12 mai 2014

QSE : qualité et gouvernance des systèmes d'information

Module n°4 : la gestion de crise

solucom
management & IT consulting

Agenda

1. Introduction
2. Les dispositifs de gestion de crise
3. S'entraîner avec des exercices de gestion de crise

Qu'est-ce qu'une crise ?

Une crise est …

- Une situation **soudaine**, souvent **brutale**, **inattendue**, aux **conséquences** potentiellement **très graves** pour l'entreprise et pour laquelle les **mécanismes** et réactions **habituels** sont **inadaptés**

Ses origines sont extrêmement variées

- **Naturelles** inondations, tempêtes, grands froids, légionellose, épidémies…
- **Environnementales** incendies, explosions liées à des infrastructures ou sites à risque...
- **Humaines** défaillance de processus, erreur humaine, malveillance, attentat…
- **Technologiques** panne informatique, défaillance matérielle, virus, cyber-attaque…

Des événements affectant trois dimensions

- ❶ périmètre géographique
- ❷ dimension humaine/organisationnelle
- ❸ patrimoine informationnel




Gérer une crise efficacement se prépare en amont

Gérer la crise c'est …

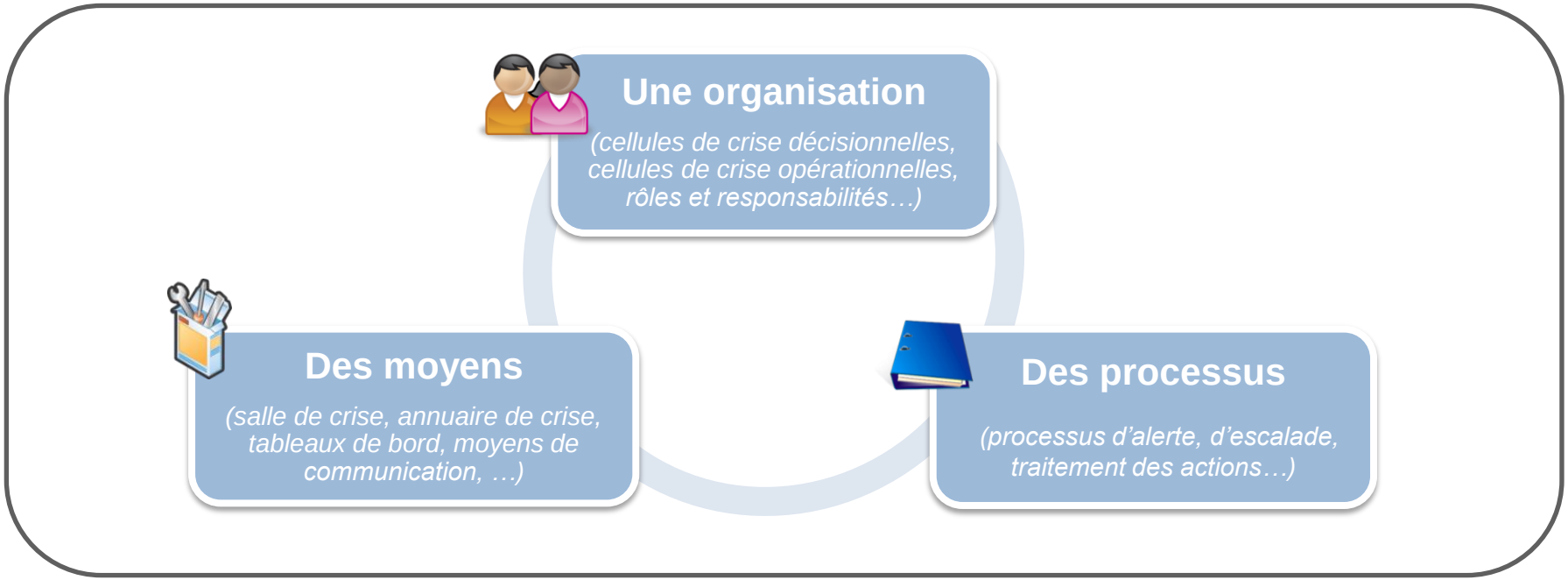
- Réunir les acteurs les plus appropriés (**mobilisation**)
- Prendre **rapidement** les bonnes décisions sur les actions à conduire pour limiter la propagation de la crise et en sortir
- **Orchestrer** la mise en œuvre des actions décidées
- Adapter la **communication** à la situation
- Utiliser les documents et démarches éprouvés

… malgré des facteurs aggravants

- Cascade des événements additionnels (médias, pouvoirs publics, partenaires de l'entreprise…)
- Pressions importantes, internes comme externes
- Capacités individuelles altérées par le stress pouvant provoquer une montée de la subjectivité

Il est essentiel de mettre en place un dispositif de crise préparé, entrainé, et maintenu dans la durée

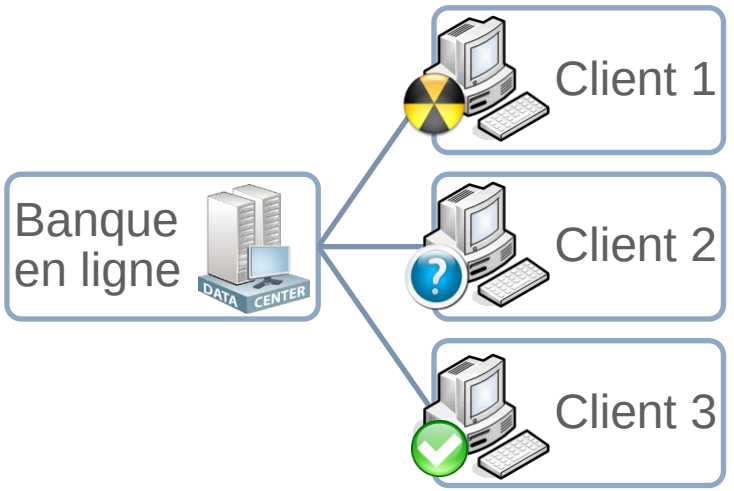
Introduction
La gestion de crise est axée sur trois piliers



- **une organisation et des processus**
  - Un **mode de gouvernance spécifique** pour prendre toute décision nécessaire à la préservation des intérêts de l'entreprise
  - Une déclinaison en plusieurs « **cellules de crise** » répondant à différents enjeux
- **… dotés de moyens et d'outils**
  - Locaux pour la tenue des réunions des cellule / outils de communication
  - Documents de crise (checklists, annuaires, main courante, …)
  - Plan de communication, plan de continuité d'activité (PCA), plan de secours industriel, …

Contexte :

- Au sein d'un groupe bancaire, vous êtes responsable de la sécurité de la **banque en ligne**
- Ces dernières heures, certains de vos clients ont remonté des **virements illégitimes** en leur nom
- Les premières investigations menées par vos équipes montrent la présence de **virus sur les ordinateurs** de ces clients



A vous de jouer :

- ***Quels sont les impacts potentiels d'un tel événement pour la banque et ses clients ?***
- ***Comment vous organisez-vous pour résoudre cette crise ?***

Agenda

1. Introduction

2. Les dispositifs de gestion de crise

   2. 1 Une organisation

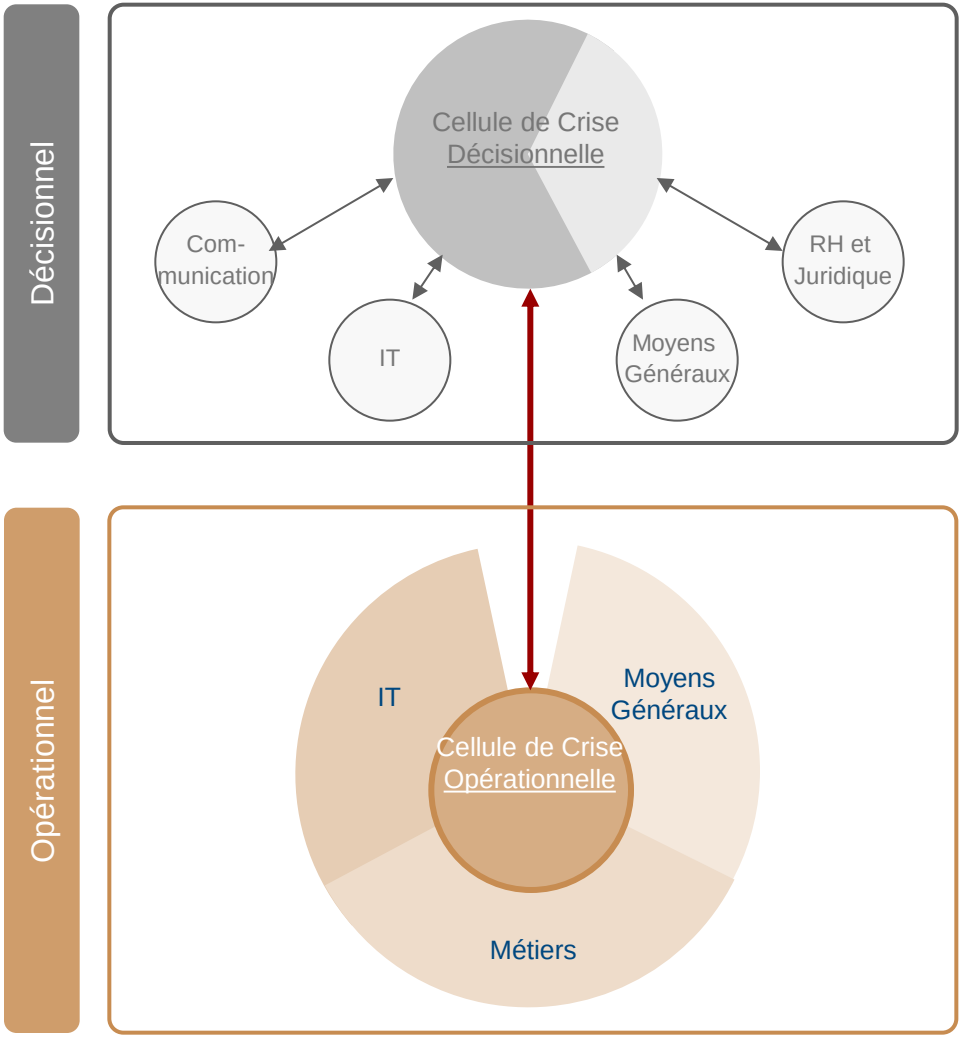
   2. 2 Des processus

   2. 3 Des moyens

   2. 4 Exemple de gestion de crise : la Crue de Seine

3. S'entraîner avec des exercices de gestion de crise

Les dispositifs de gestion de crise : une organisation
Modèle d'organisation de crise



Membres permanents

Membres de la Direction sollicités selon la nature de la crise, et/ou les Métiers sinistrés

Experts des Métiers ou Fonctions d'appui pouvant être sollicités par la Cellule de Crise Décisionnelle

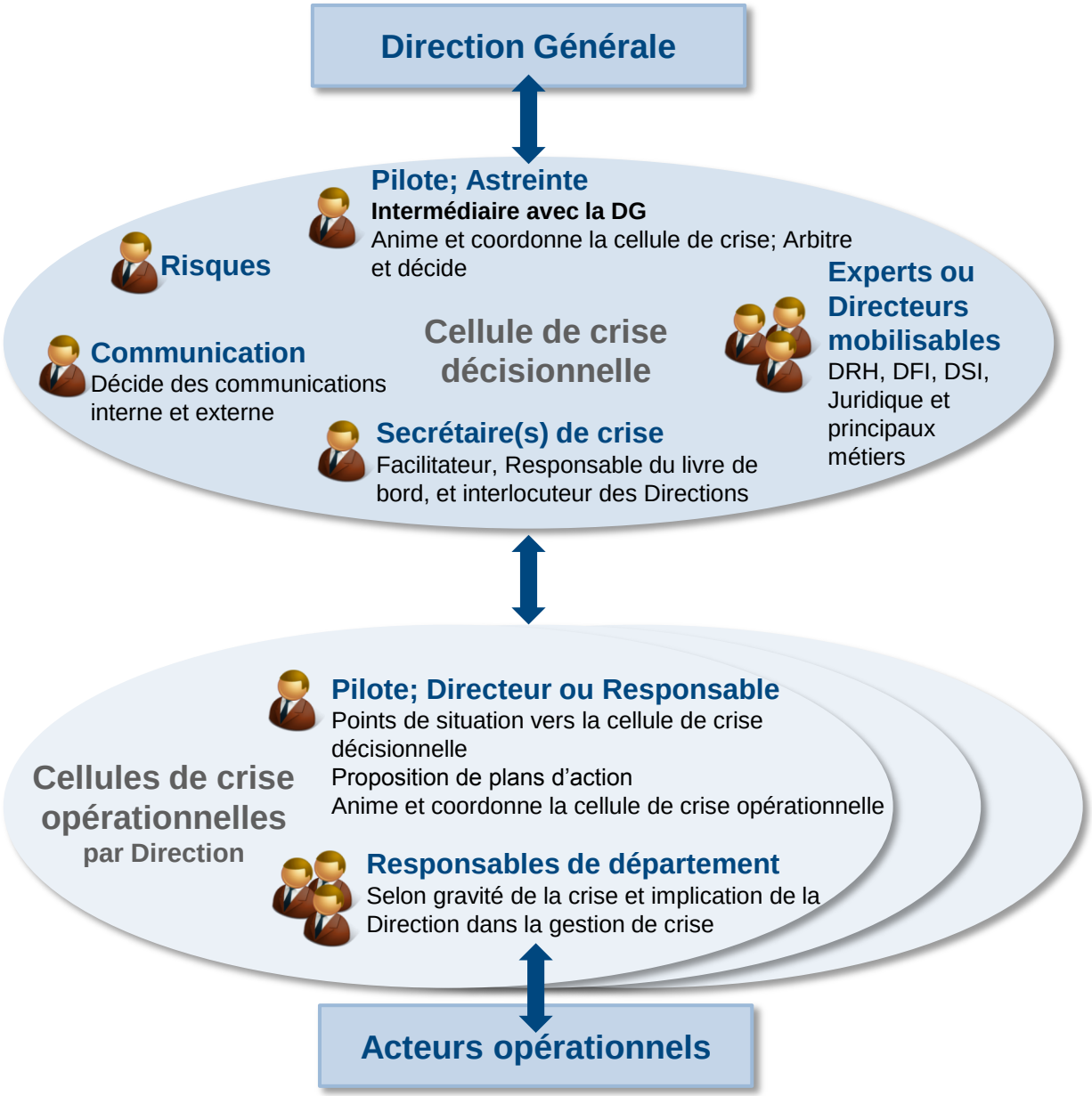
Membre(s) de coordination des cellules op.

Cellule(s) de crise opérationnelle(s) IT

Cellule(s) de crise opérationnelle(s) Métier(s)

Cellule(s) de crise opérationnelle(s) Moyens Généraux

Les dispositifs de gestion de crise : une organisation
Exemple de macro organisation : rôles et responsabilités



Rôles de la cellule de crise décisionnelle (CD) :

- Décisions et contrôles (dont déclenchement et sortie de crise)
- Suivi et pilotage de la crise
- Interlocuteur de la cellule de crise et autres cellules de crise Métiers

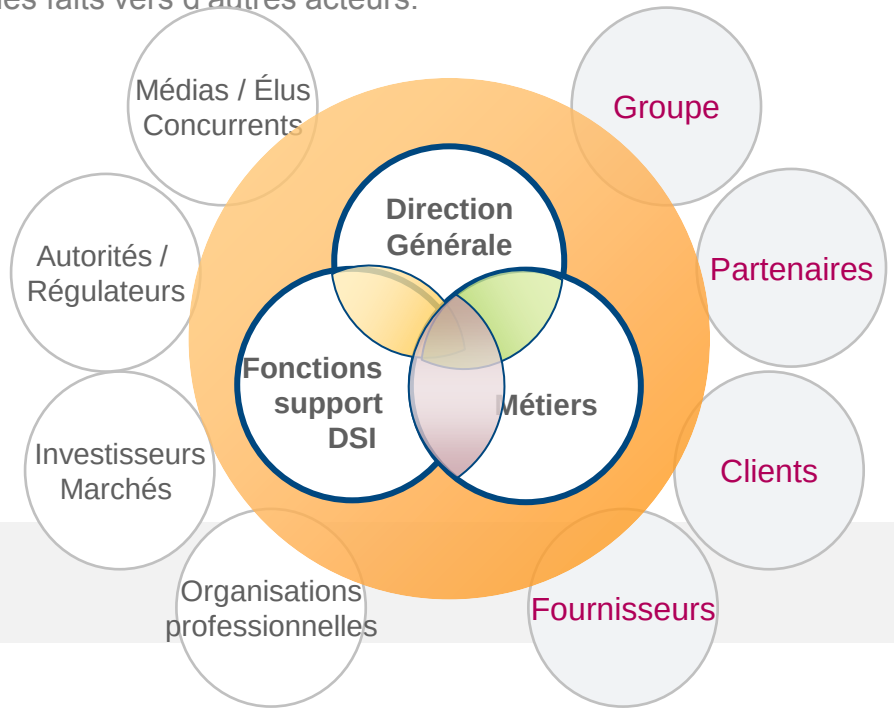
Rôles de la cellule de crise opérationnelle (CO) :

- Analyse et évaluation de la situation
- Appréciation et anticipation des impacts
- Proposition de plan d'actions à la CD
- Reporting régulier à destination de la CD
- Pilotage et coordination des acteurs opérationnels
- Sollicitation des experts en fonction de la nature de la crise

La communication : une difficulté majeure en matière de gestion de crise

Conserver la capacité à bien communiquer…

- Être **maître de sa stratégie de communication**
  - **Reconnaissance** : accepter la crise le plus rapidement possible. Communiquer clairement et fermement.
  - **Refus** : Minimiser les effets de la crise à condition d'être le seul interlocuteur à disposer des données.
  - **Report de la responsabilité** : reporter la responsabilité. Orienter les faits vers d'autres acteurs.
  - Etc.
- S'assurer de la **cohérence et pertinence des messages**
- **Maintenir le lien** entre toutes les parties prenantes de la crise
- **Adaptation des messages** aux différentes populations cible



… au travers d'interfaces de communication identifiées et exercées

- Maitriser les interfaces de communication **internes** *(Communication faite par le directeur général, par le management de proximité, etc.)*
- Maitriser les interfaces de communication **externes** *(Communication presse, site web, etc.)*

Agenda

1. Introduction

2. Les dispositifs de gestion de crise

   2. 1 Une organisation

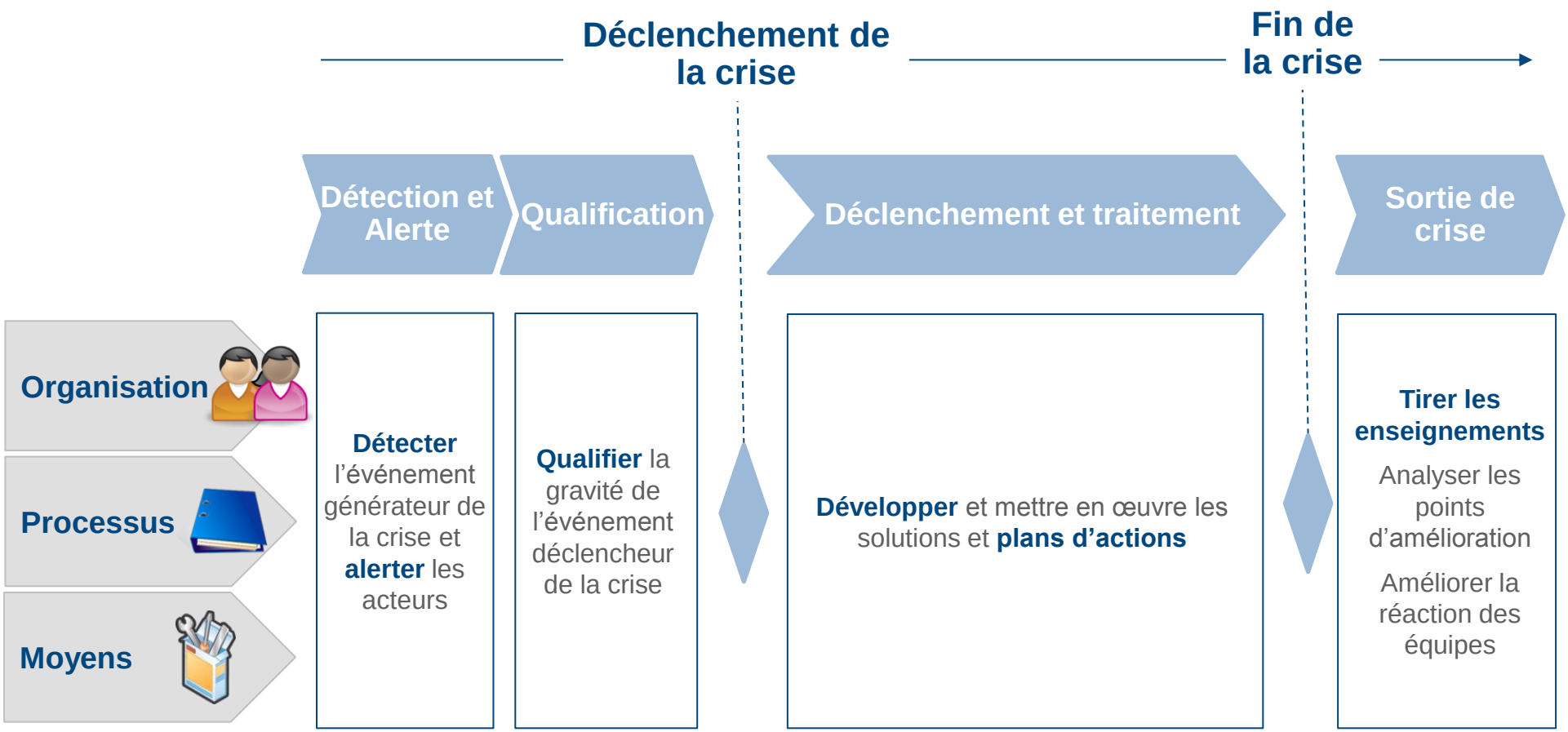
   2. 2 Des processus

   2. 3 Des moyens

   2. 4 Exemple de gestion de crise : la Crue de Seine

3. S'entraîner avec des exercices de gestion de crise

Les dispositifs de gestion de crise : des processus
Le processus de gestion de crise se décline en quatre phases



Processus – exemple de la détection d'un incident SI : détection et alerte

Détection

Acteurs	Actions	Documentation
Acteurs opérationnels	1 Détection de l'incident par un utilisateur externe / Détection de l'incident par un acteur interne / Détection de l'incident par un prestataire	
	2 Appel au Helpdesk et pré-diagnostic / Pré-diagnostic par l'acteur interne / Pré-diagnostic du prestataire en interne	Fiche pré-diagnostic
Responsable de domaine	3 Remontée au responsable de domaine	

Processus – exemple de la détection d'un incident SI : qualification

Qualification

Acteurs	Actions	Documentation
Responsable de domaine	4 Qualification de l'incident	
Responsable de domaine	Incident grave ? — Non → Traitement de l'incident hors gestion de crise et suivi de l'évolution	
Responsable de domaine	Oui → 5 Alerte du responsable* de coordination Cellule de crise Décisionnelle de son périmètre	Annuaire de crise
	Responsable joignable ? — Non → retour à l'alerte	
Responsable de coordination Cellule de crise Décisionnelle alerté	Oui → 6 Accusé de réception et analyse de la situation	
	Aggravation de la situation ? — Oui → retour à la qualification ; Non → Traitement de l'incident hors gestion de crise et suivi de l'évolution	Fiche Diagnostic

* Ou de son suppléant

Processus – exemple de la détection d'un incident SI : diagnostic de la crise

Afin de diagnostiquer la gravité de l'incident, les acteurs disposent d'une grille d'aide à la décision adaptée au contexte

Utilisateurs impactés	Périmètre applicatif impacté	Durée estimée du sinistre
Quelques sites utilisateurs non critiques	**Aucune application critique ou très critique**	**< 2 heures**
Un site utilisateur critique impacté	**1 à 2 applications critiques**	**2 heures ≤ T ≤ 4 heures**
Plusieurs sites utilisateurs critiques	**Plus de deux applications critiques ou une application très critique**	**> 4 heures ou inconnue**

Alerte systématique du responsable de coordination de la cellule de crise décisionnelle SI de son périmètre dans les cas suivants :

- 3 critères sont au niveau rouge
- 2 critères sont au niveau rouge et 1 critère au niveau orange

Processus – exemple de la détection d'un incident SI : déclenchement

Déclenchement

Acteurs	Actions	Documentation
Responsable de coordination Cellule de crise Décisionnelle alerté	6 Analyse de la situation	Fiche Diagnostic
	Risque de crise ? Non → Traitement de l'incident hors gestion de crise et suivi de l'évolution	
	Oui	
	7 Alerte du Directeur de crise*	
	Directeur joignable ? Non (* Ou de son suppléant)	
	Oui	
Directeur de crise	8 Accusé de réception	
	Crise avérée ? Non → Aggravation de la situation ? Oui / Non	PV de déclenchement de crise
	Oui	
Directeur de crise	9 Activation de la CD	Annuaire de crise
Responsables de coordination Cellule Décisionnelle	10 Activation de la CO	

Processus – exemple de la détection d'un incident SI : traitement

Traitement

Acteurs	Actions	Documentation
CO et CD	11 Proposition de plan d'action par la CO ↔ Validation des orientations par la CD et envoi relevé de décisions	
CO	12 Lancement des actions du plan défini 13 Point de situation par la CO à la CD	Modèle de relevé de décision CD Modèle de reporting CO
CD	14 Analyse de la situation par la CD Besoin de revue du plan d'action? — Oui → 11 Non Fin de la crise ? — Non → 13 Oui	Journal de bord CD

Processus – exemple de la détection d'un incident SI : sortie de crise

Sortie de crise et Retour d'expérience

Acteurs	Actions	Documentation
CD	15 Envoi PV de fin de crise	PV de sortie de crise
CO et CD	16 Réalisation d'un bilan « à chaud » de la crise	
Ensemble des acteurs de la crise	17 Bilan final « à froid » de la crise	Rex de crise
RSSI	18 Suivi des actions correctives et préventives	

Agenda

1. Introduction

2. Les dispositifs de gestion de crise

   2. 1 Une organisation

   2. 2 Des processus

   2. 3 Des moyens

   2. 4 Exemple de gestion de crise : la Crue de Seine

3. S'entraîner avec des exercices de gestion de crise

Les dispositifs de gestion de crise : des moyens
Exemple de moyens

Des moyens de communication


Téléphone(s)
Audioconf.


Fax


Mobiles


Ordinateur(s)
Accès réseau(x)

De la documentation…


Annuaire
de crise


Procédures (diagnostic, journal de bord…)

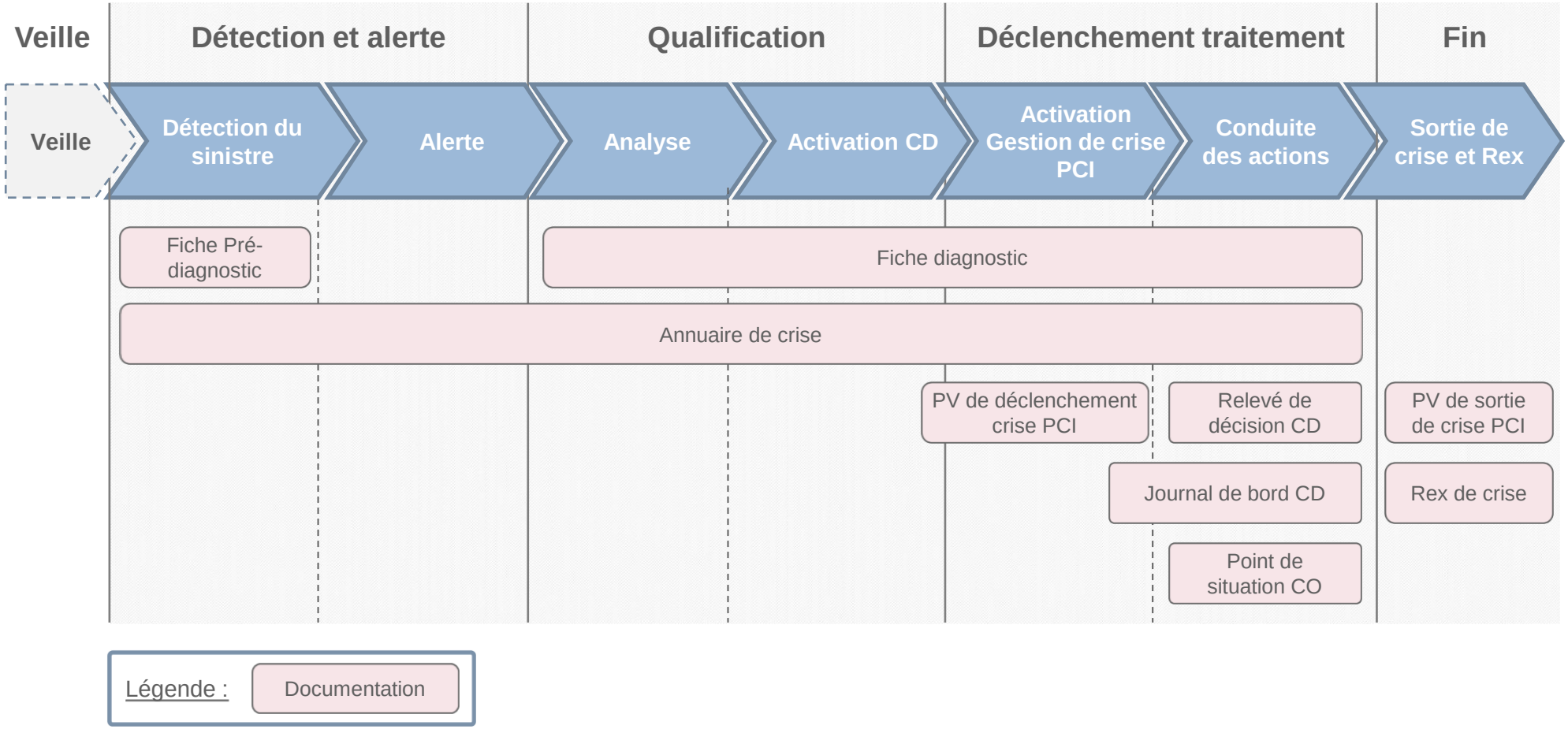
Des locaux dédiés


Salle « sur site »


Salle « hors site »
inaccessibilité du site nominal

Les dispositifs de gestion de crise : des moyens
Exemple de documentation de crise

Pour chaque étape, des documents doivent être disponibles pour servir de support à la gestion de crise. Ils sont consignées dans un classeur de crise mis à disposition des cellules de crise DSI.



Agenda

1. Introduction

2. Les dispositifs de gestion de crise

2. 1 Une organisation

2. 2 Des processus

2. 3 Des moyens

2. 4 Exemple de gestion de crise : la Crue de Seine

3. S'entraîner avec des exercices de gestion de crise

Exemple de gestion de crise : la Crue de Seine
Des impacts importants sur l'ensemble des réseaux en Île de France…

Électricité :

1 500 000 de foyers seront concernés par le risque de coupure électrique

Transports en commun :

140km sur 250km du réseau de métro fermés préventivement. Arrêt de fonctionnement des RER A, B et C, des gares de Lyon et d'Austerlitz et des lignes de métro

Télécommunications :

Réseau potentiellement coupé compte tenu des coupures de l'alimentation électrique

Jusqu'à

58

milliards d'€ de dégâts

Transport routier :

- **100% des ponts à Paris** et en Petite Couronne seront inaccessibles
- Les autoroutes A86, A4 et A6 coupées à certains endroits
- Engorgement des voies de circulation

Energie :

40% des clients ne seraient plus alimentés par le chauffage urbain

De nombreux centres de distribution d'hydrocarbures sont inondés

Assainissement :

Les égouts débordent et l'élimination des déchets ménagers est rendue très difficile

Eau potable :

5 000 000 de personnes seraient privées d'eau potable et **1 300 000** de personnes subiraient une dégradation de qualité de l'eau

Exemple de gestion de crise : la Crue de Seine
…et pour les entreprises en bord de Seine : cas d'une banque

Des impacts forts et rapides

- **Siège rapidement impacté *(dès la phase 2)***
- **30% des agences fermées 50% perturbées**
- **Perturbation importante des Ressources Humaines. Absentéisme important à prévoir**

Un dispositif spécifique pour ce scénario de crise

- **3 sites de repli pour le siège**
- **1 organisation de repli spécifique pour les agences**
- **1 dispositif RH spécifique *(accompagnement et suivi)***
- **Des moyens logistiques mis en œuvre**

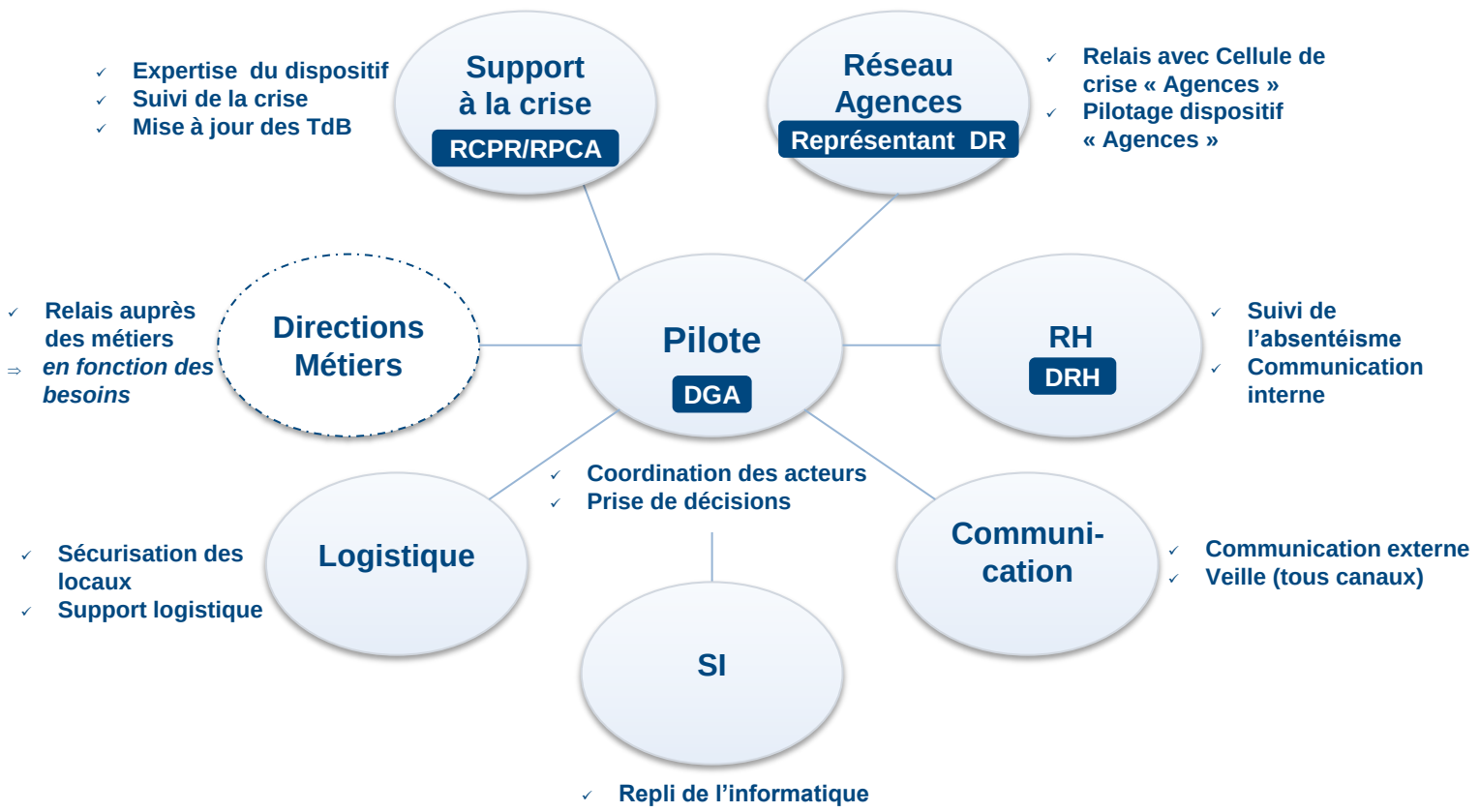
Rôle de la cellule de crise : utiliser le dispositif prévu

Exemple de gestion de crise : la Crue de Seine
Un traitement adapté à la gravité de la situation

Fiche Scénario

	Phase 1 3,20m – 6m	Phase 2 6m – 7m	Phase 3 7m – 8m	Phase 4 > 8m	Phase 5 Décrue
Événements déclencheurs	Alerte Vigicrue	Premières infiltrations par les sous-sols	Inaccessibilité des quelques sites	Très fort absentéisme, crise régionale	Décrue suffisante pour engager la reprise des activités essentielles
Objectifs pour l'entreprise	**Informer, prévenir, préparer**	**Limiter les perturbations, préparer le repli**	**Orchestrer le repli (à minima du noyau dur des activités)**	**Gérer le repli (à minima des activités du cœur)**	**Relancer l'activité**
Gestion de crise	Traitement de l'alerte, Veille sur l'évolution de la situation	Convocation de la cellule de crise pour analyse et coordination	Repli de la cellule de crise et déclenchement et orchestration du repli des effectifs clés	**Situation extrême : gestion de la situation par la cellule de crise selon l'évolution**	Pilotage : ▪ de la remise en état des infrastructures ▪ de la reprise des activités essentielles
Communication	Communication interne auprès des acteurs du PCA	Mise en place des outils de communication de crise Réponse aux sollicitations externes	Communication interne auprès de tout le personnel Réponse aux sollicitations externes		Communication interne post crise Réponse aux sollicitations externes
Logistique		Préparation des sites de repli	Accompagnement au repli		Évaluation des travaux et remise en état
Management		Réponse aux sollicitations des collaborateurs	Application de la procédure de repli du PCA métier		Expression de besoins pour prioriser les travaux
RH		Surveillance de l'absentéisme	Solutions d'accompagnement RH		Surveillance de l'absentéisme
Agences	Convocation de la cellule de crise « Agences »	Repli des premières agences impactées Communication préventive aux clients « coffres »	Fermeture préventive d' agences et repli. Réaffectation des collaborateurs		Réouverture progressive des agences

Exemple de gestion de crise : la Crue de Seine
Une cellule de crise décisionnelle à la composition adaptée



Moyens à disposition de la cellule

- Mémento de crise
- Fiche scénario
- « Cockpit de crise »
- « Qui fait quoi ? »
- Journal de crise

Moyens logistiques :

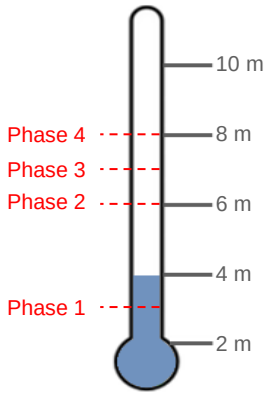
- **Salle** dédiée
- **Communication** : messagerie et téléphonie habituelles
- **Restauration / Hébergement**

Légende Moyens à disposition ✓ Rôle dans la cellule

Exemple de gestion de crise : la Crue de Seine
Des indicateurs objectifs permettant de se prononcer sur la sortie de crise

Ampleur de la crue

Source : site Vigicrue »



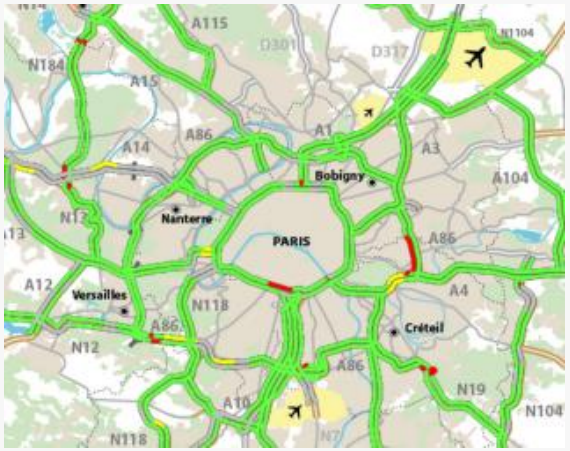
Niveau de l'eau
Paris Austerlitz
04/02/14 - 16:51

Tendance

Transports

Source : site « Sytadin »

Réseau routier



Source : sites « Info RATP » & « Info SNCF »

Transports en commun

Lignes ouvertes

M T	16/24	Détail
RER	5/5	Détail
	2/8	Détail

Réseaux et services

Source : dépêches AFP

Électricité	30 000 foyers sans électricité
Énergie	…
Assainissement	…
Eau potable	…
Télécommunications	…

Annonces & instructions des pouvoirs publics

Source : dépêches AFP

03/02/2014 – 14:36	*« Les habitants des Hauts de Seine invités à limiter leurs déplacements »*
03/02/2014 – 10:12	…
02/02/2014 – 19:24	…

Agenda

1. Introduction
2. Les dispositifs de gestion de crise
3. S'entraîner avec des exercices de gestion de crise

3. 1 Comment préparer l'exercice ?

3. 2 Attaque informatique : un exercice de gestion de crise cybercriminalité

S’entraîner avec des exercices de gestion de crise
Exercer son dispositif dédié à la gestion de crise est un facteur de succès !

De la théorie…

- Une **crise** est une situation soudaine, souvent brutale, inattendue, aux **conséquences potentiellement très graves pour l’entreprise.**
- La survenance d’une crise rend inadapté les mécanismes et réactions habituels de l’entreprise. La gestion de crise nécessite de mettre en place :
  - **Des moyens**
  - **Une organisation**
  - **Des processus**

Le dispositif de gestion de crise doit donc être :

- **Préparé**
- **Entraîné**

- **Maintenu**

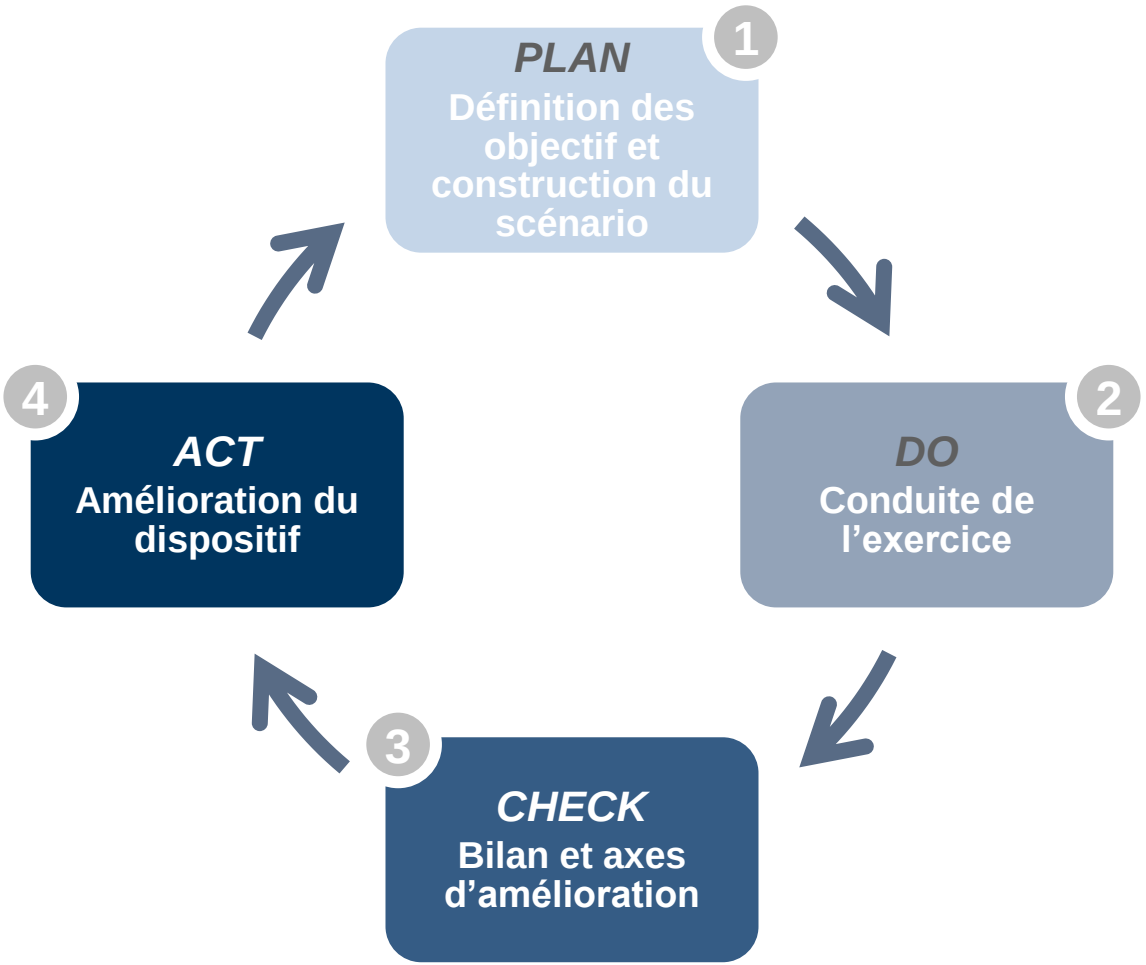
… à la pratique

- **Un exercice à adapter au degré de maturité de l’entreprise à la gestion de crise :**

Sensibiliser	Former	Éprouver	Améliorer
▪ Présenter le dispositif ▪ Impliquer les acteurs ▪ **Prise de conscience de la problématique**	▪ Faire s’approprier le dispositif aux acteurs ▪ Manipuler / Connaître le dispositif	▪ S’assurer de l’appropriation ▪ Améliorer le dispositif ▪ Se rapprocher d’une crise réelle(stress…)	▪ Introduire de nouvelles crises ▪ Faire évoluer les process / l’organisation

Propriété de Solucom, reproduction interdite

S’entraîner avec des exercices de gestion de crise
Un exercice de gestion de crise s’inscrit dans une logique d’amélioration continue



Propriété de Solucom, reproduction interdite

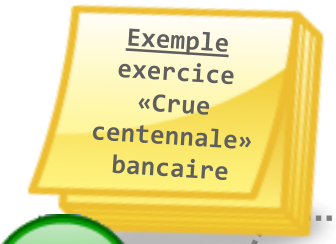
S’entraîner avec des exercices de gestion de crise
Tester un périmètre précis du dispositif de gestion de crise

Plan / Act / Do / Check

Les composantes de la gestion de crise

- Organisation
- Moyens
- Processus

La définition du périmètre de l’exercice passe par la sélection des composantes à tester



	Organisation	Moyens	Processus
Éléments des composantes testés	▪ Cellule de crise Agences	▪ Outil de réaffectation des collaborateurs ▪ Salle de crise ▪ Tableaux de bord ▪ Journal de crise et suivi des actions	▪ Fermeture des agences ▪ Gestion des incivilités ▪ Alimentation des DAB
Éléments des composantes non testés	▪ Cellule de crise Siège	▪ Outil d’alerte (veille « vigicrue ») ▪ Annuaire de crise ▪ Moyens de communication externes	▪ Gestion des coffres-forts ▪ Montée en charge la cellule de crise ▪ Atomisation de la cellule de crise ▪ Coordination avec la cellule de crise Siège

Propriété de Solucom, reproduction interdite

S'entraîner avec des exercices de gestion de crise
L'interactivité, un concept au cœur de l'exercice de gestion de crise

Plan
Act
Do
Check

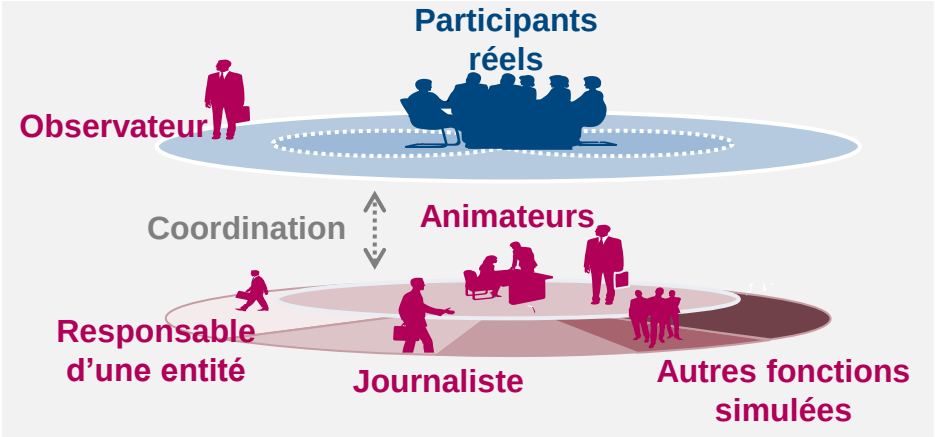
Journal de bord

Document dans lequel est restitué de façon précise et complète **le déroulement de l'exercice par l'observateur**

Tableaux de bord

Document dans lequel est restitué de façon précise et complète **le déroulement de l'exercice par l'observateur**

Cellule de crise



Cellule d'animation

Chronogramme

Document permettant d' :

- **Identifier les acteurs impliqués** dans l'organisation de l'exercice
- Recenser **l'ordonnancement et le timing précis des actions et des animations**

Les stimuli

Signaux de stress et informations communiqués par la cellule d'animation à la cellule de crise pendant l'exercice:

- **Supports textes** (e-mails internes et externes, dépêches,…)
- **Événements sonores et vidéos** (Appels téléphoniques, flash radios/tv)
- **Événements réels**

Les stimuli utilisés évoluent avec le degré de maturité de l'entreprise à la gestion de crise

Propriété de Solucom, reproduction interdite

S’entraîner avec des exercices de gestion de crise
Un bilan de l’exercice: établir des constats et identifier des axes d’amélioration

Plan · Act · Do · Check

1 Bilan à chaud

- Collecter, partager et confronter **des perceptions des participants sur le déroulement de l’exercice** en vue d’aboutir à des premiers constats

2 Bilan à froid

- Formaliser les **conclusions finales** de l’exercice
- Définir un **plan d’action** pour faire évoluer le dispositif

3 Amélioration du dispositif

- Continuer à **maintenir, entraîner et améliorer le dispositif de gestion** de crise quelles que soient les conclusions du bilan.

Constat	Proposition d’amélioration	Acteurs	Priorité	Complexité
C08 : La boite à outils de la communication gagnerait à être plus opérationnelle (messages parfois trop longs ou trop compliqués, absence de communication web,…).	P08.1 : Faire une nouvelle version de la boite à outils afin de la rendre plus opérationnelle (messages plus courts, plus simples contenant l’information essentielle).	Michel Dupond	Élevée	Moyenne
	P08.2 : Faire valider, par le directeur Communication, la boite à outils contenant les messages pré-rédigés. La cellule de crise ne devra valider pendant la crise que les éléments de contexte à intégrer (hauteur d’eau, décisions de la cellule de crise,…).	Caroline Martin	Élevée	Moyenne

Propriété de Solucom, reproduction interdite

Agenda

1. Introduction
2. Les dispositifs de gestion de crise
3. S'entraîner avec des exercices de gestion de crise

3. 1 Comment préparer l'exercice ?

3. 2 Attaque informatique : un exercice de gestion de crise cybercriminalité

Propriété de Solucom, reproduction interdite

Un exercice de crise cybercriminalité
Un exercice pour sensibiliser à la cybercriminalité…

3 objectifs de l'exercice…

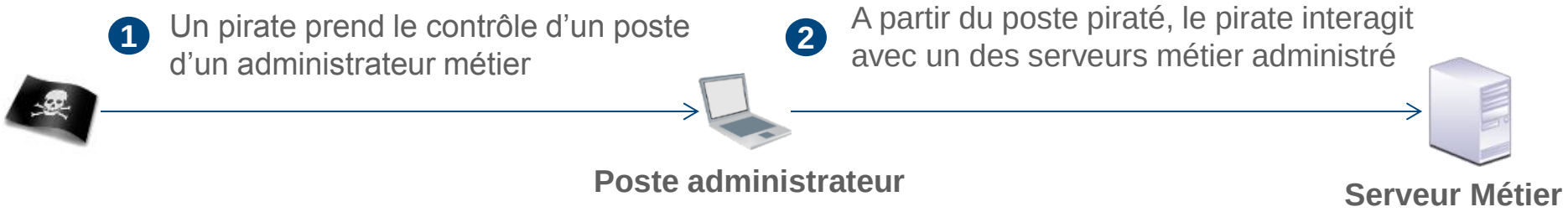
- Travailler sur la **détection et la qualification** d'un incident technique en « incident de sécurité »
- Vérifier que les **campagnes de sensibilisation** réalisées portent leur fruit (connaissance des symptômes et des procédures)
- Sensibiliser les équipes à travers l'exercice et faire des personnes impliquées des **ambassadeurs du sujet**

…Pour 3 enjeux de la filière SSI

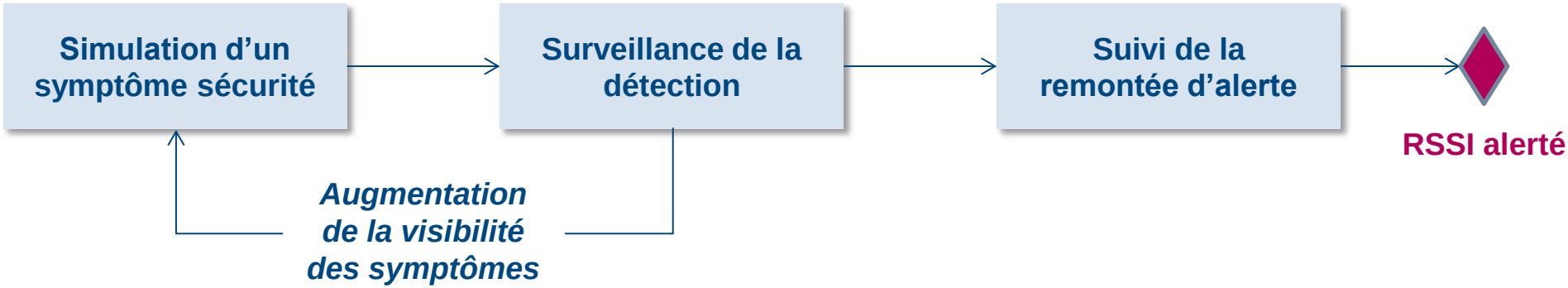
- La SSI souhaite vérifier que l'équipe ciblée sait différencier incident de sécurité et incident d'exploitation
- La SSI souhaite apporter du poids à son travail de sensibilisation à la sécurité
- La SSI souhaite que les acteurs et les cibles parlent « Sécurité » suite à l'exercice

L'exercice est réalisé techniquement sans prévenir les cibles…

Le scénario considéré est le suivant :



Et sera simulé ainsi :



Ce qu'il s'est passé…

Envoi de symptômes techniques bureautiques gradués sur deux jours

Un utilisateur les supprime : Pas de réaction…

Quelques utilisateurs voient l'alerte : Pas de réaction…

Personne ne voit les fichiers : Pas de réaction !

Quelques utilisateurs voient les alertes : Pas de réaction !!

Les utilisateurs commencent à discuter…

L'incident est enfin qualifié et remonté correctement !

Stimulations par téléphone, graduées, sur un jour

L'utilisateur ne voit rien…

L'utilisateur supprime les fichiers : pas de remontée d'alerte !

L'utilisateur prévient son manager…

L'utilisateur remonte l'alerte…

Un exercice de crise cybercriminalité
Quel bilan tirer de cet exercice ?

	Points forts	Axes d'amélioration
Détection et qualification de l'incident	▪ L'incident sécurité a été **détecté et qualifié** par les utilisateurs ciblés	▪ **Seuls les signaux forts ont suscité une réaction** des utilisateurs, à la fois côté serveur et bureautique
Remontée d'alerte sécurité	▪ **Réaction positive** des utilisateurs ciblés qui ont bien **remonté les alertes**	▪ Il a fallu **un temps de réaction** avant la remontée ▪ Certaines remontées **ne sont pas prévues par les procédures de remontée d'alerte sécurité**
Réaction et application des bonnes pratiques sécurité	▪ Les utilisateurs ont eu **certains bons réflexes face aux attaques** (regarder les logs de connexions, investiguer sur l'incident)	▪ Une partie des actions menées est **contraire aux bonnes pratiques** (suppression de fichiers impliquant la suppression de certaines traces utiles)

Deux attitudes…

Anticipation

Mise en place de dispositifs de gestion de crise spécifiques cybercriminalité

Entrainement

Conduite de tests « cybercriminalité » pour éprouver ces dispositifs

The power of simplicity
«Ce qui est simple est fort»

www.solucom.fr

Contact

Raphaël BRUN

Consultant senior

Tel : +33 (0)1 49 03 26 65

Mobile : +33 (0)6 10 38 03 00

Mail : raphael.brun@solucom.fr