICE

## ÉTAPE 1

Cette étape vous permettra de prendre en main le kit documentaire ainsi que de vous sensibiliser à la méthodologie de gestion de crise et d'organisation d'exercice



Prendre en main le **guide d'utilisation du pack documentaire** et récupérer l'ensemble des documents du pack pour pouvoir commencer l'organisation de l'exercice.



Parcourir le **support de présentation des enjeux, objectifs et méthodologie** de gestion de crise. Il vous fournira un socle méthodologique permettant d'appréhender l'organisation de l'exercice.



# 3. TUTORIEL D'ORGANISATION D'EXERCICE

## ÉTAPE 2

Il est maintenant temps de cadrer votre exercice et de définir les principaux éléments qui vont vous permettre de l'organiser



Prendre en main le **cahier des charges**, il vous présentera les différents éléments à définir pour pouvoir organiser votre exercice.



Prendre connaissance du document **d'organisation-type de cellules de crise**. Il vous proposera la composition de votre / vos cellule(s) de crise en fonction du niveau de complexité de votre exercice.



# 3. TUTORIEL D'ORGANISATION D'EXERCICE

## ÉTAPE 3

Vous allez maintenant pouvoir préparer le scénario ainsi que le chronogramme pour qu'ils s'adaptent au mieux aux spécificités de votre SI et votre organisation.



Au regard des éléments à adapter dans le **chronogramme** générique fournis, identifier les éléments propres à votre SI et à votre organisation (actif, application, processus critiques, etc.).



Repasser sur le **chronogramme** en modifiant les champs en rouge avec les éléments identifiés à l'étape ci-dessus que ce soit en termes d'acteur ou de contenu de stimuli, l'idée étant que le contenu soit le plus réaliste possible.



# 3. TUTORIEL D'ORGANISATION D'EXERCICE

## Étape 3 : Adapter le chronogramme

| EXERCICE JOP 2024 |         |  |                                   |  |
|-------------------|---------|--|-----------------------------------|--|
| N°                | HORAIRE | Type d'événement / sujet   | Degré de complexité de l'exercice | Catégorie d'acteur / Au sein d'un référentiel spécifique   |
|                   |         | <p>1.1. Ten de 8 à 12</p> <p>1.2. Ten de 14 à 16</p> <p>1.3. Ten de 18 à 20</p> <p>1.4. Ten de 22 à 24</p> <p>1.5. Ten de 26 à 28</p> <p>1.6. Ten de 30 à 32</p> <p>1.7. Ten de 34 à 36</p> <p>1.8. Ten de 38 à 40</p> <p>1.9. Ten de 42 à 44</p> <p>1.10. Ten de 46 à 48</p> <p>1.11. Ten de 50 à 52</p> <p>1.12. Ten de 54 à 56</p> <p>1.13. Ten de 58 à 60</p> <p>1.14. Ten de 62 à 64</p> <p>1.15. Ten de 66 à 68</p> <p>1.16. Ten de 70 à 72</p> <p>1.17. Ten de 74 à 76</p> <p>1.18. Ten de 78 à 80</p> <p>1.19. Ten de 82 à 84</p> <p>1.20. Ten de 86 à 88</p> <p>1.21. Ten de 90 à 92</p> <p>1.22. Ten de 94 à 96</p> <p>1.23. Ten de 98 à 100</p>   |                                   | <p>Contexte de l'exercice [C1]</p> <p><b>Temporalié :</b> Nous sommes le jour d'un grand événement sportif dans le cadre des JOF2024. Votre organisation accueille et par retour nous en direct à la télévision.</p> <p><b>Vecteurs d'attaques :</b> Différents vecteurs d'attaques ont été déployés comme : intrusion via mail de hameçonnage à un collaborateur puis sur un accès exposé à Internet, intrusion via compromission d'un poste via clé USB piégée.</p> <p><b>Impacts :</b> Ces différents attaques ont 2 grandes typologies d'impacts sur votre organisation : des impacts de confidentialité sur</p>   |
|                   |         | <p>2.1. Ten de 102 à 104</p> <p>2.2. Ten de 106 à 108</p> <p>2.3. Ten de 110 à 112</p> <p>2.4. Ten de 114 à 116</p> <p>2.5. Ten de 118 à 120</p> <p>2.6. Ten de 122 à 124</p> <p>2.7. Ten de 126 à 128</p> <p>2.8. Ten de 130 à 132</p> <p>2.9. Ten de 134 à 136</p> <p>2.10. Ten de 138 à 140</p> <p>2.11. Ten de 142 à 144</p> <p>2.12. Ten de 146 à 148</p> <p>2.13. Ten de 150 à 152</p> <p>2.14. Ten de 154 à 156</p> <p>2.15. Ten de 158 à 160</p> <p>2.16. Ten de 162 à 164</p> <p>2.17. Ten de 166 à 168</p> <p>2.18. Ten de 170 à 172</p> <p>2.19. Ten de 174 à 176</p> <p>2.20. Ten de 178 à 180</p> <p>2.21. Ten de 182 à 184</p> <p>2.22. Ten de 186 à 188</p> <p>2.23. Ten de 190 à 192</p> <p>2.24. Ten de 194 à 196</p> <p>2.25. Ten de 198 à 200</p> |                                   | <p>Contexte de l'exercice [C2]</p> <p><b>Temporalié :</b> Nous sommes le jour d'un grand événement sportif dans le cadre des JOF2024. Votre organisation accueille et par retour nous en direct à la télévision.</p> <p><b>Vecteurs d'attaques :</b> Différents vecteurs d'attaques ont été déployés comme : intrusion via mail de hameçonnage à un collaborateur puis sur un accès exposé à Internet, intrusion via compromission d'un poste via clé USB piégée et intrusion via compromission d'un ordinateur.</p> <p><b>Impacts :</b> Les 3 grandes typologies d'impacts sur votre organisation sont : des impacts de confidentialité sur</p>   |
|                   |         | <p>3.1. Ten de 202 à 204</p> <p>3.2. Ten de 206 à 208</p> <p>3.3. Ten de 210 à 212</p> <p>3.4. Ten de 214 à 216</p> <p>3.5. Ten de 218 à 220</p> <p>3.6. Ten de 222 à 224</p> <p>3.7. Ten de 226 à 228</p> <p>3.8. Ten de 230 à 232</p> <p>3.9. Ten de 234 à 236</p> <p>3.10. Ten de 238 à 240</p> <p>3.11. Ten de 242 à 244</p> <p>3.12. Ten de 246 à 248</p> <p>3.13. Ten de 250 à 252</p> <p>3.14. Ten de 254 à 256</p> <p>3.15. Ten de 258 à 260</p> <p>3.16. Ten de 262 à 264</p> <p>3.17. Ten de 266 à 268</p> <p>3.18. Ten de 270 à 272</p> <p>3.19. Ten de 274 à 276</p> <p>3.20. Ten de 278 à 280</p> <p>3.21. Ten de 282 à 284</p> <p>3.22. Ten de 286 à 288</p> <p>3.23. Ten de 290 à 292</p> <p>3.24. Ten de 294 à 296</p> <p>3.25. Ten de 298 à 300</p> |                                   | <p>Contexte de l'exercice [C3]</p> <p><b>Temporalié :</b> Nous sommes le jour d'un grand événement sportif dans le cadre des JOF2024. Votre organisation accueille et par retour nous en direct à la télévision.</p> <p><b>Vecteurs d'attaques :</b> Différents vecteurs d'attaques ont été déployés comme : intrusion via mail de hameçonnage à un collaborateur puis sur un accès exposé à Internet, intrusion via compromission d'un poste via clé USB piégée, intrusion via compromission d'un ordinateur et intrusion via compromission d'un serveur.</p> <p><b>Impacts :</b> Les 3 grandes typologies d'impacts sur votre organisation sont : des impacts de confidentialité sur</p> |
|                   |         | <p>4.1. Ten de 302 à 304</p> <p>4.2. Ten de 306 à 308</p> <p>4.3. Ten de 310 à 312</p> <p>4.4. Ten de 314 à 316</p> <p>4.5. Ten de 318 à 320</p> <p>4.6. Ten de 322 à 324</p> <p>4.7. Ten de 326 à 328</p> <p>4.8. Ten de 330 à 332</p> <p>4.9. Ten de 334 à 336</p> <p>4.10. Ten de 338 à 340</p> <p>4.11. Ten de 342 à 344</p> <p>4.12. Ten de 346 à 348</p> <p>4.13. Ten de 350 à 352</p> <p>4.14. Ten de 354 à 356</p> <p>4.15. Ten de 358 à 360</p> <p>4.16. Ten de 362 à 364</p> <p>4.17. Ten de 366 à 368</p> <p>4.18. Ten de 370 à 372</p> <p>4.19. Ten de 374 à 376</p> <p>4.20. Ten de 378 à 380</p> <p>4.21. Ten de 382 à 384</p> <p>4.22. Ten de 386 à 388</p> <p>4.23. Ten de 390 à 392</p> <p>4.24. Ten de 394 à 396</p> <p>4.25. Ten de 398 à 400</p> |                                   | <p>Contexte de l'exercice [C4]</p> <p><b>Temporalié :</b> Nous sommes le jour d'un grand événement sportif dans le cadre des JOF2024. Votre organisation accueille et par retour nous en direct à la télévision.</p> <p><b>Vecteurs d'attaques :</b> Différents vecteurs d'attaques ont été déployés comme : intrusion via mail de hameçonnage à un collaborateur puis sur un accès exposé à Internet, intrusion via compromission d'un poste via clé USB piégée, intrusion via compromission d'un ordinateur et intrusion via compromission d'un serveur.</p> <p><b>Impacts :</b> Les 3 grandes typologies d'impacts sur votre organisation sont : des impacts de confidentialité sur</p> |

Sélectionner la/les case(s) correspondant à votre niveau de complexité

Modifier l'ensemble des éléments rouges entre crochets pour les adapter à votre organisation

|          |                                 |              |                     |  |                    |                                |                            |  |
|----------|---------------------------------|--------------|---------------------|--|--------------------|--------------------------------|----------------------------|--|
| 09:30:00 | DEDEK                           | C1 / C2 / C3 | Tous les opérateurs | Bonjour, l'exercice commence maintenant. N'hésitez pas à contacter votre équipe d'animation pour toute question ou incompréhension.<br>[09:30:00-09:30:01]   | DIADANE            | Tous les jours                 | Mail                       | Aucune action particulière attendue.   |
| 09:35:00 | Métiers / Plaine application IT | C1 / C2 / C3 | Tous les opérateurs | Bonjour, un grand contact avec vous car mon équipe et moi-même venons poursuivre à votre équipement. [nommer une application critique dans le cadre de l'organisation de l'activité] message d'erreur s'affiche lorsque nous tentons d'accéder. Que devons nous faire? Nous devons absolument y accéder car [nommer le principe de l'application dans le cadre de l'activité]  | Manges/Vincent     | [responsable métier compétent] | Appel téléphonique ou mail | Signalement/échange avec le responsable compétent  |
| 09:38:00 | Plaine application IT           | C1 / C2 / C3 | Tous les opérateurs | Bonjour, je reçois beaucoup de signalements en interne, il semblerait que [nommer une application critique dans le cadre de l'organisation de l'activité] soit concerné par l'apparition d'un message d'erreur sur leurs postes informatiques et n'arrive pas à accéder à leurs fichiers de travail. Je vous joins une photo de message en PJ. Pourriez vous me transmettre des consignes ou des éléments de réponse que mon équipe et moi pourrions leur apporter des pistes pour la continuité de leur activité? | Arnaud IT ou David | [responsable métier compétent] | Appel téléphonique         | Prese en compte de la situation!<br>- Déconnecter au plus tôt les supports sauvegardés après vous être assurés qu'ils ne sont pas infectés<br>- Isoler les équipements infectés du SI en les déconnectant du réseau.<br>- Vérifier la présence ou non d'une éventuelle connexion sans fil sur ces équipements d'accès votre système d'information en isolant toutes les communications vers et depuis Internet.<br>- Rechercher dans les journaux du système d'information<br>- Si les machines infectées le permettent, il est donc recommandé d'activer la mise en veille prolongée afin de faire cesser l'activité du programme malveillant tout en préservant la mémoire en vue d'une analyse ultérieure |



# 3. TUTORIEL D'ORGANISATION D'EXERCICE

## ÉTAPE 4

Maintenant que votre scénario est déterminé, vous allez pouvoir préparer les différents supports pour permettre à vos joueurs de faire l'exercice avec des outils adaptés.



Remplir les **annuaires des joueurs et des animateurs** avec les coordonnées à contacter pendant l'exercice en faisant bien attention de respecter le niveau de complexité de votre exercice.



Adapter le **support de briefing des joueurs** en fonction des éléments que vous avez défini à l'étape précédente.



# 3. TUTORIEL D'ORGANISATION D'EXERCICE

## Étape 4 : Remplir les annuaires



Penser à sélectionner le bon niveau de complexité

| EXERCICE DE GESTION DE CRISE D'ORIGINE CYBER N 1<br>ANNUAIRE DES JOUEURS |               |              |           |
|--|---------------|--------------|-----------|
| Num/prénom   | Fonction/rôle | Adresse mail | Téléphone |
| Joueurs  |               |              |           |
|  |               |              |           |
|  |               |              |           |

Pour l'annuaire joueurs, indiquer le nom/prénom ainsi que les coordonnées de chacun des joueurs

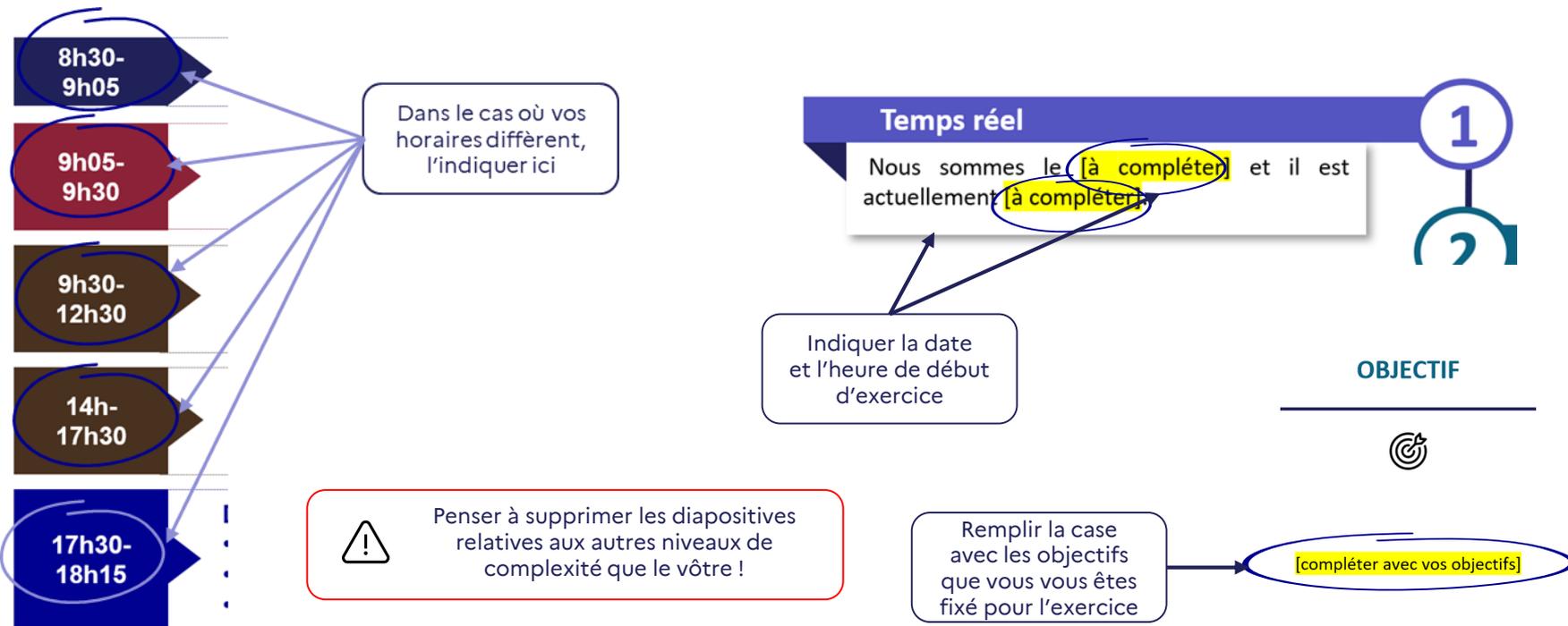
Pour l'annuaire animateurs, indiquer les coordonnées de chacune des entités simulées

| Fonction/rôle           | Adresse mail | Téléphone |
|-------------------------|--------------|-----------|
| Animateur de l'exercice |              |           |
| CHIL                    |              |           |
| DGSI                    |              |           |
| ANSSI                   |              |           |
| Préfecture              |              |           |



# 3. TUTORIEL D'ORGANISATION D'EXERCICE

## Étape 4 : Adapter le support de briefing joueurs





# 3. TUTORIEL D'ORGANISATION D'EXERCICE

## ÉTAPE 5

Une fois que votre exercice est prêt d'un point de vue planification, il est temps de le présenter aux observateurs et aux animateurs afin de les préparer à leur rôle.



Transmettre aux observateurs le **support méthodologique d'observation**. Il leur permettra de prendre connaissance de leur rôle et ainsi d'avoir des retours d'observation les plus pertinents possibles



Présenter le scénario de l'exercice aux observateurs et aux animateurs après avoir adapté le **support de présentation du scénario** à votre exercice. Cela leur permettra de prendre connaissance de ce qui va être joué.



Transmettre la **grille d'observation** aux observateurs pour qu'ils puissent en prendre connaissance en amont de l'exercice.



# 3. TUTORIEL D'ORGANISATION D'EXERCICE

## ÉTAPE 6

**C'est le Jour J !**

Il convient tout de même de vous assurer d'avoir tous les documents et toutes les informations nécessaires afin que l'exercice puisse se dérouler au mieux



Réaliser le briefing des joueurs avec le support de présentation adapté précédemment



Transmettre l'ensemble des documents supports aux parties concernées, **main courante** et **annuaires pour les joueurs, chronogramme** pour les animateurs etc.



### 3. TUTORIEL D'ORGANISATION D'EXERCICE

#### ÉTAPE 7

Maintenant que l'exercice est terminé, il est important de réaliser les RETEX de l'exercice afin de pouvoir en tirer les enseignements nécessaires et mettre en place un plan d'action pertinent



Réaliser le RETEX à chaud juste après la fin de l'exercice. Pour cela, prenez connaissance du **support de méthodologie de RETEX à chaud**. Vous disposez aussi d'un **modèle de support de RETEX à chaud** que vous n'avez qu'à modifier



Transmettre aux participants puis recueillir le **questionnaire de RETEX à froid**. Il vous permettra de préparer au mieux votre RETEX à froid et de recueillir les ressentis plus construits des participants.



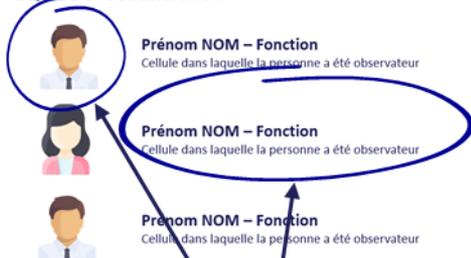
Réaliser le RETEX à froid dans le mois suivant l'exercice. Pour cela, prenez connaissance du **guide méthodologique de RETEX à froid**. Adaptez le **modèle de support de RETEX à froid** en intégrant les éléments des grilles et des questionnaires, cela vous permettra d'établir un plan d'action avec les participants.



# 3. TUTORIEL D'ORGANISATION D'EXERCICE

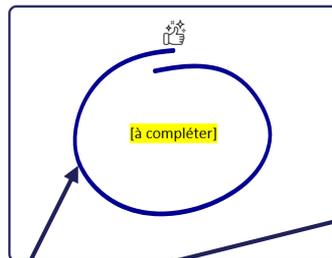
## Étape 7 : Réaliser le RETEX à chaud

### EQUIPE D'OBSERVATION

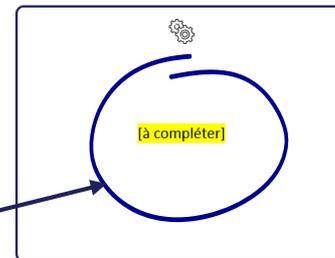


Indiquer la composition des équipes de planification, d'observation et d'animation

### Points forts



### Axes d'amélioration



Compléter les points forts et axes d'amélioration au fur et à mesure des tours de table pour en conserver la synthèse

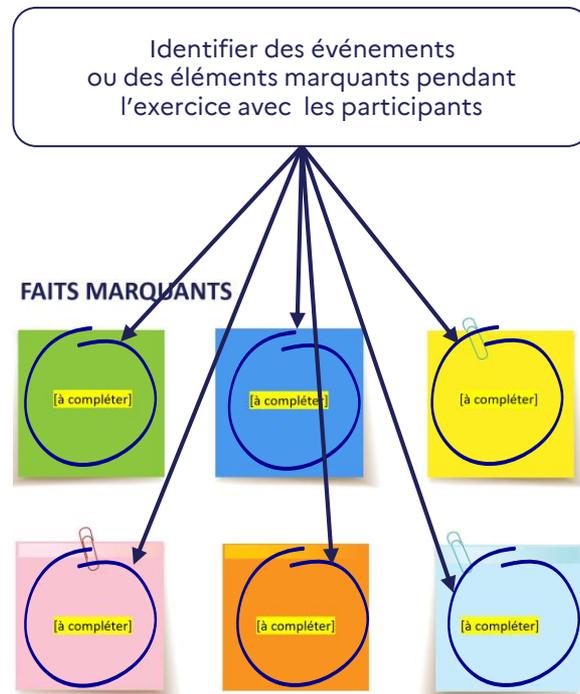
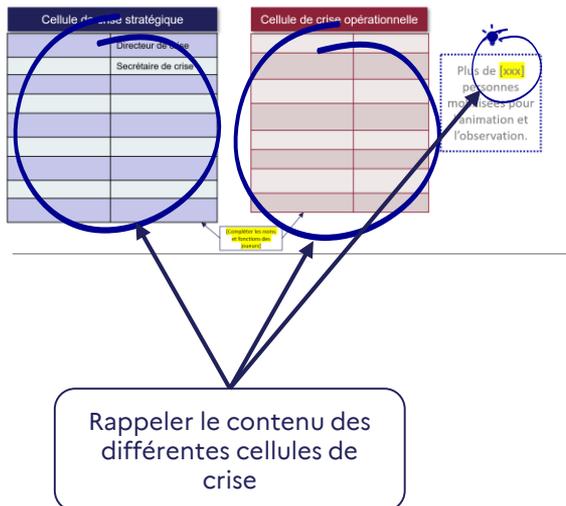
Préciser la date et le lieu du RETEX au froid pour permettre aux participants d'adapter leur planning





# 3. TUTORIEL D'ORGANISATION D'EXERCICE

## Étape 7 : Réaliser le RETEX à froid





# 3. TUTORIEL D'ORGANISATION D'EXERCICE

## Étape 7 : Réaliser le RETEX à froid

| Thème                               | Score | Points forts | Points à améliorer |
|-------------------------------------|-------|--------------|--------------------|
| Méthodologie de la cellule de crise |       |              |                    |
| Organisation de la cellule de crise |       |              |                    |
| Communication interne et externe    |       |              |                    |
| Prise de décision                   |       |              |                    |
| Réponse métier                      |       |              |                    |

Identifier les points forts et axes d'amélioration issus des questionnaires de RETEX à froid

Élaborer un plan d'action à partir des synthèses des résultats et le rapporter dans le tableau ci-dessous

| Axe d'amélioration identifié | Proposition de mesure d'amélioration | Délai de mise en place |
|------------------------------|--------------------------------------|------------------------|
|                              |                                      |                        |
|                              |                                      |                        |
|                              |                                      |                        |
|                              |                                      |                        |



**RÉPUBLIQUE  
FRANÇAISE**

*Liberté  
Égalité  
Fraternité*

