Plan de Continuité d'Activité
Démarche globale

Emmanuel BESLUAU

Vision d'ensemble du PCA

Appréciation des risques PCA
- pour les réduire si besoin
- quels scénarios de sinistre ?
- quelles alertes ?

Business Impact Analysis
- quels processus critiques ?
- quelle durée d'interruption ?
- quels modes dégradés ?
- quels moyens ?

Stratégie de continuité :
Face à tel scénario de sinistre : comment poursuit-on les processus critiques ? Comment se protéger ? Que faut-il préparer ?

Préparation

Missions PRA et responsables

Dispositif de pilotage de la crise

Suite de tâches PRA à exécuter par étapes

Exercices, tests, MCO

Formation et sensibilisation

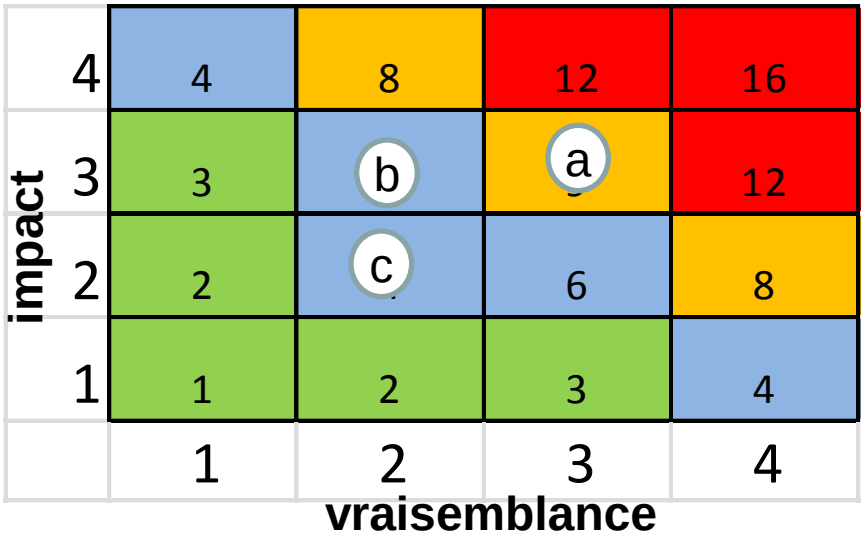
Exécution

Gouvernance – Politique - Audit

Risque : Exemple (extrait)

Type de sinistre identifiés site XXX	Impact	Vraisembl.	Gravité	*justifications et explication des analyses et appréciations*
Industriels	**I**	**V**	**G**	**commentaires / explications**
Accident centrale nucléaire	1	1		Centrale de Nogent sur Seine, la plus proche à plus de 100 km
Accident industriel extrême	1	2		les zones à risques sont hors de Paris (Nanterre, Genevilliers)
Sinistre de type Seveso	1	2		idem N°2
Incendie et pollution liés au voisinage	2	2		présence de stockage d'hydrocarbure proche ; mais sous contrôle ; éventuellement évacuation une demie journée
Rayonnement électromagnétique (radars, haute tension, etc.)	so	so		a priori sans objet
Fuite de gaz	1	2		impact éventuel : difficulté pour certains personnels sur le trajet travail-domicile ; évacuation des locaux une demie journée
Explosion de gazoduc	1	1		les zones à risques sont éloignées ; impact éventuel : difficulté pour certains personnels sur le trajet travail-domicile
Chute d'avion	3	2		normalement : contournement de Paris ; exposition en tant qu'immeuble de grande hauteur
Pollution suite à accident de transport de matières dangereuses	2	2		proche voie ferré mais voyageurs ; éventuellement problème en périphérie de Paris : trajet domicile travail
Naturels				
Inondation, crue centennale, rupture de barrage	2	2		Montparnasse en point haut ; impact pour les trajets domicile-travail des collaborateurs
Séisme	1	2		Paris en zone de sismicité "très faible" (1/5)
Sinistre kéraunique élevé (impact foudre)	2	2		niveau kéraunique à 15 dans le département (assez faible) (source : énergie-foudre) ; IGH protégé ; impact en coupure temporaire de courant
Tempête, ouragan	2	2		difficultés éventuelles sur le trajet travail-domicile
Neige, verglas	2	2		neige en 1996 ; difficultés sur le trajet travail-domicile
Pluie diluvienne	2	2		effet sur le terrain plus proche de la Seine ; difficultés sur le trajet travail-domicile
Dégâts provoqués par des rongeurs	2	1		impacts en coupure de courant ou réseau ; a priori non et pièges à souris dans les parkings
Glissement de terrain, éboulement, risque minier	2	2		risque cité par les documents de la mairie ; immeuble dans la zone ; construit en ???
Environnementaux (hors site)				
Voisinage hostile	1	1		zone mixte bureaux / habitation calme
Légionellose (aéroréfrigérants)	2	1		contrôles trimestriels faits avec propriétaires
Arrêt électrique et non approvisionnement en carburant	2	2		les locaux techniques d'étages et le local serveur sont protégés par deux onduleurs redondants et groupe électrogène ???l x jours) et connexion groupe électrogène
Arrêt télécom logique	3	1		Contrat télécom type MPLS. GTR 4 heures S1 (donc 24/7). ???
Arrêt télécom physique	3	2		accès télécom groupés dans un local spécial spécial ; demande au propriétaire. Fibre optique en redondance et passage par deux cheminements différents.
Attentat de grande ampleur (nucléaire, biochimique, etc.)	3	2		type d'attentat peu vraisemblable en fonction de l'environnement et du site ; pourrait viser la gare Montparnasse
Attentat sur une cible terroriste proche (explosif)	3	2		Peut viser les sites ?? proches mais pas ABCD spécifiquement
Attentat ciblé sur votre entreprise	3	1		ABCD peu connue et cible peu vraisemblable ; agents de sécurité en entrée ; porte parking avec badge
Attaque par un forcené armé	4	2		absence de contrôle des accès physiques en entrée principale ; Existence de menaces reçues. Pas de PC sécurité sur le site

Exemple de grille d'évaluation



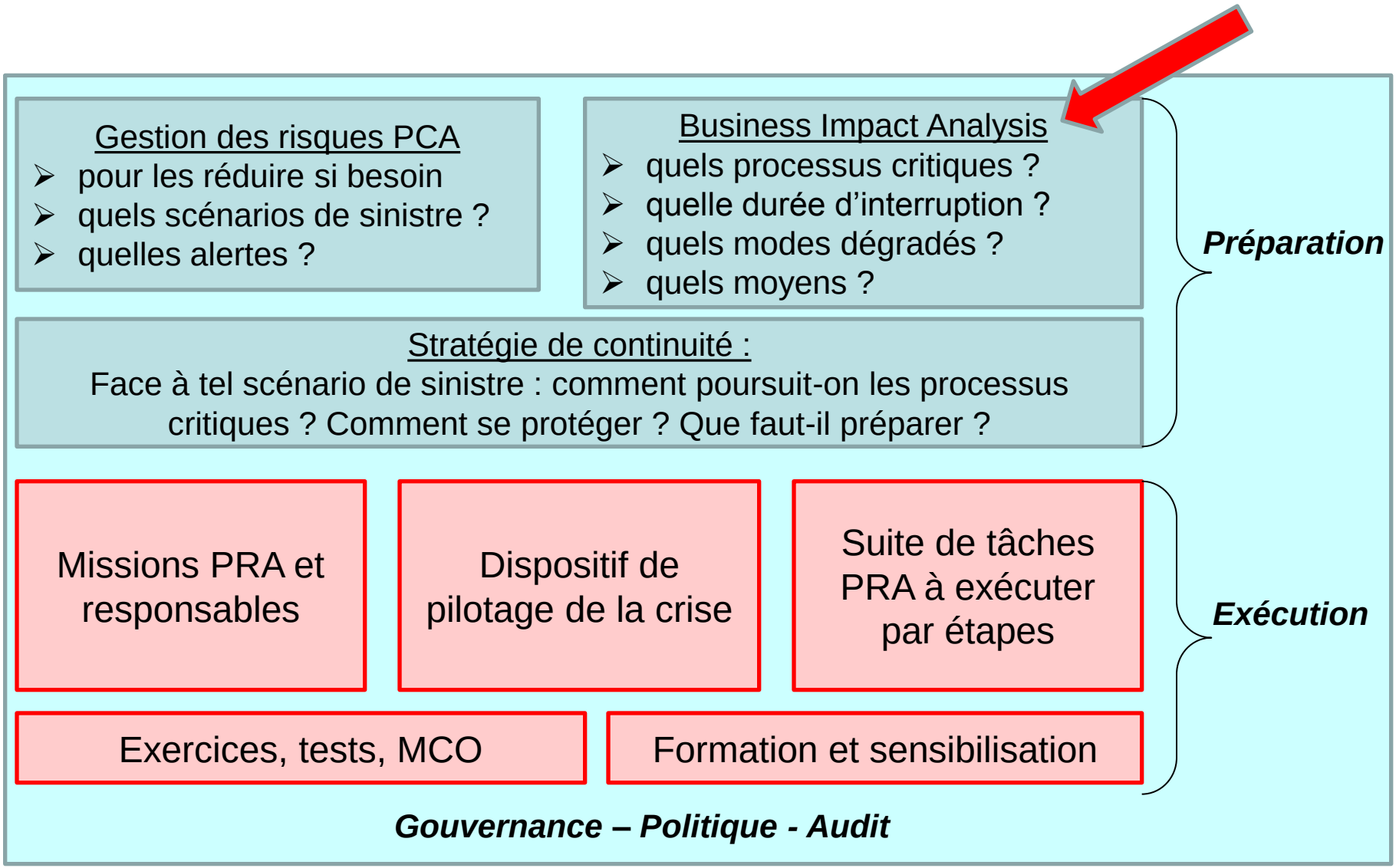
	à supprimer très CT
	à réduire CT
	à réduire MT
	acceptable

		I	*V*	*G*
a	inondation	3	3	9
b	transport de matières dangereuses	3	2	6
c	incendie dû au voisinage	2	2	4

Evaluation de quatre options :

- Accepter le risque
  - s'il est faible
  - si les autres options sont trop onéreuses
- Éviter ou supprimer le risque
  - idéal mais souvent très cher
- Réduire le risque
  - en jouant sur les paramètres du risque
  - plan d'actions d'amélioration
- Transférer ou partager le risque
  - à une compagnie d'assurance
  - à un prestataire externe

➢ Attention à utiliser une méthode efficace



BIA : Objectif

- Déterminer les activités prioritaires en analysant les divers impacts de leur disparition
- Pour cela, il faut :
  - cerner les activités (métier, bon niveau de maille)
  - évaluer les impacts d'un arrêt (k€, image, violation...)
  - en déduire les activités 'prioritaires ou critiques'
- Pour les activités jugées critiques, il faut :
  - lister les contraintes de reprises : DMIA et PDMA
  - évaluer les exigences sur les moyens

➢ Le BIA est au cœur de la démarche !

Phase 2 : Analyser les processus

Et.2 : estimer les impacts financiers et opérationnels

Entité :		Impact évalué				
Processus	Durée d'arrêt	Financier	Image	Contrat	Règlement	DMIA
Gérer la relation client	< 1 h	1	1	1	1	1 j
	> 1h & < 4h	1	2	2	2	
	> 4h & <1 j	**2**	**3**	**3**	**3**	
	au-delà	3	3	3	3	
Réclamation client 1212	< 0,5 h		2	2	3	1 h
	> 0.5h &		**3**	**3**	**3**	
			3	3	3	
Gérer le recouvrement client			1	1	1	5 j
			1	2	2	
	> < 5j	**3**	**1**	**2**	**3**	
	au-delà	3	2	3	3	
Rétablissement client sous 24 heures	< 2 h	1	1	1	1	1 j
	> 2h & < 4h	2	2	1	1	
	> 4h & <1 j	**2**	**3**	**3**	**3**	
Gérer les ventes en ligne	< 3 j	2	2	1	2	4 j
	> 3 j & < 4j	**3**	**3**	**3**	**3**	

Exemple

Phase 4: Déterminer les paramètres de reprise

Etape 3 : procédures de secours pour processus critiques

- « existe-t-il des procédures ou des actions de contournement pour votre processus en cas de sinistre ? »

- « lister les activités ou travaux non couverts par ces procédures de contournement et qu'il serait nécessaire de prendre en compte »

De l'utilité du BIA

- Se focaliser plus sur les fins que sur les moyens
- Connaître ce qui est « vraiment critique » dans l'entreprise
- Permettre aux gestionnaires de moyens (IT, services généraux) de gérer des priorités bien ciblées
- Développer une vision service
- « Penser interruption et sinistre »

Gestion des risques PCA
- pour les réduire si besoin
- quels scénarios de sinistre ?
- quelles alertes ?

Business Impact Analysis
- quels processus critiques ?
- quelle durée d'interruption ?
- quels modes dégr[illegible]és ?
- quels moyen[illegible]

Stratégie de continuité :
Face à tel scénario de sinistre : comment poursuit-on les processus critiques ? Comment se protéger ? Que faut-il préparer ?

Préparation

Missions PRA et responsables

Dispositif de pilotage de la crise

Suite de tâches PRA à exécuter par étapes

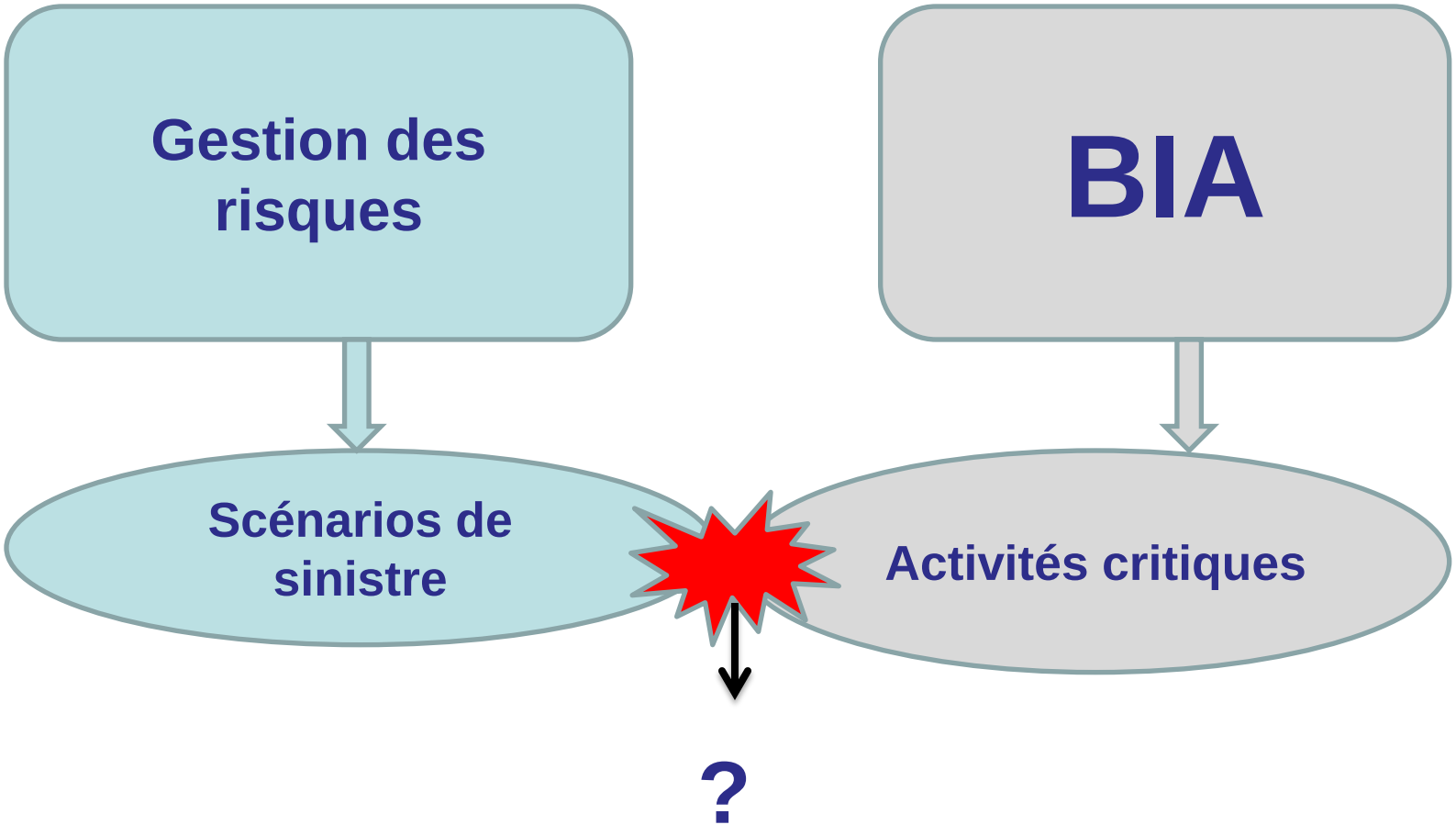
Exercices, tests, MCO

Formation et sensibilisation

Exécution

Gouvernance – Politique - Audit

Décider à l'avance :



Objectif

- Partir d'un contexte partagé :
  - les exigences identifiées en BIA,
  - les scénarios de sinistres résiduels
- Choisir les options de protection / continuité / reprise:
  - les locaux de bureaux
  - l'infrastructure et l'IT
  - la production manufacturière
  - les données et enregistrements critiques
  - les RH (ex : pandémie)
  - les transports et logistique

➢ En visant un niveau de service acceptable

Gestion des risques PCA
- pour les réduire si besoin
- quels scénarios de sinistre ?
- quelles alertes ?

Business Impact Analysis
- quels processus critiques ?
- quelle durée d'interruption ?
- quels modes dégradés ?
- quels moyens ?

Préparation

Stratégie de continuité :
Face à tel scénario de sinistre : comment poursuit-on les processus critiques ? Comment se protéger ? Que faut-il préparer ?

Missions PRA et responsables

Dispositif de pilotage de la crise

Suite de tâches PRA à exécuter par étapes

Exercices, tests, MCO

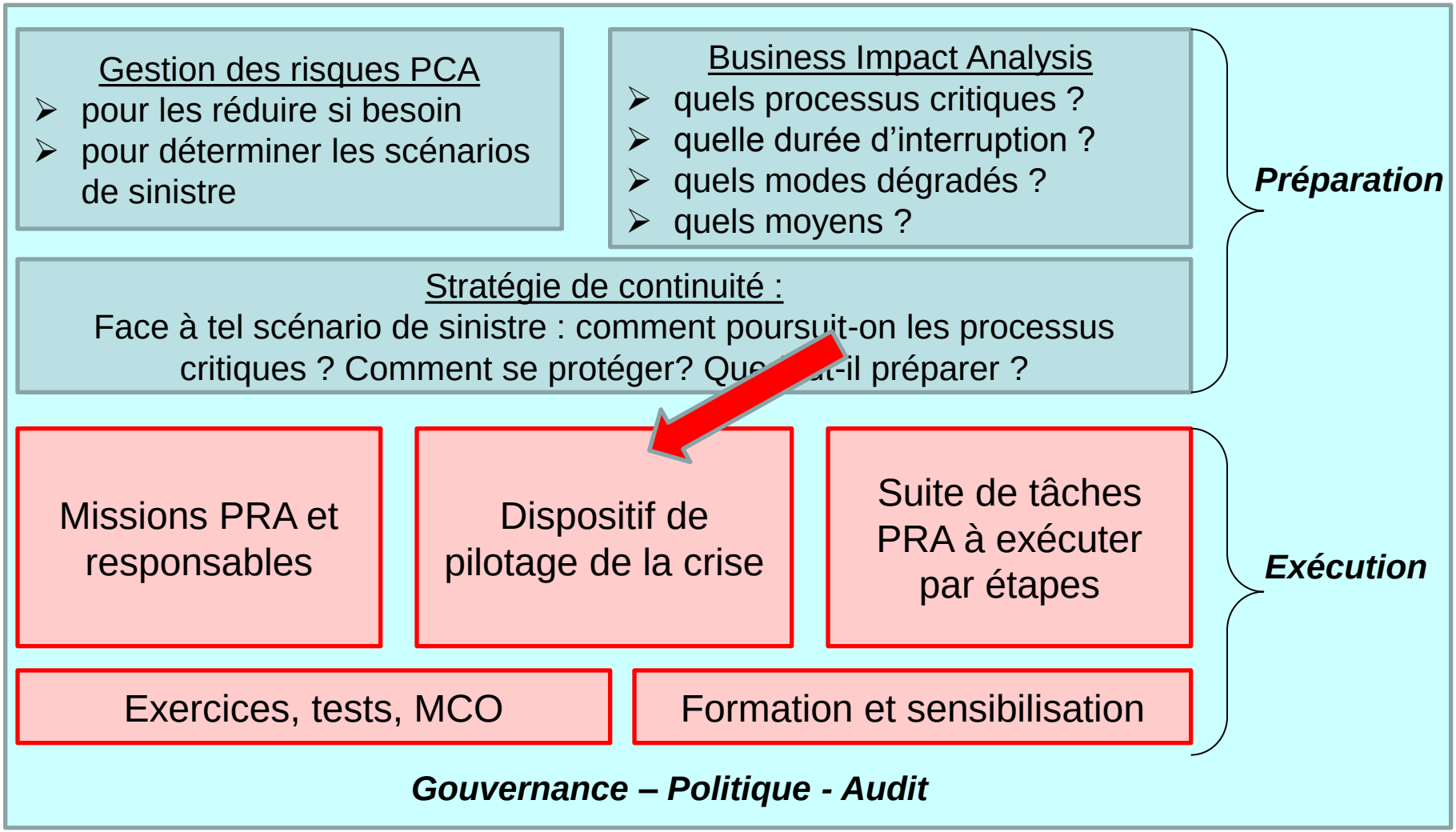
Formation et sensibilisation

Exécution

Gouvernance – Politique - Audit

Qui sera responsable de quoi ?

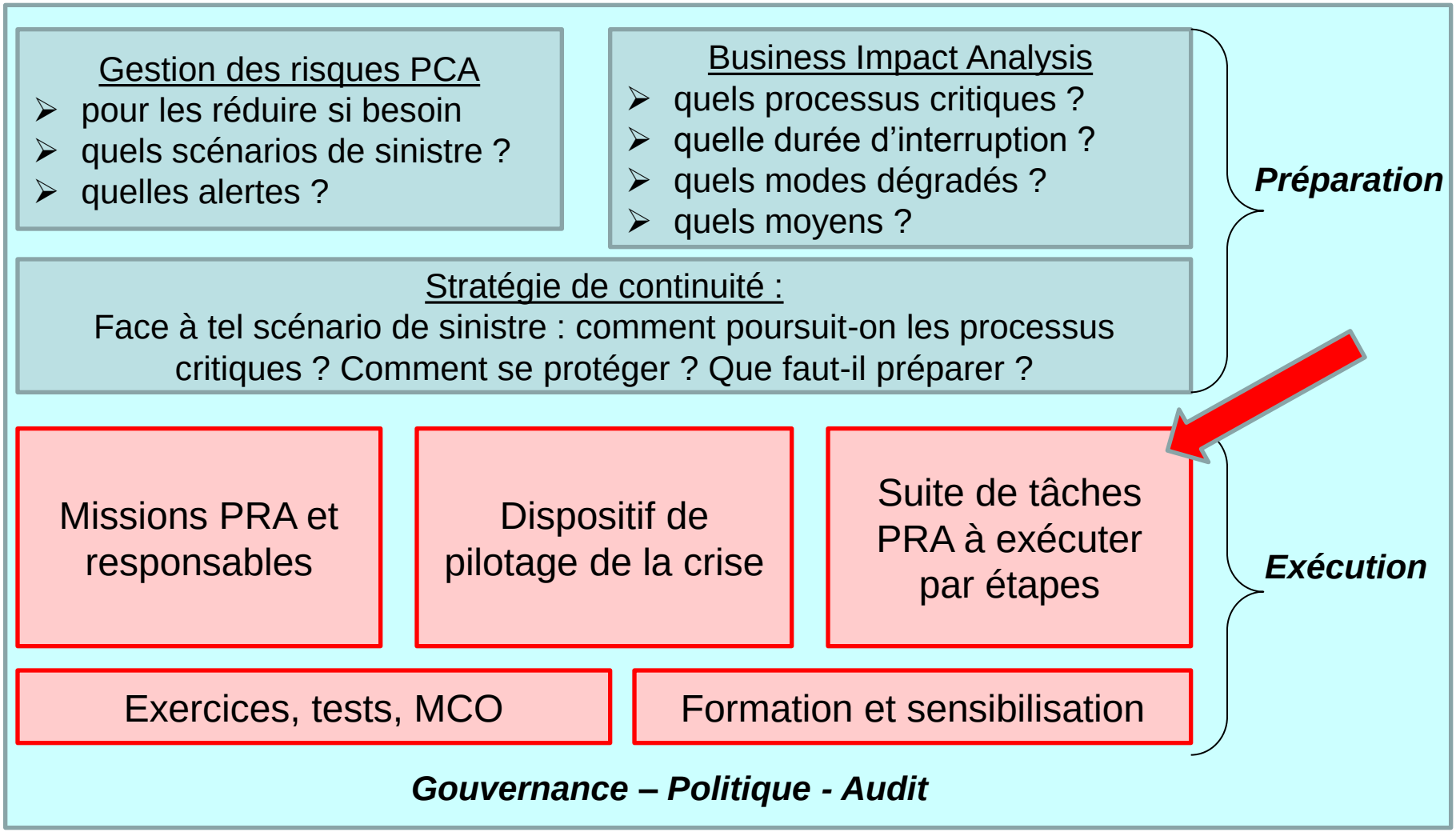
- Le groupe de gestion de crise : «état major»
  - ordonne et contrôle l'exécution du Plan
  - est responsable des interventions de secours
  - mène les actions de communication
- Le groupe de redémarrage des activités : «métiers»
  - voit et défend l'intérêt des métiers
  - est tourné vers les utilisateurs / clients
  - peut comporter des représentants spéciaux (international, classifications particulières)
- Le groupe opérationnel de récupération : «moyens»
  - est sur le terrain, proche des moyens
  - vise à récupérer et (re)mettre en ordre de marche
  - sur le site sinistré et le ou les sites de reprise,…



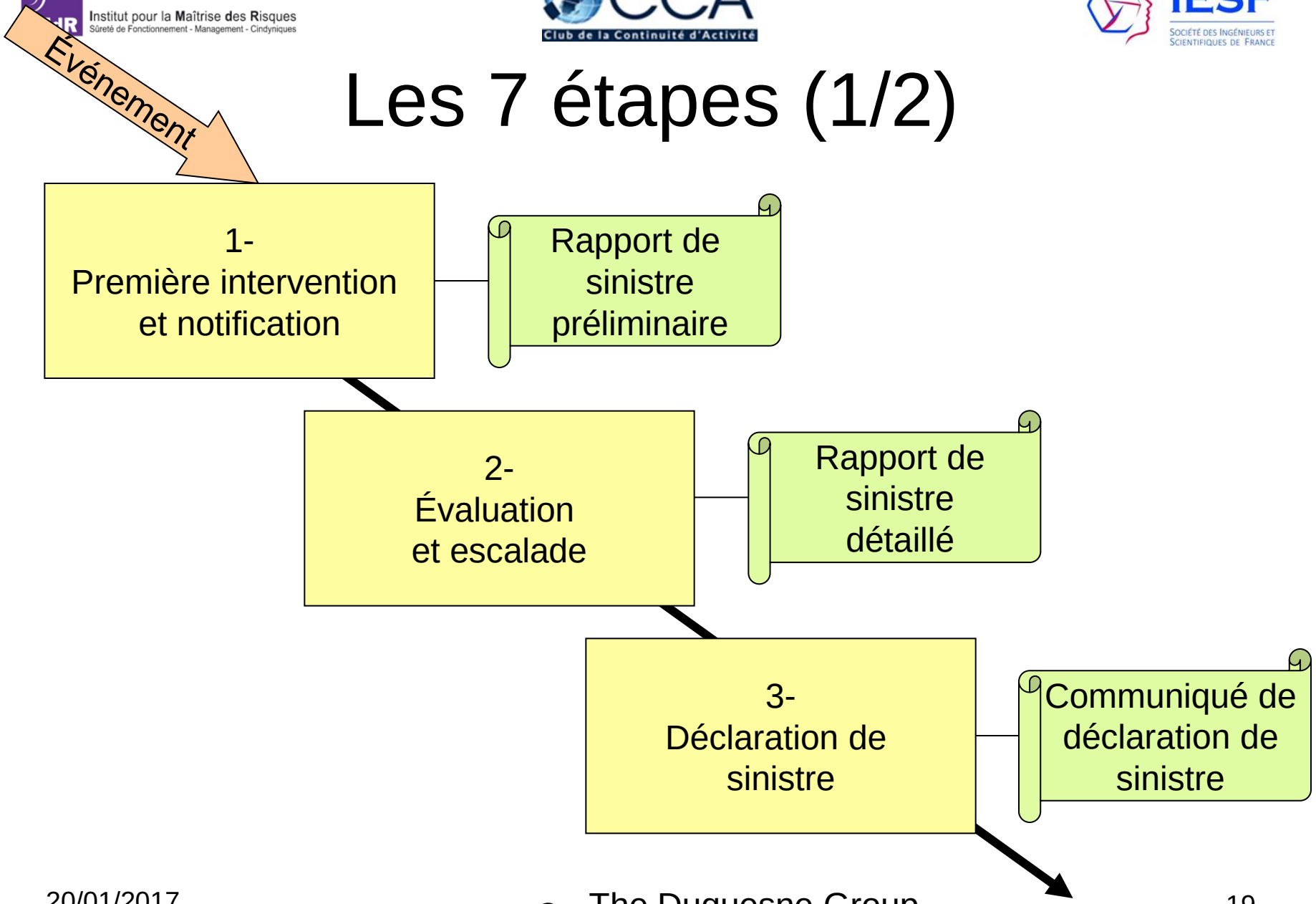
Crise : trois fonctions à mener :

- Commandement : ordonnancer les actions
  - vision centrale vs. visions locales
  - porte la responsabilité de l'entreprise
  - déclanche les plans préparés
- Contrôle et arbitrage
  - suivre les actions et les ajuster selon réel
  - arbitrage permanent sur des ressources rares
  - tenir la chronologie des événements (main courante)
- Communication
  - seule source à considérer comme fiable
  - en appel sortant uniquement
  - outils qui doivent marcher sous sinistre

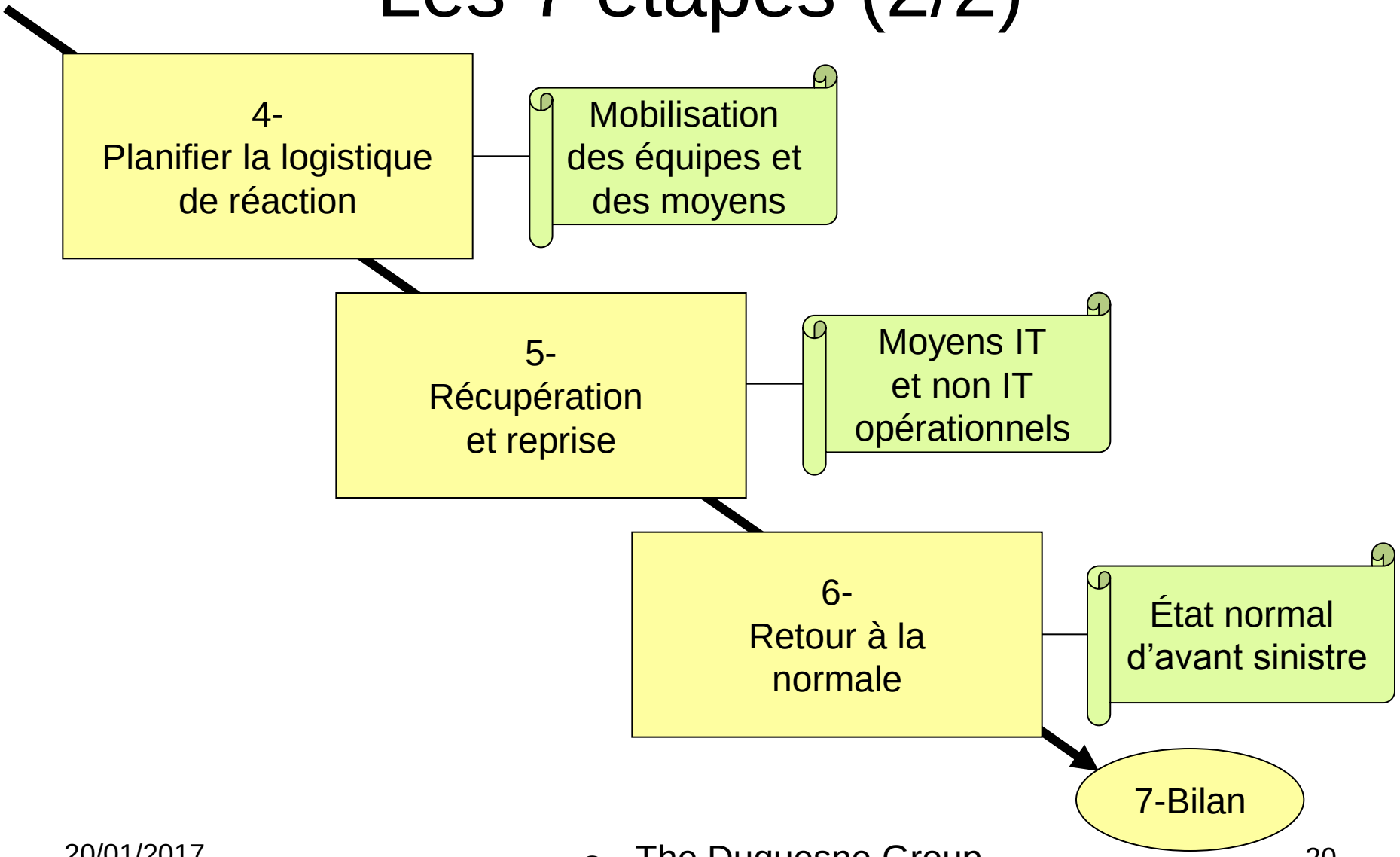
➢ Délégations de pouvoirs à faire avant !



Les 7 étapes (1/2)

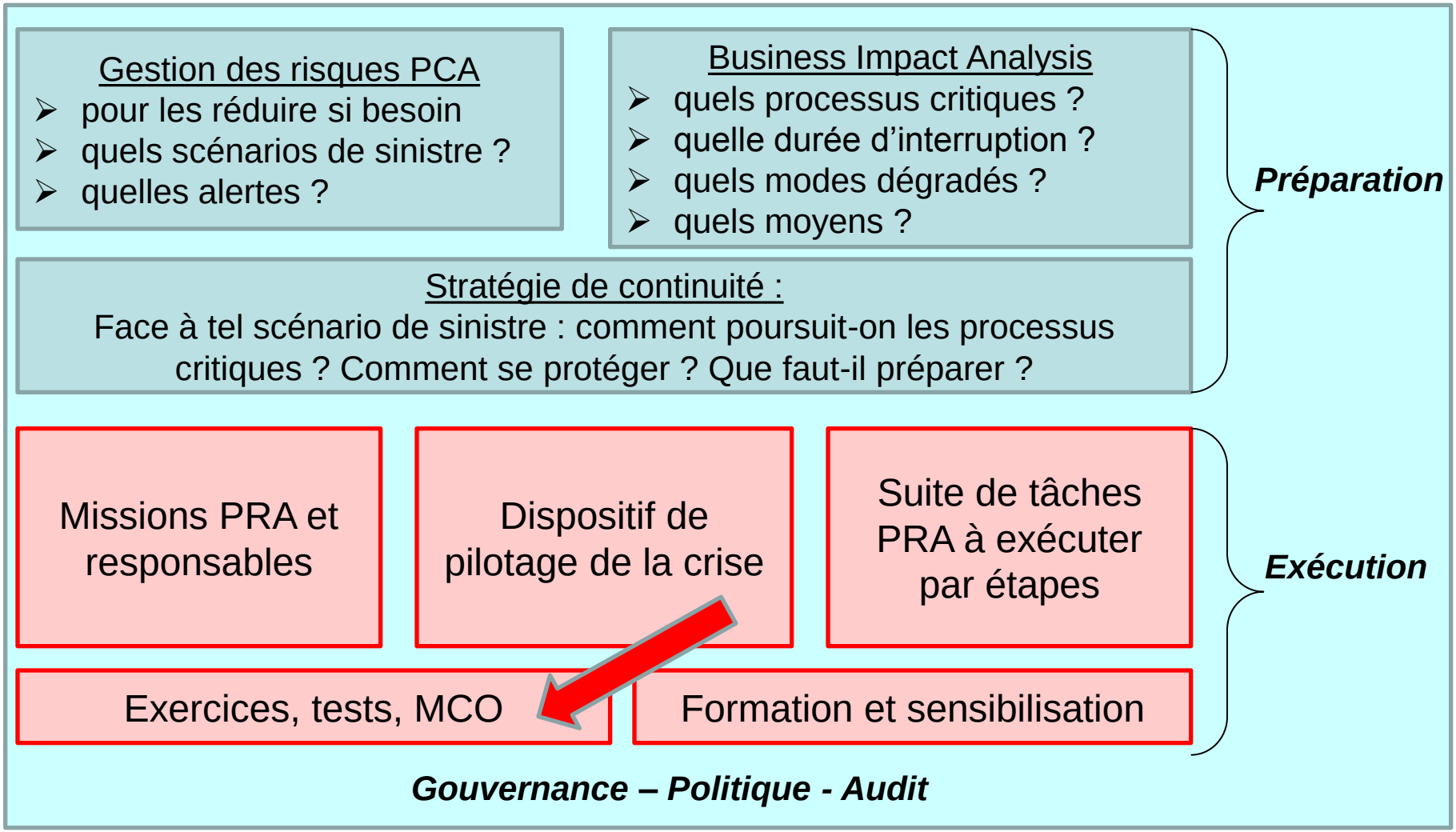


Les 7 étapes (2/2)

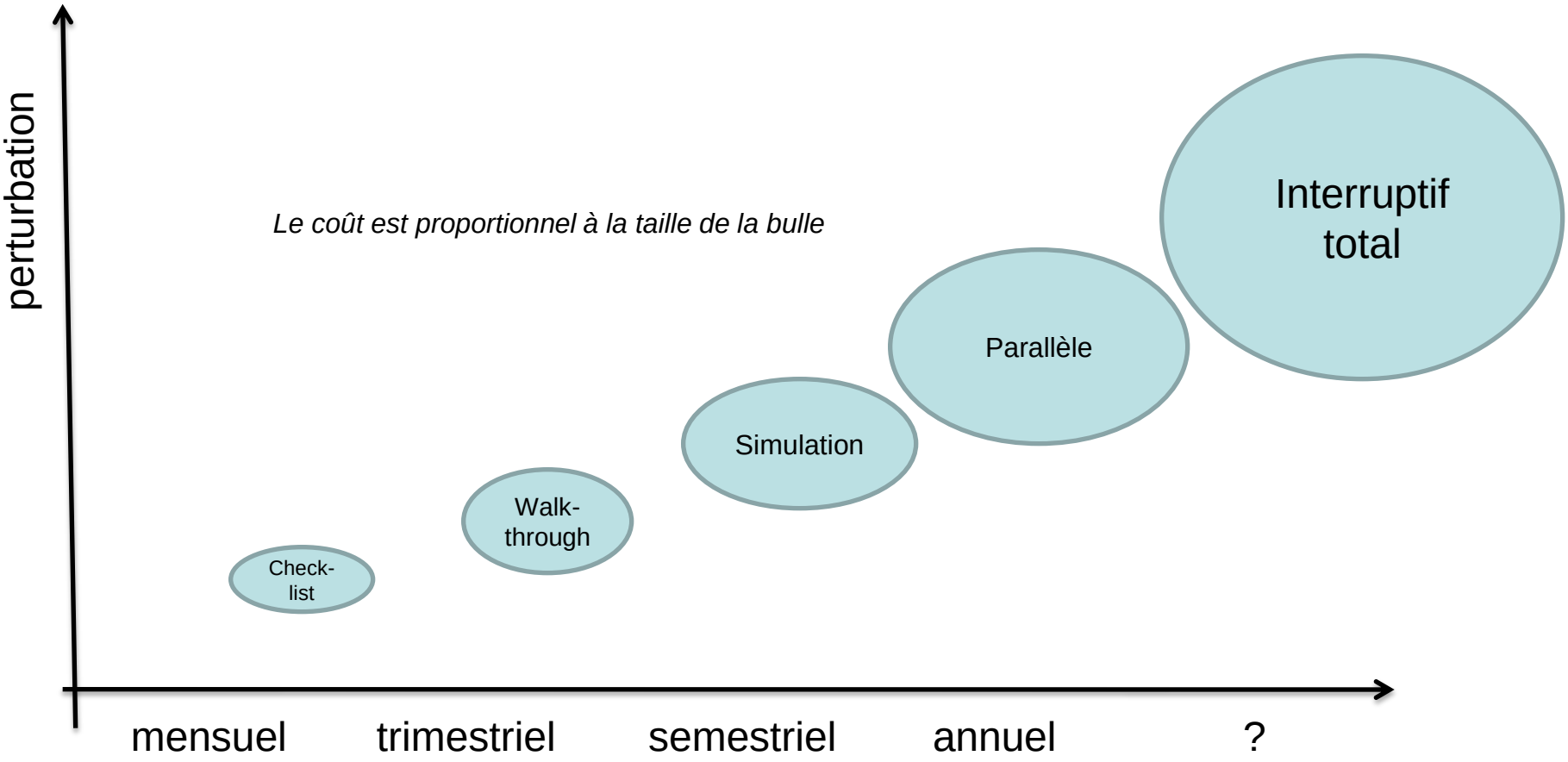


Etape 5-2

5	Actions sur le site de secours	
1	Préparer	
	1	Le groupe d'intervention est sur place et opérationnel
	2	Communiquer les paramètres (RTO, MTO, processus critiques)
	3	S'assurer que les listes d'inventaire, configuration hard+soft sont connues
	4	S'assurer que le groupe dispose des méthodes et outils de redémarrage et paramétrage
	5	Vérifier que l'infrastructure est correctement préparée (racks, câbles, énergies, connexions, …)
	6	Réceptionner ce qui arrive (hard+soft) et vérifier la conformité
	7	Prendre connaissance des consignes associées
	8	Recevoir et sécuriser les média de secours
	9	Faire un bilan 'ressources prévues'='ressources présentes' ?
	10	Planifier la suite en fonction du 9 et du Centre de gestion
	11	Vérifier les bons droits d'accès
2	Mettre en route IT et réseau	
	1	Étudier les plans d'implantation serveurs et stockage
	2	Étudier les plans réseaux et répartiteur
	3	Effectuer les montages et connexions nécessaires
	4	Initialiser et configurer serveurs et stockages
	5	Effectuer les paramétrages réseau
	6	Réaliser les interconnexions SAN, NAS, serveurs
	7	Configurer les sous-systèmes, utiliser les routines
	8	Mettre en place les protections (sécurité,…)
	9	Activer les liens avec les bureaux de secours ou autres sites à connecter
	10	Tester ce qui précède, éventuellement répéter
3	Restaurer les applications critiques	
	1	Revoir la liste des priorités
	2	Étudier les procédures d'installation et paramétrage
	3	Vérifier les droits d'accès système et administrateur
	4	Vérifier la gestion des droits d'accès des utilisateurs
	5	Restaurer ou installer les applications critiques
	6	Restaurer les données à partir des points propres prévus, vérifier leur cohérence
	7	Appliquer si c'est possible les traitements de mise à jour des données
	8	Tester les applications avec un identifiant utilisateur test
	9	Tester à partir du ou des sites des utilisateurs
	10	Prévenir les utilisateurs de la disponibilité des applications avec ou sans restriction



Coût et fréquence des tests



Bien cerner les sous-ensembles testables !

Exemple de campagne de tests

Objectifs	Méthode	Dispositif	Fréquence	Impact
actualité des listes du Plan	test check-list sur PCA	équipe RPCA	trimestrielle	nul à faible
vérifier que le CdC est opérationnel	simulation des 3 premières étapes du PRA	équipe RPCA + groupe GdC	2 par an puis annuelle	faible
viabilité du PCA site 1	walk-through du PRA sur site 1	équipe RPCA + équipe site 1	annuelle	moyen
viabilité du PCA site 2	walk-through du PRA sur site 2	équipe RPCA + équipe site 2	annuelle	moyen
viabilité du PCA site 3	walk-through du PRA sur site 3	équipe RPCA + équipe site 3	annuelle	moyen
améliorer la communication	walk-through sur Plan de Com.	équipe RPCA + Dir Com	2 par an puis annuelle	faible

Formation & sensibilisation

- Mettre en place assez vite des sessions
  - de sensibilisation de la plupart des acteurs
  - de formation des chefs de projets et contributeurs majeurs
- Maintenir la conscience ‘continuité d’activité’ éveillée *«awareness» (BCI)*
- Utiliser les exercices de tests assez tôt
  - apport pédagogique très fort des exercices

Gestion des risques PCA
- pour les réduire si besoin
- quels scénarios de sinistre ?
- quelles alertes ?

Business Impact Analysis
- quels processus critiques ?
- quelle durée d'interruption ?
- quels modes dégradés ?
- quels moyens ?

Stratégie de continuité :
Face à tel scénario de sinistre : comment poursuit-on les processus critiques ? Comment se protéger ? Que faut-il préparer ?

Préparation

Missions PRA et responsables

Dispositif de pilotage de la crise

Suite de tâches PRA à exécuter par étapes

Exercices, tests, MCO

Formation et sensibilisation

Exécution

Gouvernance – Politique - Audit

Au départ : la politique de continuité

- Document venant de la DG
  - donnant une orientation claire vers la CA
  - actant des décisions, des choix
  - distribuant les responsabilités
- Cadre général de toute action de CA
  - budget spécifique
  - comité spécial de la continuité
- Mise en place d'un dispositif
  - pour élaborer le PCA et suivre sa construction
  - puis pour le maintenir dans la durée
- Typique des normes 'système de management'

Exemple d'audit :

Copyright Duquesne Group

Bilan de l'impact sur les Activités	Situation client	Remarques : sur ce qui existe déjà en tout ou partie	Actions qui seraient utiles à faire	Signal
Déterminer les activités critiques				
Identifier et décrire les activités	fait (qualité ISO)	la description correspond au réel	OK	
Estimer les impacts financiers	en cours	actions de BIA menées dans la semaine du 4 au 8 mai 2010	poursuivre	
Estimer les impacts opérationnels				
Estimer d'autres impacts				
Lister les activités critiques	en cours			
Déterminer les configurations sous-jacentes				
MTD : Maximum Tolerable Downtime ou DIMA	en cours	actions de BIA menées dans la semaine du 4 au 8 mai 2010	poursuivre	
hiérarchiser les priorités				
description des systèmes informatiques sous-jacents				
description des applications informatiques sous-jacentes				
description des autres ressources sous-jacentes				
Déterminer les paramètres de reprise				
Recovery Time Objective et Work Recovery Time	partiellement vu	notions peu documentées	étudier sur les moyens IT	
ajustement avec le MTD ou DIMA	pas vu	catégories A et B pour les applications IT	à faire pour l'IT au moins	
RPO	vu à l'IT		approfondir sur l'existant	
procédures de mode dégradé nécessaires	partiellement vu	quasiment pas documenté	reste à approfondir et documenter	
Documentation de l'analyse				
Outil de conservation de la documentation produite		la base de processus documenté est utilisable		
Outil de workflow possible	non	à priori n'existe pas		

Introduction | Risques | BIA | Stratégie | PRA missions-responsables | PRA Planning | Tests | Gouvernance | Formation | Diagramme

Plan de Continuité d'Activité

Formations

Certification de personnes

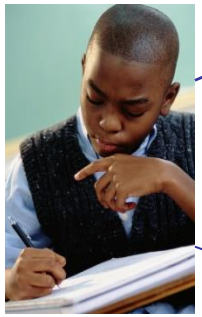
Conformité ISO 17024

Cours ISO 22301

Ex : Duquesne Group

Suit un cours > 40 heures

Agrée le cours tous les ans



Niveau Bac+2
ou 5 ans d'exp.

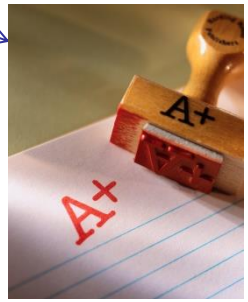
certificateur

Ex : LSTI

accrédite **COFRAC**

Passe un examen 3h30 norme seule

Fait et corrige l'examen



Si note > 65/100 élève certifié « provisional »

Puis « montée en grade » selon le cursus :

Provisional Implementer	Provisional Auditor
Implementer	Auditor
Lead Implementer	Lead Auditor

Attention, il existe des certifications qui ne respectent pas cette logique de séparation des devoirs

Liste des formations

Cours : Tour d'horizon "informatique et continuité" 26/11/2014

L'informatique est un socle incontournable de nos sociétés ; pouvoir en comprendre les technologies, appréhender rapidement les principaux enjeux en matière de fiabilité et continuité, positionner les démarches majeures et en comprendre les raisons, tels sont les objectifs de ce cours synthétique de vulgarisation sur une journée.

Cours "BIA et appréciation des risques" : l'essentiel en un jour 09/10/2014

BIA et appréciation des risques sont des étapes importantes avant tout PCA. Or ce sont deux exercices distincts et délicats. Pour les mener avec efficacité, il faut préparer une approche concrète. Une journée sur le sujet avec E.Besluau notre associé.

Cours "Auditer un PCA interne ou d'un fournisseur" : l'essentiel en un jour 09/10/2014

Avez-vous un PCA ? est-il correct ? Cette question est posée à vous-même ou à vos fournisseurs et ne peut se contenter d'une réponse en deux lignes ou 10 slides puisés sur Internet...

Comment structurer la discussion ? quelles questions ? quelles preuves ? Le tour du sujet en un jour.

Cours certifiant ISO 22301 - Lead Implementer 20/04/2016

Le cours certifiant de référence, le premier mis en place à la sortie de la norme par ceux qui ont participé à sa traduction.

Agréé par LSTI, le certificateur qui fait passer l'examen.

Conforme aux règles ISO.

Dispensé par E.Besluau son créateur et des formateurs certifiés ayant passé

Cours "Gestion de crise, PRA et tests" : l'essentiel en un jour 09/10/2014

La gestion de crise réduite à l'échange de numéros de téléphones entre dirigeants qui "se débrouilleront" : cela ne suffit plus. En une journée faites le tour du sujet avec E.Besluau, des exemples pratiques et des recommandations opérationnelles.

Cours "La norme ISO 22301 sur la continuité" : l'essentiel en un jour 09/10/2014

Cette norme de mai 2012 reste assez méconnue. Pourtant, elle va structurer le paysage de la Continuité. Pourquoi et comment ? Quel impact sur vos PCA, PRA, PCIT, ... ? En un jour le tour du sujet avec E.Besluau implémenteur certifié.

Cours "Prendre en main un PCA : méthode et projet" en deux jours. 09/10/2014

Le cours de référence pour tout responsable en charge de la continuité d'activité en entreprise. Une formation synthétique mais complète sur deux jours, capitalisant sur une riche expérience de mise en oeuvre avec méthode. Animé par E.Besluau qui fournit des exemples et des templates divers.

Formation : faire certifier ISO27001 votre entreprise 08/04/2016

Vous êtes chargé de faire certifier le "Système de Management de la Sécurité de l'Information" (SMSI) de votre entreprise.

Ce SMSI est plus ou moins en place, des éléments existent, d'autres sont absents. Votre management vous presse pour obtenir la certification ISO 27001.

Ne pas oubliez

- Les séances de sensibilisation
- Les exercices divers
  - De simulation de crise (ex : CCA)
  - Internes entreprise
- Les formations pour les personnels mobilisables

➢ En se rapprochant de la réalité du terrain

➢ En évoquant les risques de manière réaliste

Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

CCA
Club de la Continuité d'Activité

IESF
Société des Ingénieurs et Scientifiques de France

Merci de votre attention
et bonne continuité !

Emmanuel BESLUAU

The Duquesne Group

eb@duquesnegroup.com

Tél : +33 (0) 6 14 21 15 03

L'expertise en continuité

« Management de la continuité d'activité »
(livre aux Editions Eyrolles)