



La continuité des affaires :
Une démarche qui crée de la valeur



ÇA VOUS AVANTAGE

Les thèmes de la présentation

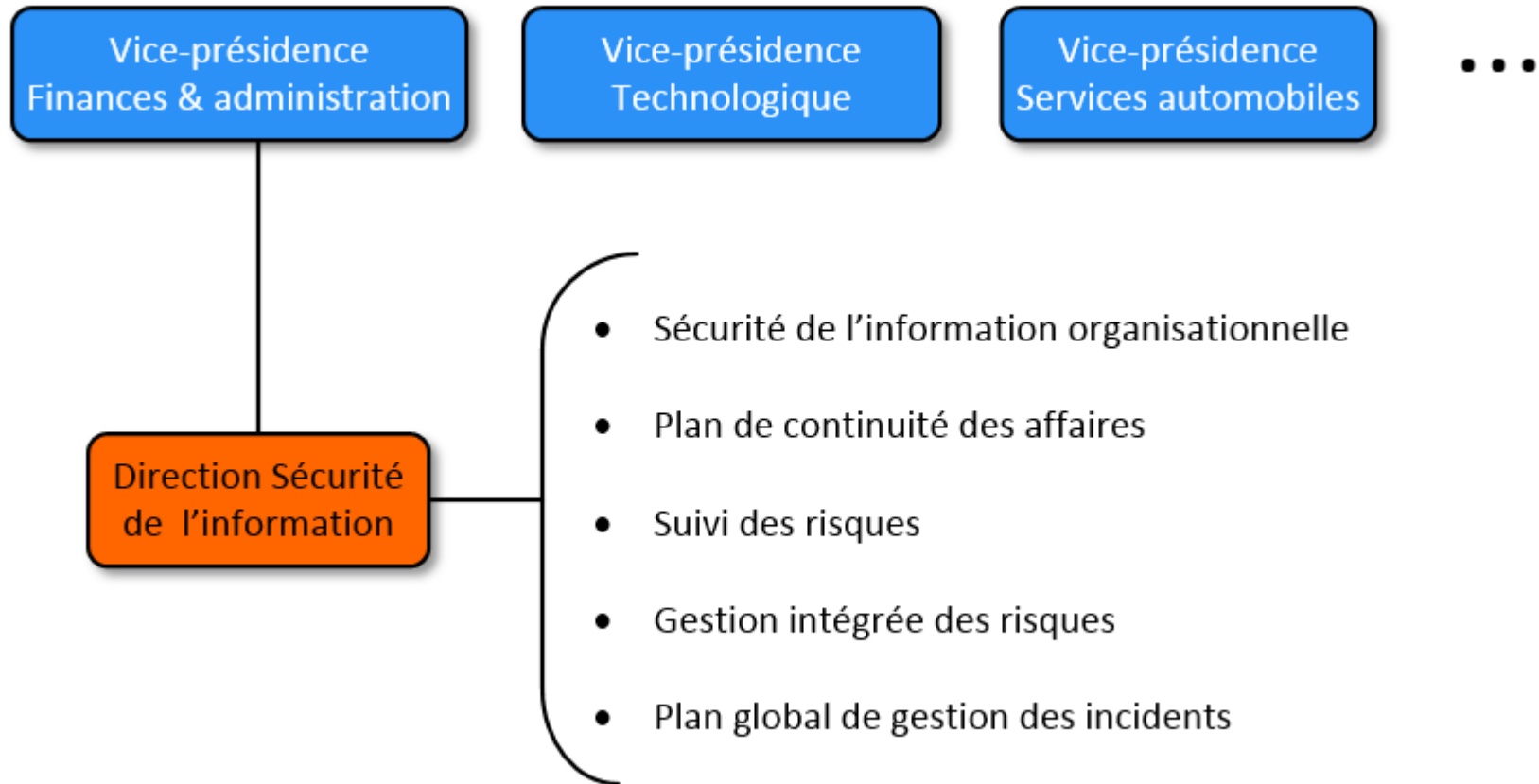
- L'organisation CAA-Québec
- La démarche de transformation d'un plan de relève informatique en un processus de continuité des affaires
- Un plan global de gestion des incidents
- Maximisation de la valeur de nos ressources par l'utilisation d'une intelligence applicative
- Constats post-implantation

L'organisation

- 109 ans d'existence
- Plus de 1,2 million de membres
- Plus de 1 000 employés
- 14 centres Voyages, 11 centres d'immatriculation, 4 écoles de conduite, 3 bureaux administratifs et d'autres en développement

« CAA-Québec, organisme à but non lucratif, assure la tranquillité d'esprit à chacun de ses membres en lui offrant des avantages, des produits et des services de haute qualité dans les domaines de l'automobile, du voyage, de l'habitation et de l'assurance. »

Organisation & responsabilités



Grandes étapes

2008

Mise en place centralisée et structurée de la sécurité informatique

2009

Passage de la sécurité informatique à la sécurité de l'information: principalement liée à la norme PCI et aux standards AAA

2013

Présentation d'un projet sur la continuité des affaires

2014

Transformation du plan de continuité des opérations en plan de continuité des affaires: identification des risques opérationnels liés aux fonctions critiques

Été 2014

Lancement du projet de la gestion intégrée des risques (GIR)

2015

Mise en place du nouveau plan de continuité des affaires

Mise en place de la GIR

Il était une fois...

- Début des années 90 :** Une préoccupation depuis le tout premier système informatique
- Milieu des années 90 :** Le temps de reprise était relié à la capacité de relève disponible à cette époque
- 2000 :** Une première révision du plan de relève informatique
- 2009 :** Un rehaussement de la relève informatique en plan de continuité des opérations
- 2013:** Le BIA fait ressortir des lacunes majeures à combler dû à l'introduction d'un nouveau concept, la DIMA
- 2014-2015:** Un projet pour corriger les écarts

D'une pierre, deux coups!

« Un BIA pour évaluer les risques opérationnels et de péril »

- Présenter un projet à la direction pour créer de la valeur en augmentant notre résilience opérationnelle
- Déterminer les seuils d'impacts avec le comité directeur composé de membres de la direction
- Effectuer un inventaire des risques et des moyens de contrôle relié à 5 types d'incidents potentiels pouvant devenir un sinistre majeur

D'une pierre, deux coups!

« Un BIA pour évaluer les risques opérationnels et de péril »

- Corroborer les craintes des directeurs grâce aux faits observés
- Effectuer une reddition de compte auprès de la direction
- Entreprendre une réflexion sur la résilience opérationnelle

Présentation des résultats

« La simplicité et la vulgarisation facilitent l'adoption »

- Synthèse sous forme de sommaire exécutif d'une page
- Un tableau de bord articulé qui suscite de l'intérêt
- Basé sur les niveaux d'impacts

Sommaire exécutif 2014 – DIMA des services et impacts des scénarios

	Services	DIMA	Incident	Service	Impact			Scénarios d'incident				
					Image	\$\$	Autre					
1	Centre de contacts SAM			✓	✓							
2	Centre de contacts SAR			✓	✓							
3	Répartition			✓	✓							
4	Services aux entreprises			✓			✓					
5	Centres Voyages (ensemble du service)			✓		✓						
6	Finances			✓			✓					
7	Service de paie						✓					
8	Voyages groupes et croisières			✓			✓					
9	Assurances			✓		✓						
10	Écoles de conduite & Formation			✓			✓					
11	CIA et garages recommandés			✓								
12	Immatriculation						✓					
	Lors d'incident											
13	Ti: Communications et soutien		immédiat				✓					
14	Ti: Infrastructures et sécurité		immédiat				✓					
15	Ti: Syst. téléphoniques et réseau		immédiat				✓					
16	Adhésions		immédiat			✓	✓					
17	Soutien aux employés		immédiat				✓					
18	Approvisionnements et services		immédiat				✓					
19	Communications et affaires publiques		immédiat		✓		✓					
20	Affaires électroniques		immédiat		✓		✓					

Les investissements

« Chaque dollar investi doit avoir une retombée dans les opérations »

- Réunir les équipes pour innover et trouver des solutions pragmatiques
- Laisser la parole aux gens leur permet de s'impliquer davantage
- Présenter au comité de vérification les projets de continuité en insistant sur les gains pour les opérations
- Distinguer la portion de dollars investis uniquement pour le sinistre majeur. Notre cible était 20 %

Sommaire exécutif 2016 – DIMA des services et impacts des scénarios

	Services	DIMA	Incident	Impact				Scénarios d'incident				
				Service	Image	\$\$	Autre					
1	Centre de contacts SAM			✓	✓							
2	Centre de contacts SAR			✓	✓							
3	Répartition			✓	✓							
4	Services aux entreprises			✓			✓					
5	Centres Voyages (ensemble du service)			✓		✓						
6	Finance			✓			✓					
7	Service de paie						✓					
8	Voyages groupes et croisières			✓			✓					
9	Assurances			✓		✓						
10	Écoles de conduite & Formation			✓			✓					
11	CIA et garages recommandés			✓								
12	Immatriculation						✓					
Lors d'incident												
13	TI: Communication et <u>soutien</u>		immédiat				✓					
14	TI: Infrastructures et <u>sécurité</u>		immédiat				✓					
15	TI: Syst. <u>téléphoniques</u> et <u>réseau</u>		immédiat				✓					
16	<u>Adhésion</u>		immédiat			✓	✓					
17	<u>Soutien</u> aux <u>employés</u>		immédiat				✓					
18	<u>Approvisionnements</u> et <u>services</u>		immédiat				✓					
19	Communication et affaires <u>publiques</u>		immédiat		✓		✓					
20	Affaires <u>électroniques</u>		immédiat		✓		✓					

Tableaux de bord

« *Présentation de suivi des risques basé sur les familles de risques* »

Facteurs internes

Perte conformité PCI
Standard AAA,
renseignements
personnels

Perte du système AXIS,
Web, téléphonique.
Risques des projets,
recrutement,
achalandage

Erreurs humaines,
sabotage

Dépenses majeures
non prévues,
investissements
majeurs non prévus

Lié au plan
stratégique et au plan
d'affaires

Risques de conformité

Risques opérationnels

Risques de périls

Risques financiers

Risques stratégiques

Lois : C-28, des
technologies,
environnement, nouvelle
réglementation

Changement dans
les lois, nouveau
standard AAA,
perte de personnel

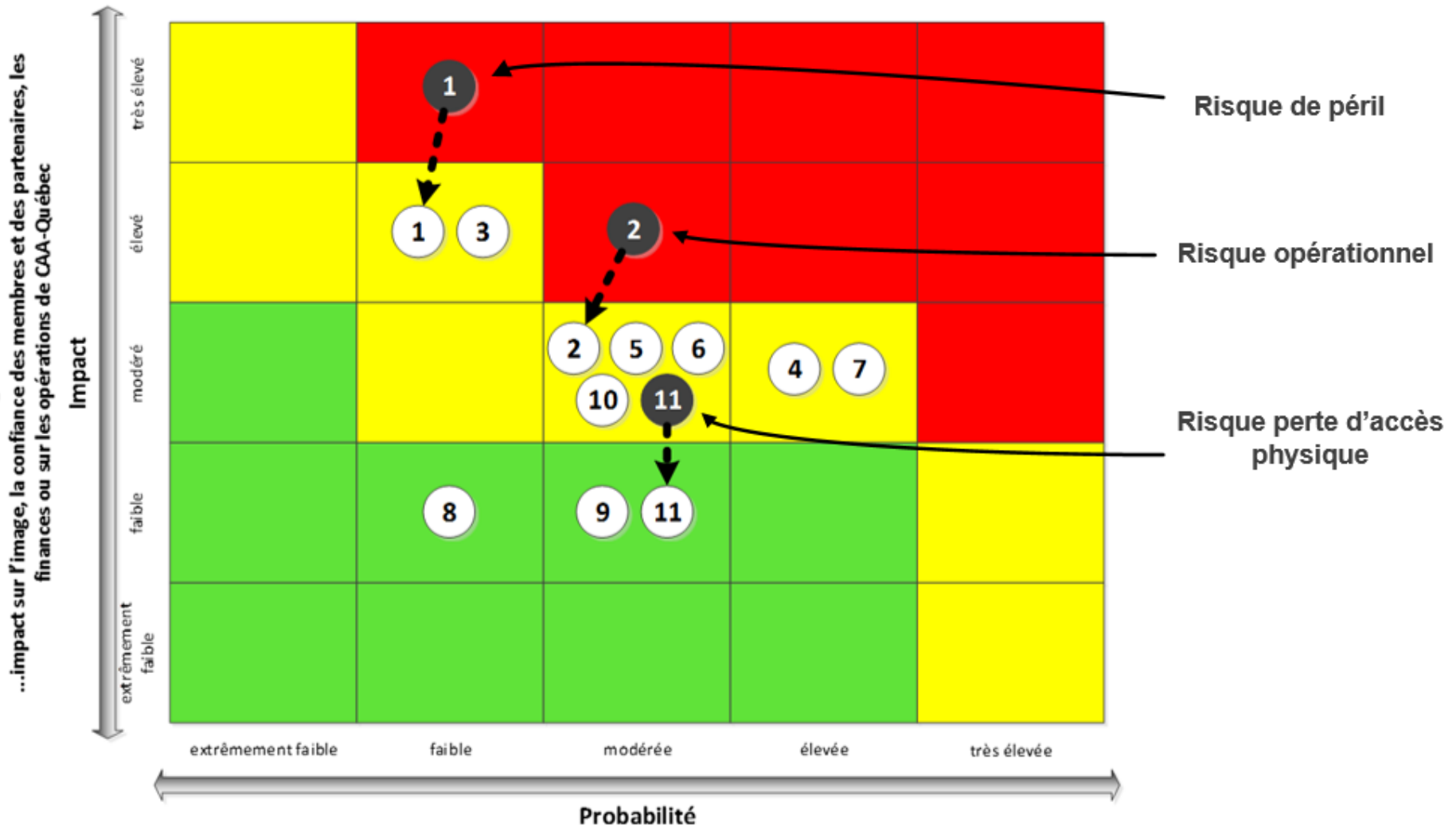
Perte d'un bâtiment,
verglas, panne électrique
majeure, manifestation
bloquant accès aux sites

Variation du prix de
l'essence, aléa climatique,
marché boursier, taux
d'intérêt, baisse
importante des
cotisations

Compétition féroce
et non anticipée,
perte d'un
partenaire
important

Facteurs externes

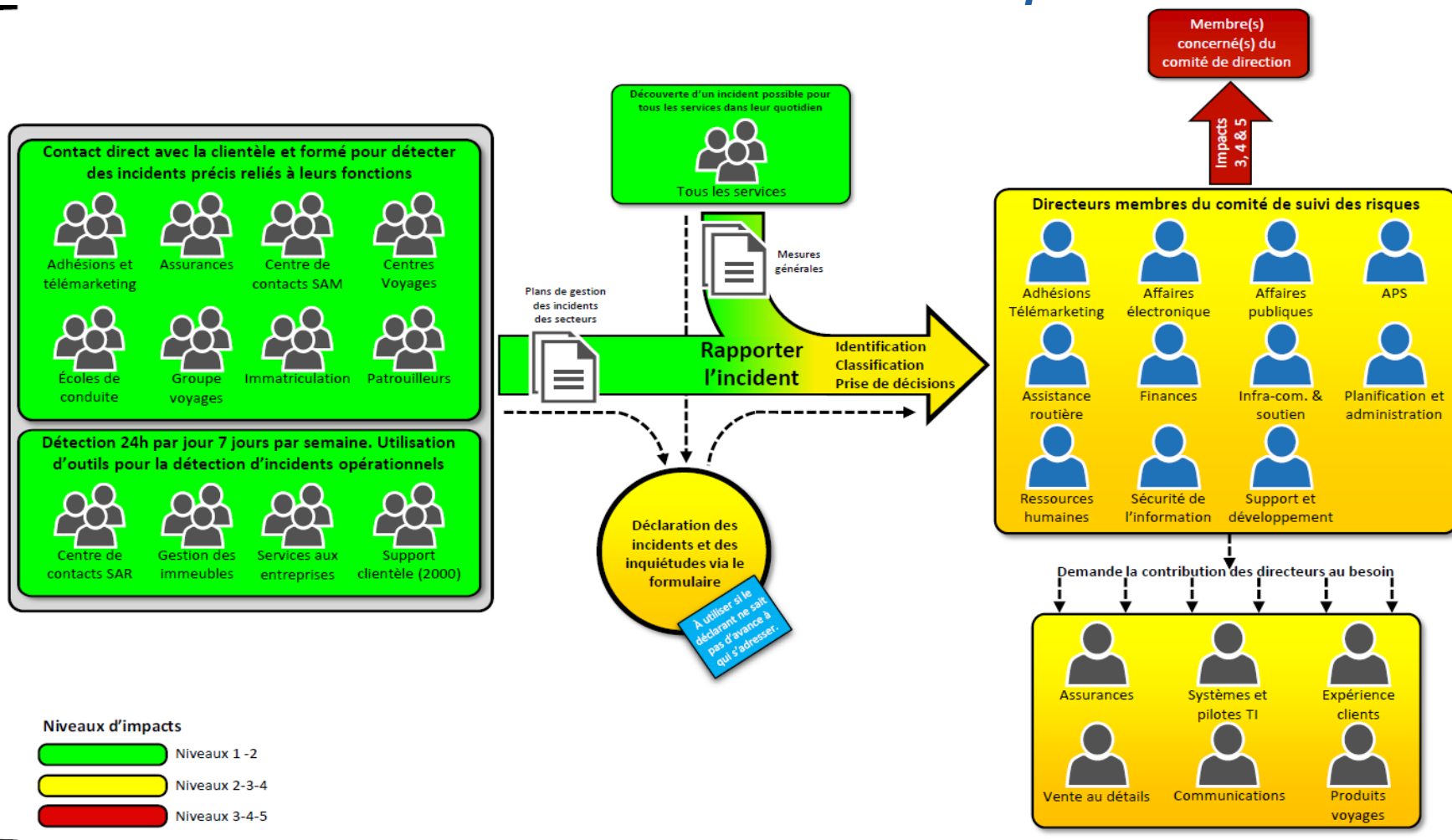
Suivi des risques 2015 - 2016



Plan global de gestion des incidents

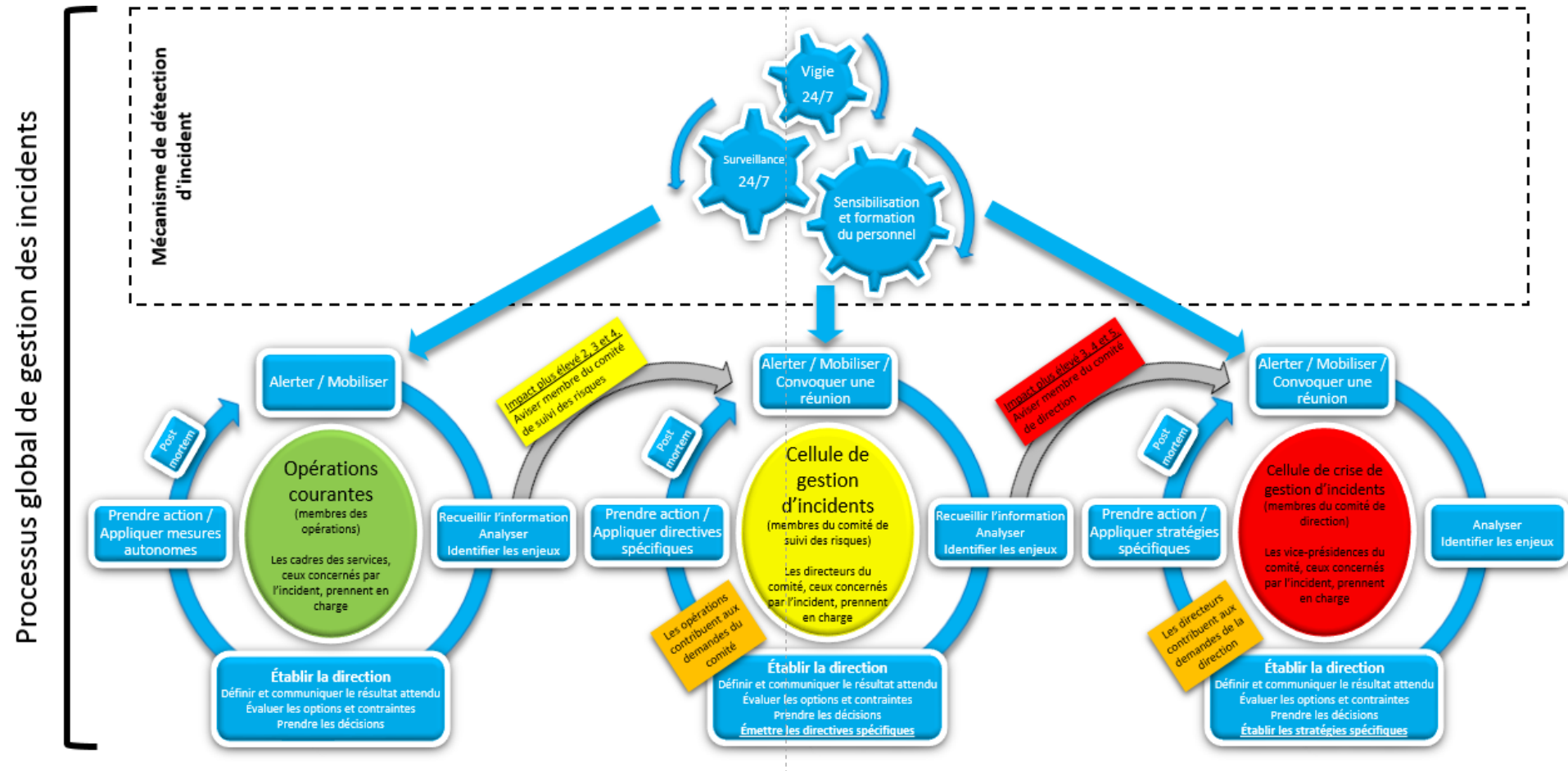
« Utiliser le comité de suivi des risques »

Plan global de gestion des incidents
(identification des services et des rôles)



Processus global de gestion des incidents

« basé sur les familles de risques »

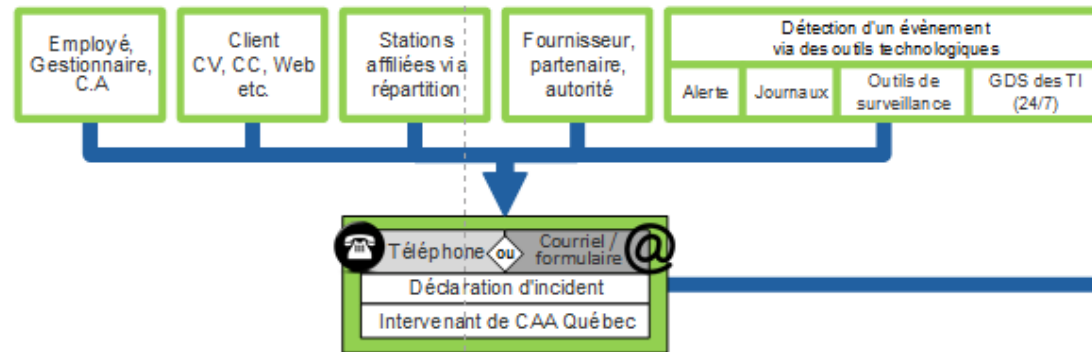


Procédure globale de gestion des incidents

« Suivre le réflexe des gens »

1

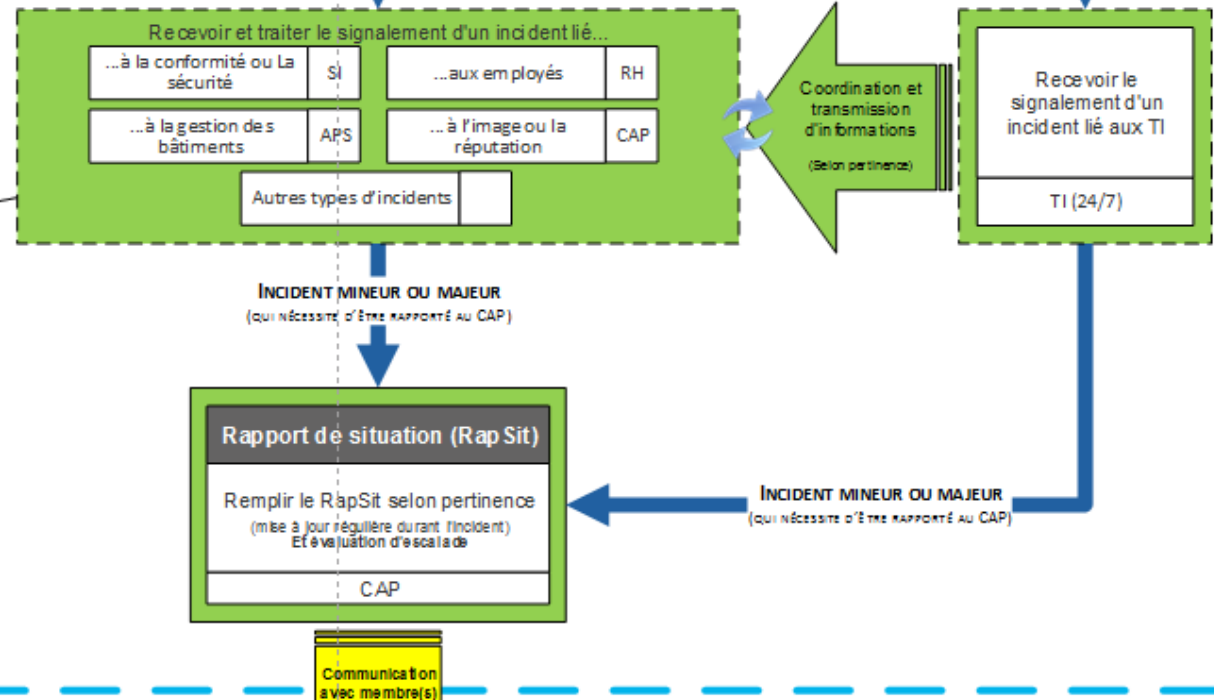
DÉTECTION - PREMIÈRE ANALYSE



2

IDENTIFICATION
CLASSIFICATION
PRISE DE DÉCISION

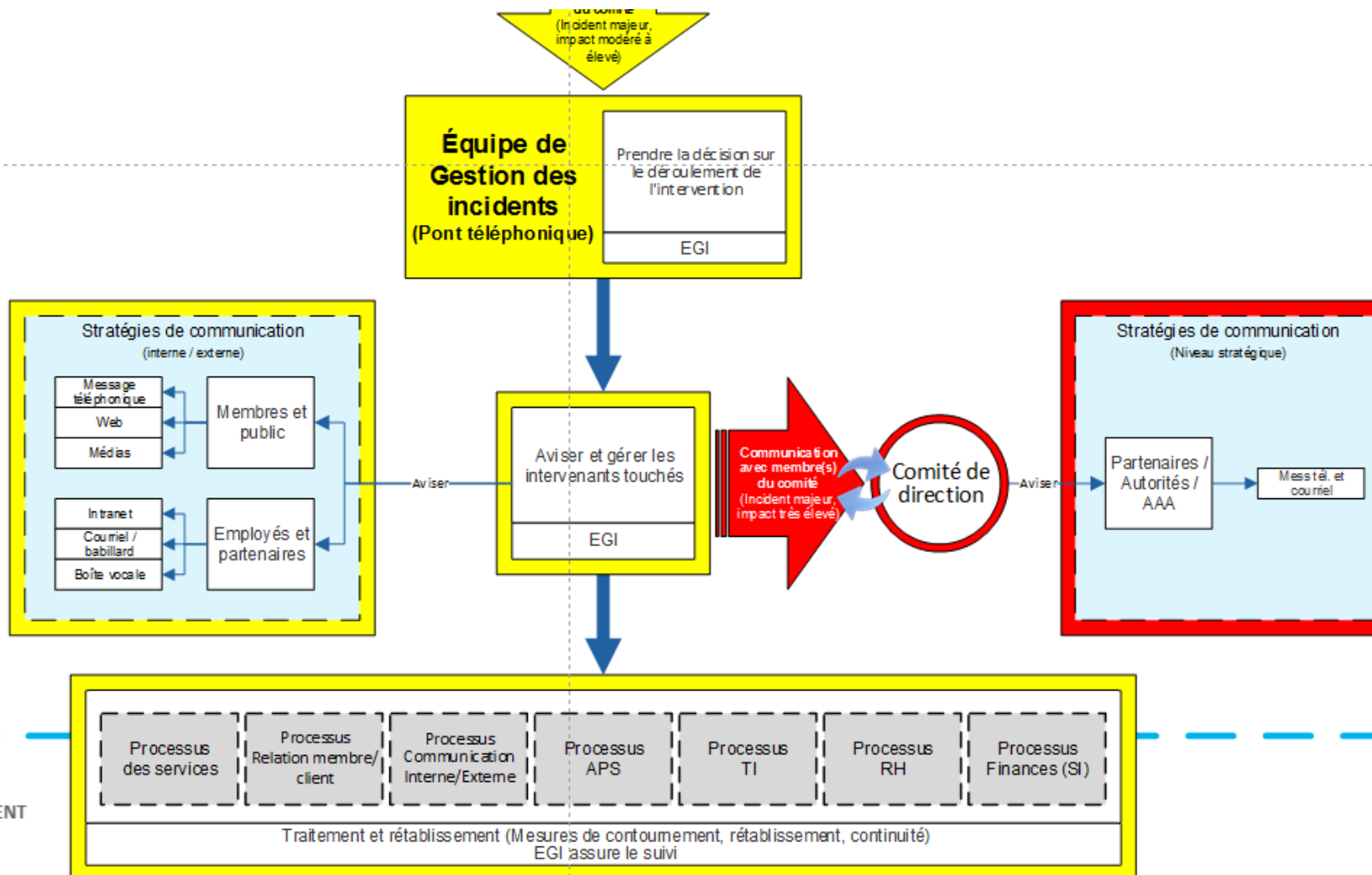
Voir plan
spécifique
pour chaque
service



Procédure globale de gestion des incidents

« Des processus par service »

3 RÉACTION



4 RÉTABLISSEMENT

Maximiser la valeur des ressources en utilisant une intelligence applicative

- Effectuer une démarche d'analyse basée sur les concepts théoriques ISO et BCI
- Choisir une application qui est conçue en tenant compte de ces concepts
- Valider que l'application offre plus qu'un dépôt de documents en supportant les équipes par sa notion d'intelligence
- Distinguer la première année des années subséquentes afin de justifier une application spécialisée

Maximiser la valeur des ressources en utilisant une intelligence applicative

- Utiliser une application de type SAAS afin d'éliminer un risque
- Valider la sécurité de l'information et leur plan de continuité
- Valider la capacité d'intégrer des flux décisionnels et d'approbation
- Identifier vos besoins en notifications

Constats post-implantation

Une première analyse des gains opérationnels

- Tout nouveau projet doit maintenant tenir compte de la sécurité de l'information, du risque opérationnel et de péril
- L'automatisation de la mise à jour des plans s'avère beaucoup moins pénible avec une application spécialisée
- L'implantation de l'application s'est avérée très simple
- Le comité de direction demande maintenant des avis aux « experts »
- Le personnel a l'impression de travailler sur du concret

Les références

Sécurité de l'information : ISO, Méhari, PCI-DSS, standard de l'AAA, protection des renseignements personnels, etc.

Continuité des affaires : ISO, BCI (*Business Continuity Institute*), sécurité civile, etc.

Gestion intégrée des risques : AMF, COSO, FERMA (*Federation of European Risk Management Associations*), etc.

Questions

