

Procédure



Gestion d'un incident utilisateur

Sommaire

1. Introduction	3
1.1. Objet de la procédure	3
1.2. Domaine d'application	3
1.3. Matrice des priorités	3
1.4. Priorité	3
1.5. Modes d'ouverture d'un incident	4
1.6. Cycle de vie d'un incident	4
2. Description des activités Incident	4
2.1. Ticket Event :	4
2.2. Ticket Utilisateur :	4
2.3. Communication via les tickets	5
2.4. Logigramme Incident	6
3. Description des activités Incident Majeur	6
3.1. Ticket P1/Incident Majeur	6
3.2. Logigramme incident P1/majeur	8
4. Description des activités Gestion Crise (Escalade Managériale)	9
4.1. Traitement de l'escalade managériale opérationnelle en heures ouvrées (HO)	10
4.2. Escalade managériale opérationnelle en Heures Non Ouvrées (HNO)	10
4.3. Composition de la cellule de crise	10
4.4. Critères d'activation	11
4.5. Logistique	11
4.6. Chronogramme déclenchement de crise	12
<i>Il s'agit d'une estimation (en partant du principe que la coupure arrive juste après le passage de la sonde de supervision)</i>	12
4.7. RACI	13
4.8. RCA /REX/FFT	13

1. Introduction

1.1. Objet de la procédure

L'objet de ce document est de décrire les différentes étapes permettant la résolution de l'incident et d'un incident majeur(crise).

Le but premier du processus de la gestion des incidents est de rétablir le fonctionnement du service dans un état "nominal" aussi vite que possible et minimiser l'impact sur la production et le business, tout en assurant le maintien de la qualité et de la disponibilité du service.

1.2. Domaine d'application

Cette procédure est applicable pour tout dysfonctionnement remonté par un utilisateur ou l'alerting.

Le processus doit fournir au client assistance et support lorsque se produit un événement anormal causant une perturbation ou une interruption de service.

La gestion d'incident :

- Enregistre, et gère les incidents jusqu'à leur clôture après résolution.
- Résout tous les incidents par priorité selon les codes de priorité.

1.3. Matrice des priorités

		Impact		
		élevé	moyen	faible
Urgence	élevée	1	2	3
	moyenne	2	3	4
	faible	3	4	5

1.4. Priorité

Priorité/Niveau service	Gold	Sliver	Bronze
P1	2h	4h	8h

P2	4h	8h	2jours
P3	8h	2jours	5 jours

1.5. Modes d'ouverture d'un incident

Via l'interfaçage Opsgénie :

- Le ticket créé par le client dans Opsgénie
- Il est ouvert automatiquement par les outils de supervision

Le ticket ouvert, l'équipe TDP s'affecte le ticket et le traite selon la priorité.

1.6. Cycle de vie d'un incident

L'équipe TDP à 15 mn pour le niveau service Gold la prise en compte, 30 min pour le niveau Silver et 60 min pour les Bronze.

Les investigations peuvent nécessiter des informations complémentaires du client. Le ticket est mis à l'état "En attente" tant que l'équipe TDP attend le retour du client.

De même, lorsque la résolution de l'incident nécessite l'intervention d'une tierce partie.

Lorsque l'incident est résolu le ticket est mis à l'état "résolu".

2. Description des activités Incident

2.1. Ticket Event :

Ouverture d'un ticket par l'outil de supervision (Prometheus ou Dynatrace) dans Opsgénie.

Le ticket est ouvert avec les informations nécessaires au traitement et la priorité adéquate.

Le traitement de ces tickets est identique à celui des tickets utilisateurs (voir ci-dessous).

2.2. Ticket Utilisateur :

Ouverture d'un ticket par l'utilisateur via Opsgénie.

Il est demandé que le ticket fasse part des informations suivantes :

- Titre
- Catégoriser le type d'incident
- Décrire le plus précisément possible le dysfonctionnement (Date et heure constaté, Nom de l'application ou Machine, symptômes constatés)

- Décrire les actions ayant menées au dysfonctionnement constaté (si cela est possible)
- Évaluer l'impact et la priorité de l'incident en fonction des caractéristiques.

L'équipe TDP analyse l'incident et décrit les activités réalisées. En cas d'Incident Majeur, il applique la procédure de gestion d'un Incident Majeur (Ci-dessous 26.1 Ticket P1/Incident Majeur).

En cas de besoin d'information complémentaire, il le mentionne dans le ticket et en modifie le statut du ticket en « Pending » et avertit l'incident manager.

Quand l'équipe TDP résout l'incident, il ferme le ticket en documentant la résolution

Lors de la résolution, si une évolution des consignes est nécessaire, il documente ces consignes pour l'équipe.

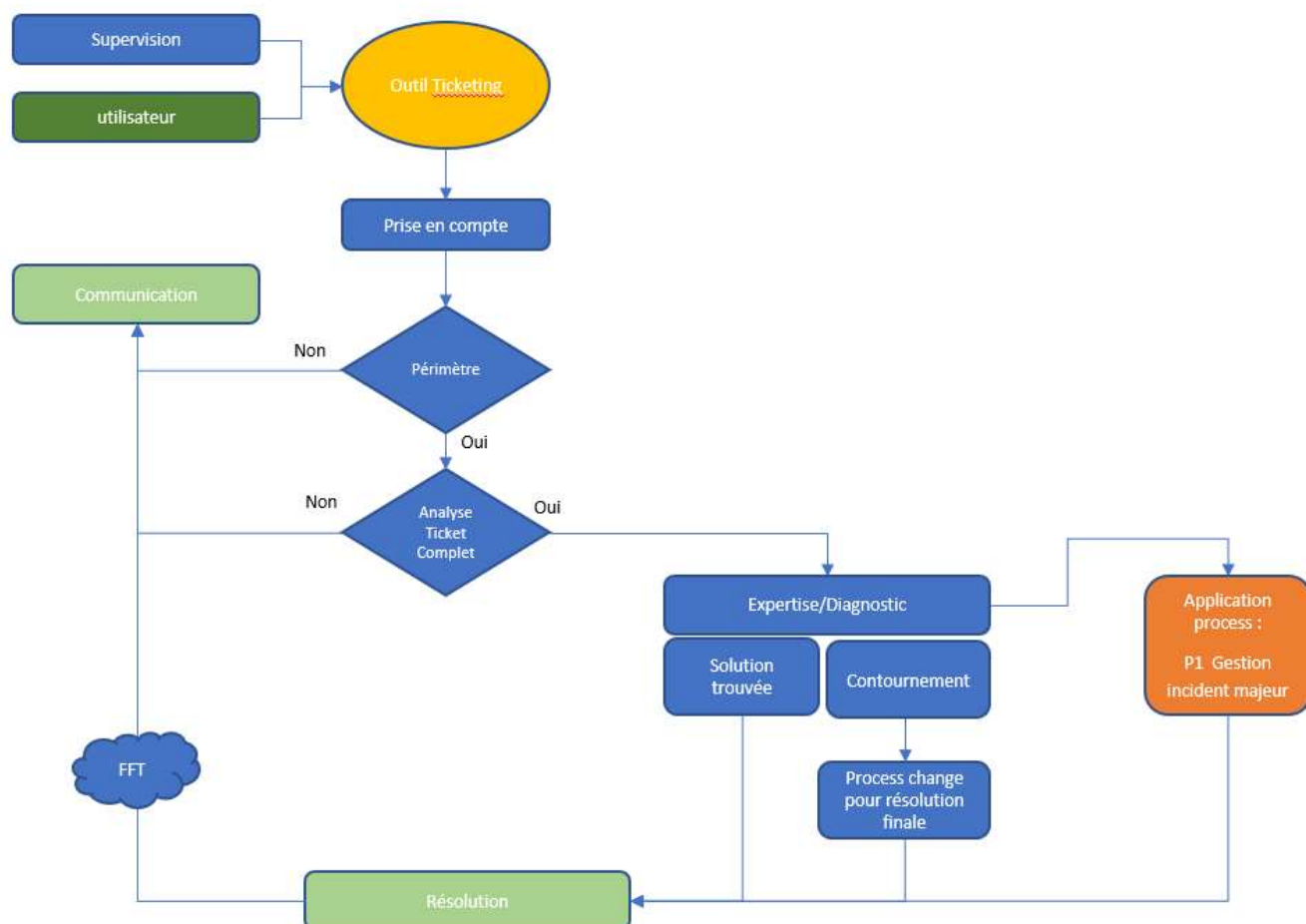
En cas d'incident récurrent ou de cause inconnue, il soumet à l'incident manager la proposition d'ouvrir un problème qui sera ensuite géré d'après le process de gestion des problèmes.

2.3. Communication via les tickets

Le ticket est mis à jour + envoi de mail aux demandeurs afin de partager

2.4. Logigramme Incident

Logigramme process incident



3. Description des activités Incident Majeur

3.1. Ticket P1/Incident Majeur

Un ticket catégorisé P1 généré par la supervision ou par un utilisateur, sera traité en priorité par l'équipe TDP.

- En cas d'incident P1 non avéré, le ticket est recatégorisé manuellement.
- En cas d'incident P1 avéré, l'incident fait l'objet :

Communications régulières par email de l'incident manager vers le client

- En cas d'incident P1 Majeur avéré, l'incident fait l'objet :
 - Déclenchement du process de crise (voir ci-dessous paragraphe 5)
 - Avertissement et déclenchement de tous les acteurs

Ouverture d'un call de crise

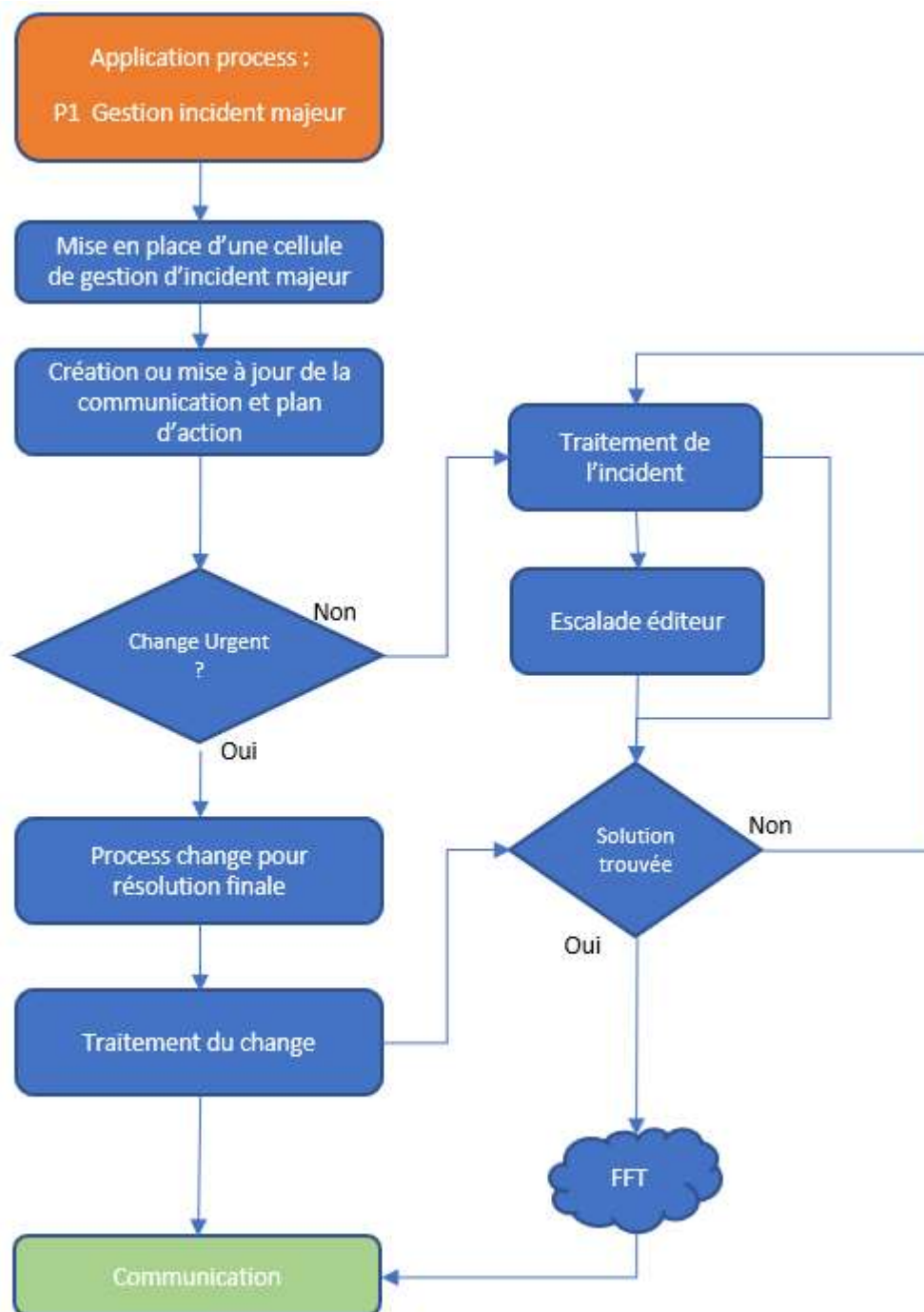
Communication régulière par email toutes les 1h (minimum) selon le plan de communication défini en call de crise

Si nécessaire, le processus de changement urgent est déclenché

Une communication de fin d'incident est envoyée en fin d'incident.

Une revue d'incident majeur est réalisée post mortem puis un rapport d'incident est transmis aux parties concernées.

3.2. Logigramme incident P1/majeur



4. Description des activités Gestion Crise (Escalade Managériale)

Le processus de Gestion des Crises s'applique en cas de détection avérée ou de forte probabilité d'une rupture majeure de service technique ou organisationnel ou de non-respect d'un engagement contractuel sur tout ou partie du SI client ou de l'infrastructure.

Elle a pour objet de mobiliser dans un ordre hiérarchique préétabli les acteurs disposant du pouvoir de décision (membres de la gouvernance du Contrat et des directions de production respectives) nécessaire à l'évaluation collégiale :

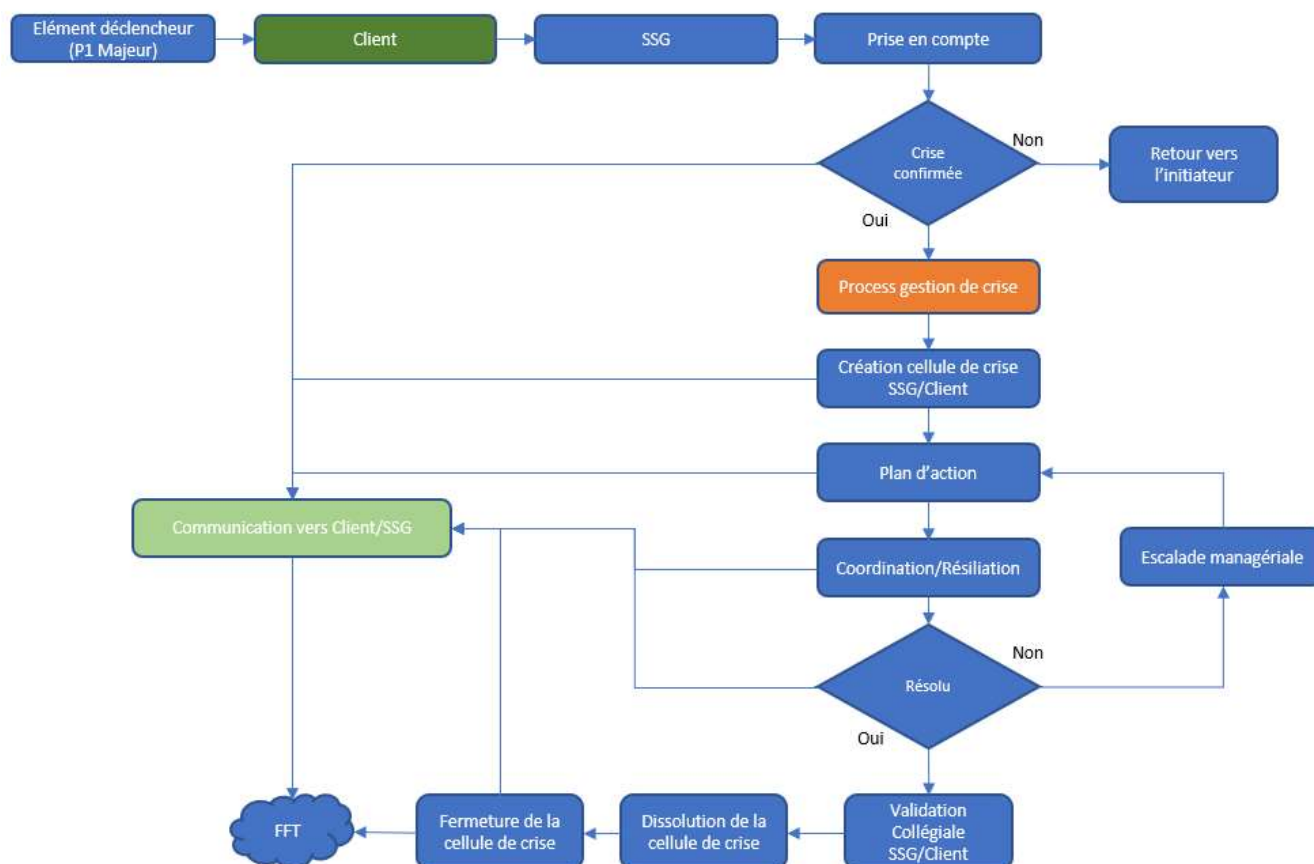
Des impacts et des besoins

Du plan d'action et de la mobilisation des moyens appropriés.

La gestion d'une crise déclenchée par l'infogérant jusqu'à sa clôture est de la responsabilité du Delivery Manager.

La gestion d'une crise déclenchée par client jusqu'à sa clôture est de la responsabilité de client

Vous trouverez ci-dessous le logigramme :



4.1. Traitement de l'escalade managériale opérationnelle en heures ouvrées (HO)

Le processus d'escalade managériale permet de transmettre et de partager les informations afin de prendre les mesures opérationnelles adéquates pouvant minimiser voire supprimer les conséquences d'un risque de dysfonctionnement ou d'un dysfonctionnement avéré et de rétablir le fonctionnement nominal des services. Dans le cadre de la gestion d'un incident, l'escalade managériale de l'infogérant peut être déclenchée par toutes les parties

Elle s'appuie sur trois niveaux d'escalade, chaque niveau déclenchant le niveau supérieur si nécessaire.

La matrice d'escalade contient les points de contact du client et de l'infogérant et des partenaires identifiés. Elle s'applique pour les jours et heures ouvrés (HO)

Elle est maintenue par le delivery manager et les mises à jour sont fournies par :

Le delivery pour les informations relatives à l'infogérant ;

Les responsables client pour les informations relatives au périmètre de responsabilité client

Les mises à jour sont validées lors du comité contractuel. Une nouvelle version du fichier est alors créée et mise à disposition.

4.2. Escalade managériale opérationnelle en Heures Non Ouvrées (HNO)

En cas d'incident P1 en HNO, Opsgénie déclenche l'astreinte technique de l'infogérant.

S'il apparaît que la résolution ne sera pas évidente ou qu'elle interviendra hors délai, une escalade managériale en HNO sera déclenchée mais elle ne s'appuie que sur deux niveaux en interne infogérant et un manager d'astreinte Client (dans le cas où cela est possible)

Les rotations d'astreintes sont renseignées chaque semaine a minima 1 jour avant le début d'un nouveau cycle d'astreinte.

4.3. Composition de la cellule de crise

Les rôles des participants à la cellule de crise sont de prendre pour leurs domaines de responsabilité les décisions de pilotage indispensables, de réquisition des ressources et d'organiser la communication autour de l'événement.

Membres permanents	Infogérant	Client
--------------------	------------	--------

Représentants groupes de compétences	Référents techniques	N/A
Pilote de la Cellule de crise	Incident Manager / Delivery Manager	Management N1 client
Représentant de la Relation Client (si niveau activé)	Directeur de Compte	Management N2 client
Direction (si niveau activé)	Directeur d'agence	Management N3 client
Membres facultatifs	Infogérant	Client
Experts/Archi	Experts/Arch techniques	Experts techniques
Sécurité	CSO et/ou RSO et/ou RSSI	RSSI

4.4. Critères d'activation

La cellule de crise doit être contactée et réunie à chaque événement de type (liste non exhaustive) :

- Tout incident MAJEUR de type : Blocage applicatif critique, attaque virale, destruction etc ...
- Indisponibilité complète et massive de l'infrastructure ou d'une partie critique pour le client
- Autres événements. Pour exemple :
 - Catastrophe naturelle limitant ou interdisant les accès aux locaux,
 - Mouvement humain ou social limitant ou interdisant les accès aux locaux,
 - Acte d'agression, de malveillance ou de terrorisme.
 - Etc ...

4.5. Logistique

La communication vers les opérationnels est réalisée par l'incident Manager et se déroule en trois parties :

- Ouverture de la crise : envoi par e-mail (hors incident messagerie) de la notification d'ouverture de la crise aux membres permanents de la cellule de crise. En cas de doute raisonnable sur un aspect
- Sécurité, contacter également les équipes sécurité.
- Un call est créé et communiqué aux acteurs.
- Traitement de la crise : selon la criticité déterminée collégialement, envoi par e-mail à fréquence régulière du statut d'avancement des opérations aux membres permanents de la cellule et aux membres facultatifs intervenants dans la résolution, communication sur la Conf-Call.
- Clôture de la crise : envoi par e-mail de la notification de clôture de la crise aux membres permanents de la cellule de crise et aux responsables opérationnels acteurs sur le traitement.

4.6. Chronogramme déclenchement de crise

Il s'agit d'une estimation dans l'hypothèse où la coupure intervient juste après le passage de la sonde de supervision. Ce délai peut aller jusqu'à 5 minutes au maximum (fréquence de monitoring).

T0	Incident P1 de type coupure de service ou forte perturbation du service (qui ne permet pas aux utilisateurs de se connecter ou utiliser l'appliquatif normalement)
T0 + 5 min	Ouverture de ticket
T0 + 15 min	Prise en compte du ticket + analyse + tentative de résolution
T0 + 30 min	Escalade à incident manager Infogérant Communication vers la DNUM de l'ouverture d'un incident P1
T0 + 45 min	Communication vers la DNUM afin de déclencher la cellule de crise
T0 + 1h00 min	Ouverture de la cellule de crise Infogérant/MTE <ul style="list-style-type: none"> • Description de l'incident • Les actions réalisées depuis le début • Prévision d'une résolution possible ou non • Plan d'action à définir • Validation du déclenchement du PRA ou non • Communication toutes les heures
T0 + 1h30	Communication vers MTE/Infogérant sur le plan d'action et son suivi
Une communication par mail est réalisée toutes les heures : <ul style="list-style-type: none"> • Avancement • Actions réalisées • Reste à faire 	
T0 + 3h30	<i>En cas de déclenchement du PRA à max T0 +1h30</i> Rétablissement du service aux utilisateurs avec encore des actions cotés Infogérant
T0 + 5h30	Communication de clôture et fin de la gestion de crise

4.7. RACI

Responsabilités / Activités	Manager Infogérant	Admin Infogérant	Client
Pilotage de l'escalade managériale (périmètre Infogérant)	A, R		C
Validation situation de crise	A, R	R	R
Pilotage de la cellule de crise (périmètre Infogérant)	A, R	I	I
Pilotage de la cellule de crise (périmètre Client)	C	I	A, R
Communication opérationnelle	A, R	I	I
Communication clients finaux /Hiérarchie	I, C	I	A, R
Mobilisation des équipes techniques Infogérant	A, R	R	I
Mobilisation des équipes Client	I	I	A, R
Validation solution acceptable ou retour au nominal	R	I	A, R
Clôture de l'escalade managériale ou de la crise (périmètre Infogérant)	A, R	I	I
Clôture de l'escalade managériale ou de la crise (périmètre Client)	I	I	A, R

R = Responsable (réalisé), A = Accountable (responsable), C = Consulted, I = Informed

4.8. RCA /REX/FFT

A la suite d'un incident majeur ou d'une crise, un rapport d'incident est rédigé afin de capitaliser sur l'expérience.

- Rédaction par l'Incident manager d'un compte-rendu synthétique mais précis diffusé de manière restreinte afin d'acter les décisions retenues et de tracer le suivi des actions notamment à travers la gestion des changements, la fiche de faits techniques en est un composant,
- Capitalisation sur la conduite de la crise : analyse point fort, point faible, plan d'action à suivre en comité de production, plan d'amélioration du processus.
- Fourniture de la version finale du REX sous 5 jours ouvrés.