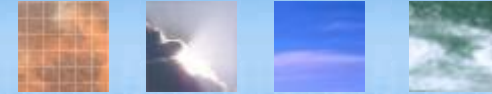


Gouvernance **SSI**

-

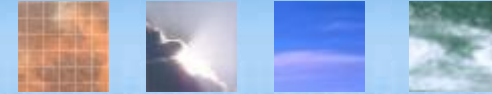
Organisation & **P**ilotage

Club 27001 – 22 janvier 2009
Pierre.dethomasson@hapsis.fr



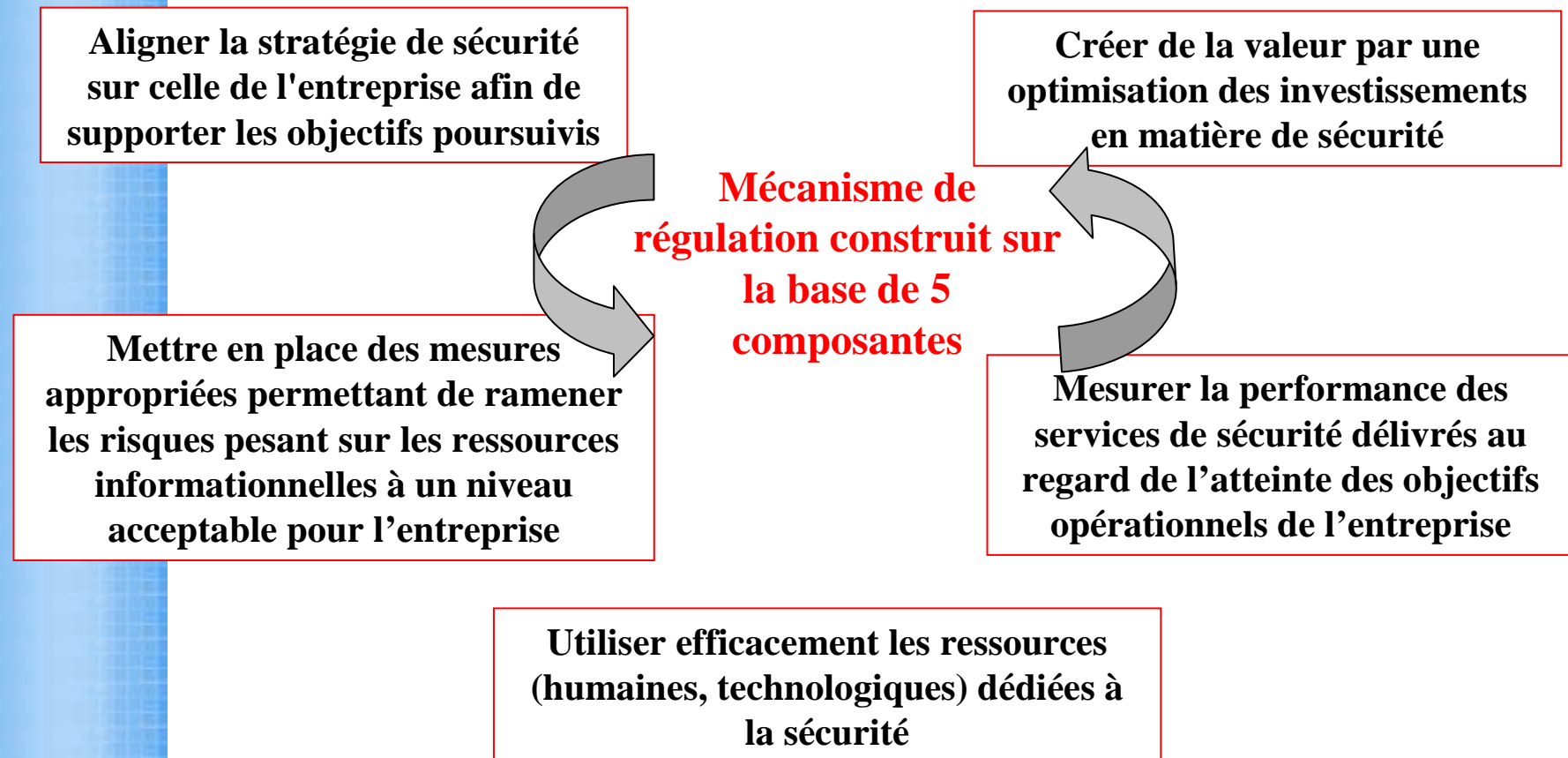
I – Approche

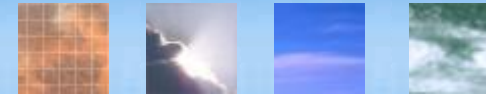
Concepts clés



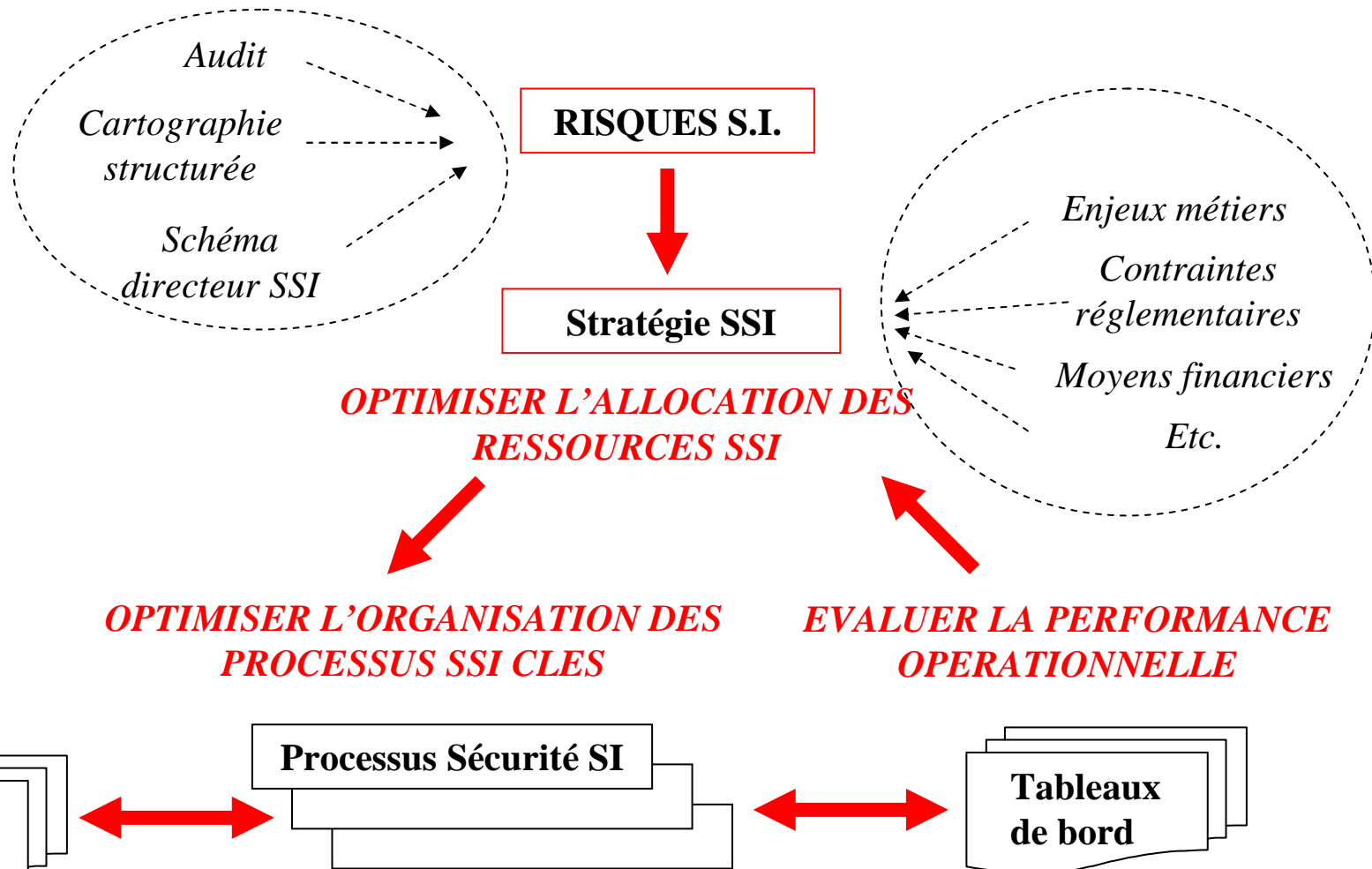
Gouvernance SSI

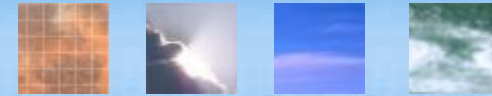
(source : Information security governance « guidance for board of directors and executive management » (2nd edition, ITGI))





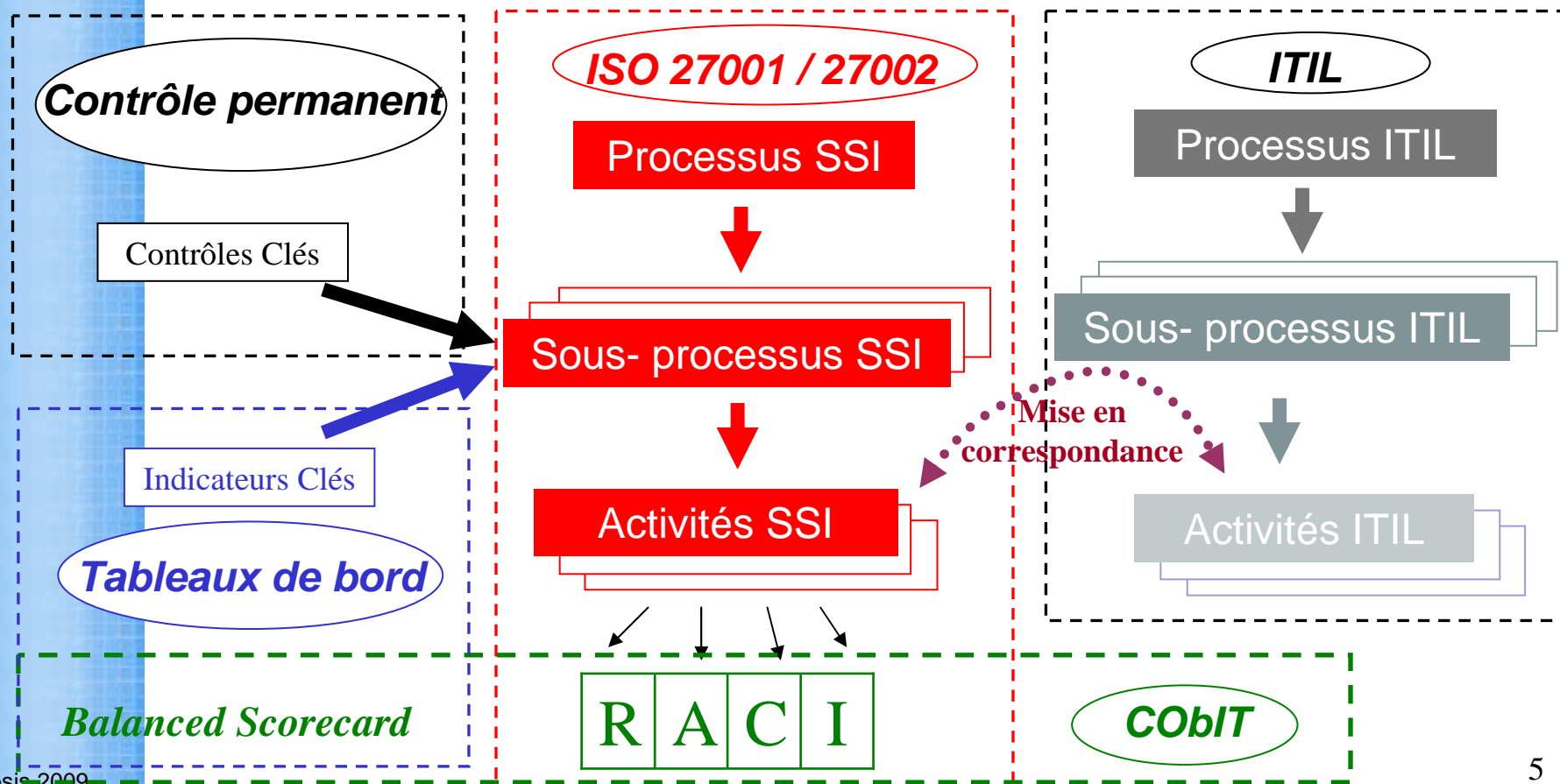
Organisation et pilotage - Principes (1/2)

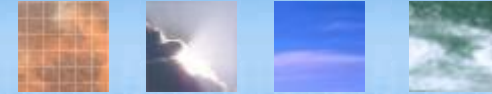




Organisation et pilotage - Principes (2/2)

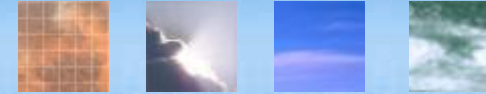
Cohérence avec les normes et meilleures pratiques en la matière



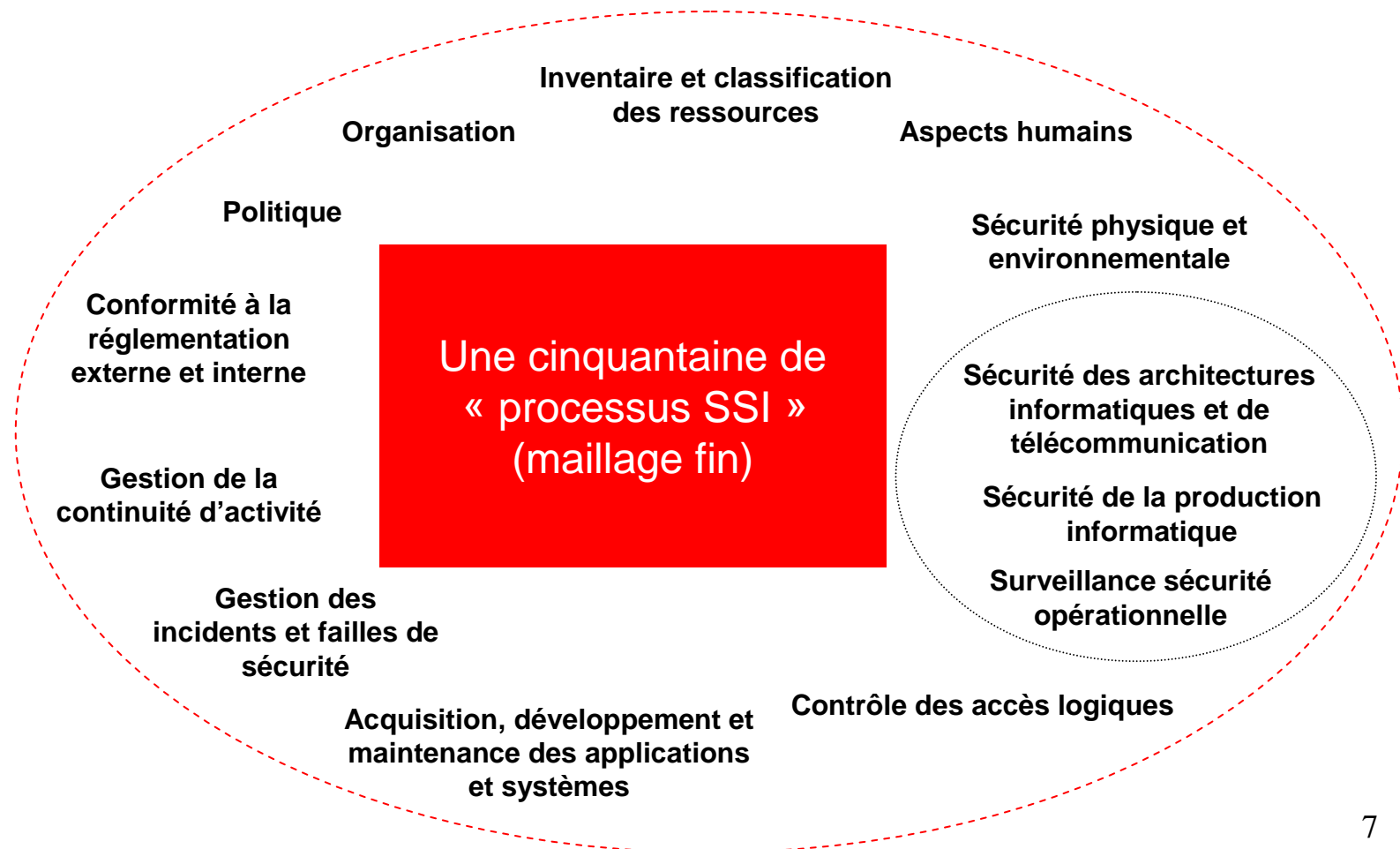


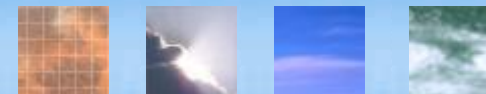
II – Volet organisationnel

Concepts clés



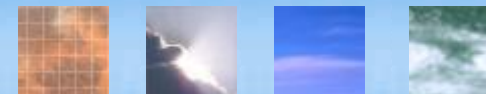
Référentiel organisationnel déclinant les contrôles de l'ISO 27002





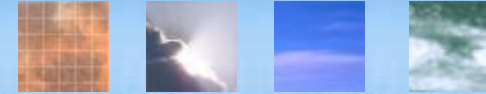
Volet organisationnel – Référentiel (*extrait*)

Gestion des incidents et failles de sécurité	
<i>Processus SSI</i>	<i>Sous-processus SSI</i>
Organiser la gestion des incidents et failles de sécurité	<ul style="list-style-type: none"> • Définir le cadre général du dispositif de gestion des incidents et failles de sécurité • Assurer la communication interne autour du dispositif de gestion des incidents et failles de sécurité
Evaluer le processus de gestion des incidents et failles de sécurité	<ul style="list-style-type: none"> • Evaluer la performance du processus de gestion des incidents et failles de sécurité
Gérer les incidents de sécurité informatiques	<ul style="list-style-type: none"> • Signaler les incidents de sécurité informatique • Réagir au signalement d'incidents de sécurité informatiques • Analyser et diagnostiquer les incidents de sécurité informatiques • Résoudre les incidents de sécurité informatiques • Piloter le traitement des incidents de sécurité informatiques • Assurer le retour d'expérience à l'égard du traitement des incidents de sécurité informatiques
Gérer les alertes de sécurité informatiques	<ul style="list-style-type: none"> • Réagir aux alertes de sécurité informatiques • Traiter les alertes de sécurité
Gérer les failles de sécurité informatiques (hors alertes issues de la veille)	<ul style="list-style-type: none"> • Signaler les failles de sécurité informatiques • Réagir au signalement de failles de sécurité informatiques • Analyser et diagnostiquer les failles de sécurité informatiques • Traiter les failles de sécurité informatiques • Piloter le traitement des failles de sécurité informatiques
Gérer les incidents ou failles de sécurité non informatiques	<ul style="list-style-type: none"> • Signaler les incidents ou failles de sécurité métiers • Réagir au signalement d'incidents ou de failles de sécurité métiers • Analyser et diagnostiquer les incidents ou failles de sécurité métiers • Résoudre les incidents ou failles de sécurité métiers • Piloter le traitement des incidents ou failles de sécurité métiers • Assurer le retour d'expérience à l'égard du traitement des incidents de sécurité métiers



Volet organisationnel – « Adhérences ITIL »

Processus SSI	Sous-processus SSI	Activité SSI	Processus (ITIL)	
Gérer les incidents de sécurité informatiques	Signaler les incidents de sécurité informatiques	Appliquer la procédure de signalement et de réaction (mesures conservatoires éventuelles) en cas d'incidents de sécurité informatiques prenant naissance au sein des environnements métier, notamment au niveau des postes de travail	Tous métiers	
	Réagir au signalement d'incidents de sécurité informatiques	Enregistrer les incidents de sécurité informatiques	Gérer les demandes et les incidents	
		Classifier le niveau de criticité des incidents de sécurité informatiques signalés		
		Déclencher la mise en place des mesures conservatoires prévues, notamment en cas de signalement d'incidents de sécurité informatiques critiques		
	Déclencher la procédure d'alerte, notamment en cas de signalement d'incidents de sécurité informatiques critiques	Analyser et diagnostiquer les incidents de sécurité informatiques	Analyser les incidents de sécurité informatiques signalés : - Investigation, qualification - Diagnostic (incident répertorié ou non, répétitif ou non, traitement connu ou solution à construire (« problème ») - Déclenchement du processus de résolution	Gérer les demandes et les incidents
	Incidents non répertoriés / répétitifs (« problèmes ») - Fabriquer les solutions de traitement ou de contournement des problèmes de sécurité informatique non répertoriés	Fabriquer une correction du SI		
	Tous types d'incidents Gérer les changements induits par la mise en place des solutions de traitement ou de contournement des incidents ou problèmes de sécurité informatiques	Gérer les changements		
	Tous types d'incidents Mettre en place les solutions de traitement des incidents ou problèmes de sécurité informatiques	Faire les mises en production		
	Piloter le traitement des incidents de sécurité informatiques	.../...	.../...	

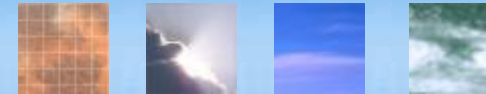


Modèle RACI (d'après COBIT)

- **R : Responsable (s)**, réalise(nt) une ou plusieurs actions relatives à l'activité / tâche
- **A : Autorité**, assure la validation / approbation du travail associé à l'activité / tâche ; rend les comptes sur le déroulement de l'activité / tâche
- **C : Contributeur(s) ou Consulté(s)**, fournit(fournissent) des ressources ou peut(peuvent) aider dans le cadre de la réalisation de l'activité / tâche, notamment dans la mesure où il(s) a(ont) l'information et/ou les aptitudes nécessaires à la finalisation de l'activité / tâche
- **I : Informé(s)**, doit(doivent) être avisé(s) des conditions de déroulement de l'activité / tâche, sans pour autant être contributeur(s)

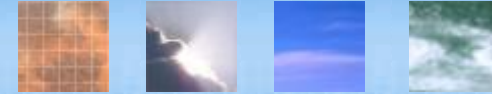
Seuls les rôles « R » et « A » doivent être systématiquement identifiés pour toute activité / tâche.

Il ne peut exister qu'une seule « Autorité » par activité / tâche



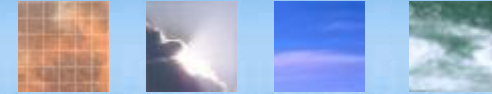
Volet organisationnel – Modélisation détaillée (exemple)

Processus	Objectifs				
	ACTIVITES	R	A	C	I
Gérer les incidents de sécurité informatiques	S'assurer que les incidents de sécurité survenant au sein des systèmes informatiques et de télécommunication font l'objet d'une procédure de traitement compatible avec les risques induits sur les systèmes d'information de l'entreprise				
Signaler les incidents de sécurité informatiques	Appliquer la procédure de signalement et de réaction (mesures conservatoires éventuelles) en cas d'incidents de sécurité informatiques prenant naissance au sein des environnements métier, notamment au niveau des postes de travail				
Réagir au signalement d'incidents de sécurité informatiques	Enregistrer les incidents de sécurité informatiques				
	Classifier le niveau de criticité des incidents de sécurité informatiques signalés				
	Déclencher la mise en place des mesures conservatoires prévues, notamment en cas de signalement d'incidents de sécurité informatiques critiques				
	Déclencher la procédure d'alerte, notamment en cas de signalement d'incidents de sécurité informatiques critiques				
Analyser et diagnostiquer les incidents de sécurité informatiques	Analyser les incidents de sécurité informatiques signalés : -Investigation, qualification -Diagnostic (incident répertorié ou non, répétitif ou non, traitement connu ou solution à construire (« problème ») -Déclenchement du processus de résolution				
Résoudre les incidents de sécurité informatiques	<u>Incidents non répertoriés / répétitifs (« problèmes »)</u> -Gérer les problèmes de sécurité informatique				
	<u>Incidents non répertoriés / répétitifs (« problèmes »)</u> -Fabriquer les solutions de traitement ou de contournement des problèmes de sécurité informatique non répertoriés				
	<u>Tous types d'incidents</u> Gérer les changements induits par la mise en place des solutions de traitement ou de contournement des incidents ou problèmes de sécurité informatiques				
	<u>Tous types d'incidents</u> Mettre en place les solutions de traitement des incidents ou problèmes de sécurité informatiques				
Piloter le traitement des incidents de sécurité informatiques	... / ...				



III – Volet pilotage

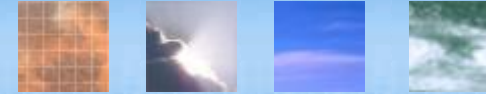
Concepts clés



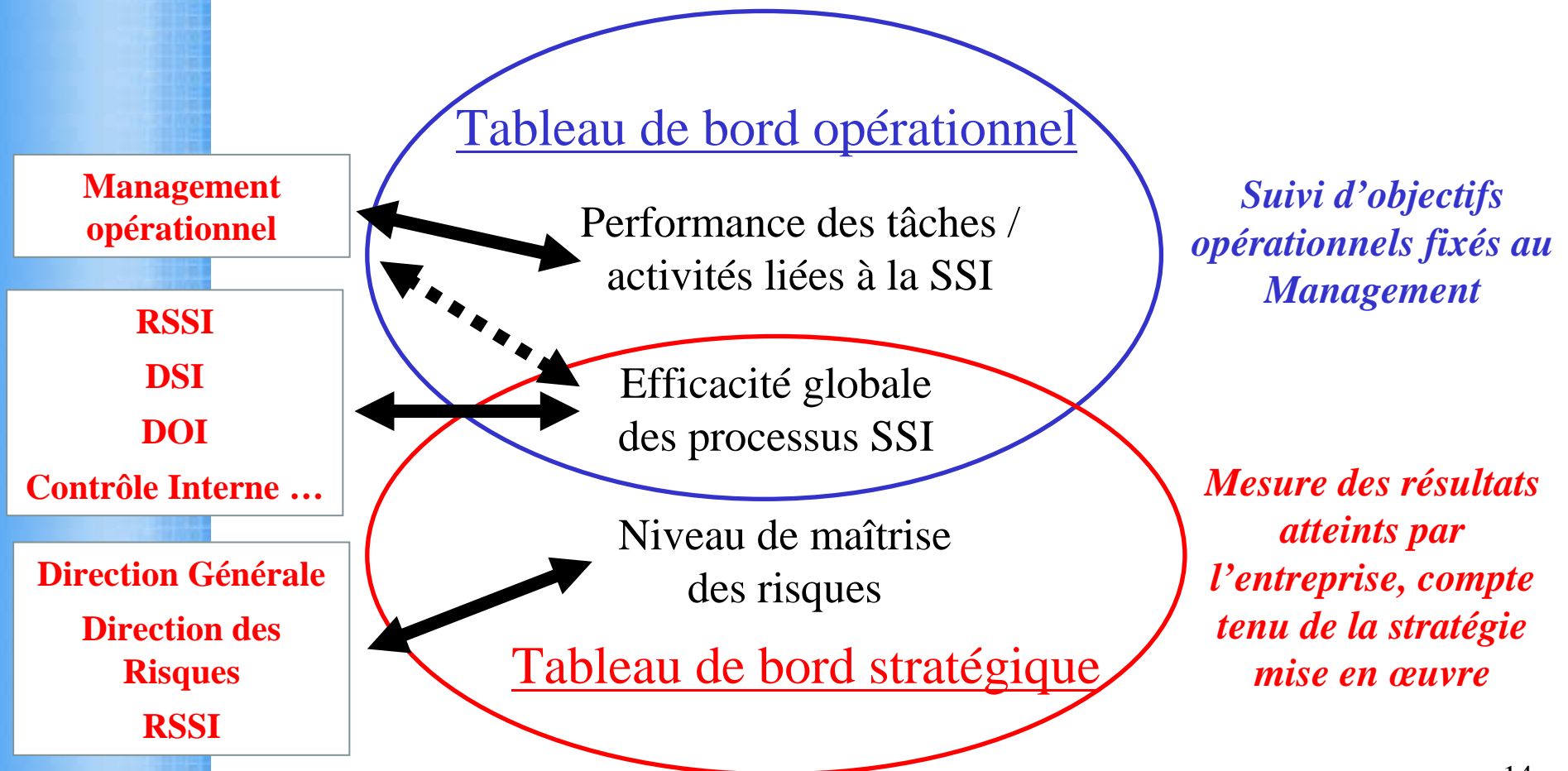
Quels objectifs ?

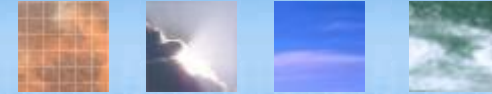
- Apprécier la **performance des tâches liées à la sécurité** placées sous la responsabilité du management opérationnel ?
- Mesurer **l'efficacité globale des processus de sécurité** mis en œuvre au sein de l'entreprise ?
- Appréhender le **niveau de maîtrise de certains risques** retenus par la direction générale ou le RSSI ?

Sans exclure les autres motivations



Quel positionnement ?



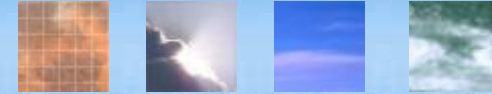


Quelles orientations ?

ISO 27001 / 27004

Balanced scorecard

COBIT



Quelles typologies d'indicateurs ?

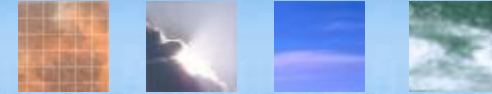
A priori

● **Indicateurs Clés de Performance** proprement dits (ICP), exprimant *a priori* les conditions du succès ou de l'échec, ils traduisent le **niveau de maîtrise opérationnelle** des processus de sécurité à l'égard de certains **facteurs clés de succès** relevant par exemple :

- Du déploiement d'une organisation et de la tenue effective de certains rôles clés
- De l'existence, du maintien et du respect de règles et de procédures opérationnelles
- Du déploiement de dispositifs technologiques et du maintien à niveau des services de sécurité qu'ils assurent
- De l'acquisition et du respect de comportements responsables

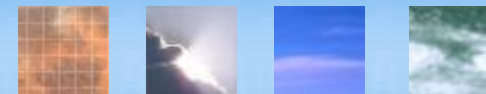
A posteriori

● **Indicateurs Clés d'Objectif** (ICO) reflétant *a posteriori* le **niveau d'efficacité globale** du processus de sécurité à l'égard de sa finalité, et ce faisant, son **taux de contribution direct ou indirect à la maîtrise de certains risques**



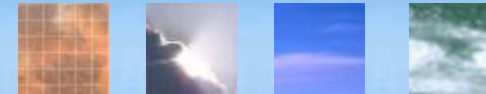
Quel éclairage fourni par le système d'indicateurs ?



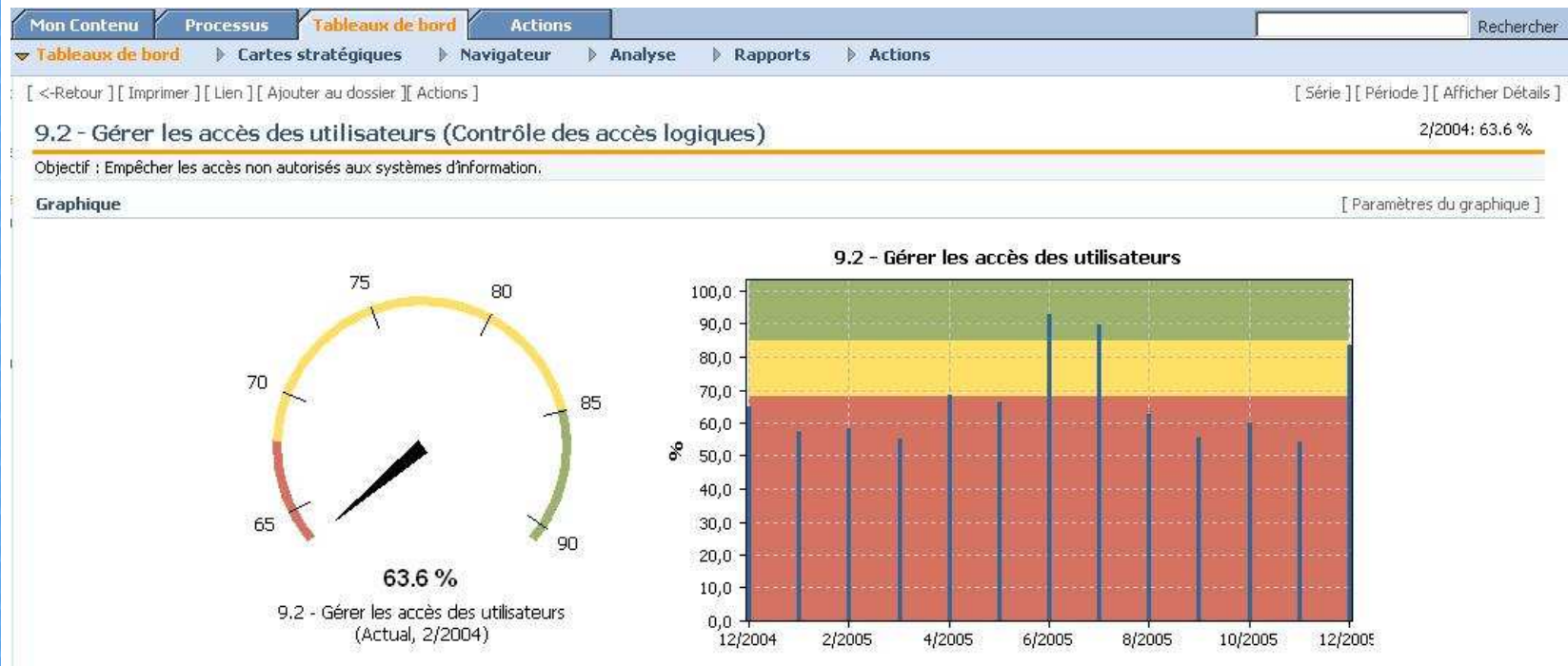


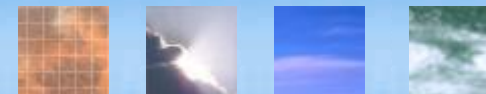
Exemples d'ICO's / ICP's (Lutte antivirale)

ICO	ICP
<p>%des postes de travail équipés d'un antivirus « à jour » (notion à préciser selon la PSSI adoptée)</p> <p>% moyen annuel de postes de travail infectés par « épisode viral » (ex : contamination supérieure à 10 postes)</p> <p>% d'évolution du nb de serveurs sensibles ayant été infectés par des codes malveillants (vers, par exemples), en glissement annuel</p> <p>% d'évolution du nb de postes de travail hébergeant des logiciels proscrits par l'entreprise (outils d'attaque, spywares, ...), en glissement annuel</p> <p>% d'évolution du nb d'heures perdues pour cause infection virale, en glissement annuel</p> <p>.../...</p>	<i>Aspects organisationnels</i>
	Existence d'une politique de lutte contre les codes malveillants / mobiles et de protection contre le téléchargement de fichiers
	Existence d'une structure spécifique à la lutte contre les codes malveillants / mobiles
	Existence d'une procédure de réaction à une attaque virale
	<i>Niveau de prévention antivirale</i>
	Fréquence de mise à jour des bases de signatures virales et des moteurs sur les passerelles de messagerie
	Fréquence de mise à jour des bases de signatures virales sur les serveurs de fichiers
	Fréquence de mise à jour des bases de signatures virales sur les postes de travail
	% de postes de travail équipés d'un dispositif de contrôle de conformité à l'égard de la protection antivirale
	% de postes de travail équipés de dispositif de contrôle des codes mobiles (blocage)
	<i>Niveau de protection</i>
	% d'évolution du nombre de postes de travail infectés par des codes malveillants détectés par les antivirus, en glissement annuel
	Délai moyen constaté d'éradication des infections virales
	% des utilisateurs ayant été formés à la conduite à tenir en cas de d'infection (ou de suspicion d'infection) de leur poste de travail
	<i>Niveau de contrôle des configurations des postes de travail</i>
	Existence d'une procédure industrialisée de contrôle du niveau de mise à jour des antivirus (moteurs et bases de signature) sur les postes de travail
Existence d'une procédure de contrôle « instantané » cyclique ou « à la demande » du niveau de mise à jour des antivirus (moteurs et bases de signature) sur les postes de travail	
Existence d'une procédure de contrôle des postes de travail vis-à-vis des logiciels proscrits (spywares, outils d'attaque, ...)	
Fréquence moyenne de contrôle des postes de travail vis-à-vis des logiciels proscrits (spywares, outils d'attaque, ...)	



Exemple de visualisation (Outil QPR Scorecard ©)





Exemple de visualisation (Outil QlikView ©)

Maitrise d'un risque

Accès au système d'information et consultation en ligne par un pirate se connectant depuis internet.

Détails >>

Au 01/10/2008

Concevoir et déployer une architecture LAN sécurisée



Authentifier les accédants aux systèmes d'information depuis le LAN



Surveiller les infrastructures informatiques et de communication



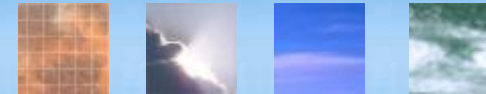
Niveau de Contribution à la maitrise du risque: 40%

Niveau de contribution à la maitrise du risque: 40%

Niveau de Contribution à la maitrise du risque: 20%

Niveau de maitrise du risque





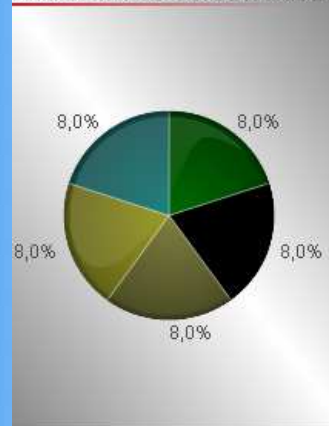
Exemple de visualisation (Outil QlikView ©)

Performance d'un processus

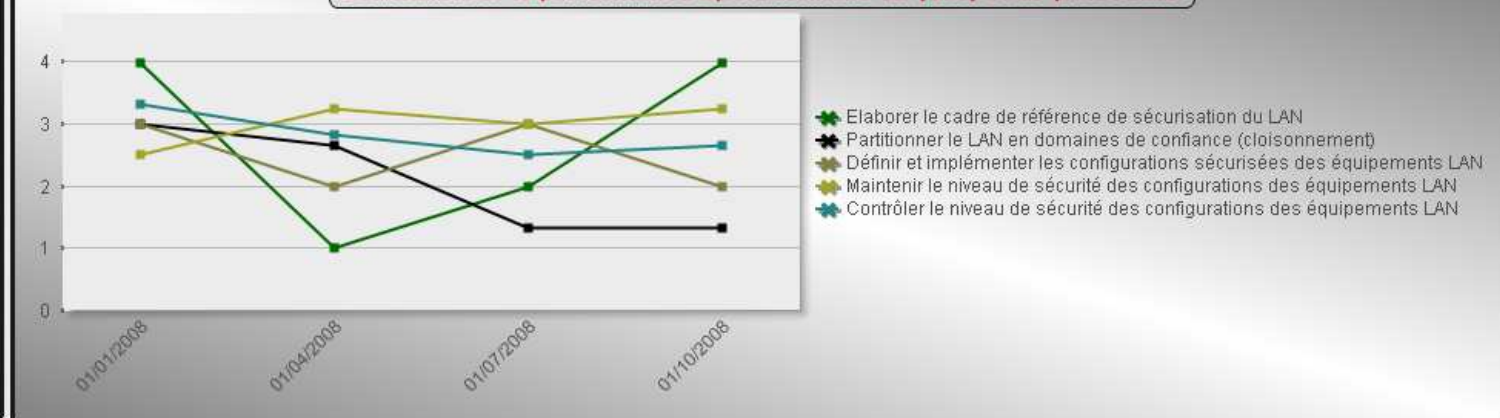
	01/01/2008	01/04/2008	01/07/2008	01/10/2008
Liste des processus				
Concevoir et déployer une architecture LAN sécurisée				Poids (%) 40

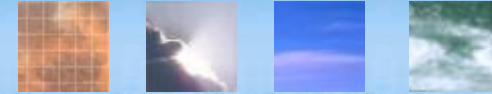
		Poids (%)
Liste des sous processus		
Elaborer le cadre de référence de sécurisation du LAN		8
Partitionner le LAN en domaines de confiance (cloisonnement)		8
Définir et implémenter les configurations sécurisées des équipements LAN		8
Maintenir le niveau de sécurité des configurations des équipements LAN		8
Contrôler le niveau de sécurité des configurations des équipements LAN		8

Contribution des Sous Processus



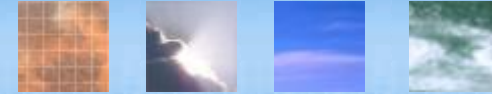
Evaluation de la performance operationnelle du (des) sous-processus





III – Volet Contrôle

Concepts clés



Les finalités (d'après CRBF)

Hiérarchie
opérationnelle

● Niveau 1

- Est effectué de manière permanente par l'acteur opérationnel lui-même dans le cadre des actions exécutées dans son activité opérationnelle
- A pour objet de s'assurer de la **justesse des opérations**, de la **qualité d'exécution des tâches** dans le respect des procédures définies

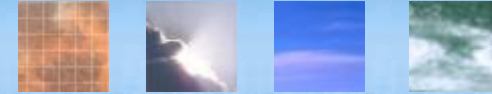
● Niveau 2

- Est un contrôle des instances opérationnelles hiérarchiques
- A pour objectif de vérifier l'**existence**, la **permanence** et la **pertinence** des contrôles de niveau 1
- Inclut les contrôles de nature réglementaire

Autorité
spécifique

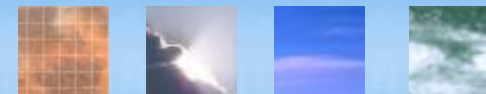
● Il appartient :

- A chaque niveau de contrôle de définir ses propres critères de vérification
- Au niveau N2 de s'assurer de la cohérence du niveau N1



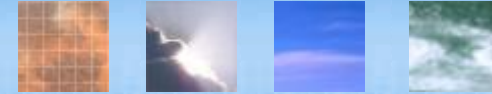
Les contrôles N1 & N2 « clés »

- Complètent les contrôles N1 et N2 « types »
- Éclairent à la fois la hiérarchie opérationnelle et le RSSI :
 - Sur le **niveau d'efficacité des contrôles « types » mis en œuvre**, au regard des **finalités** des activités de sécurité considérées
 - Le cas échéant, sur le niveau de respect de la réglementation
- Sont construits selon le découpage « processus / activités » commun aux volets **organisationnel** et **pilotage** de la modélisation relative à la gouvernance sécurité SI

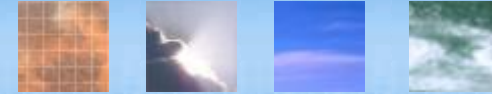


Volet contrôle N1 & N2 (exemple « Tester le PCA »)

Activité SSI	Contrôles N1 (partiel)	Contrôles N2 (partiel)
Définir une politique globale de tests du(des) PCA(s)	... / ...	
Définir un programme glissant de tests (unitaires / globaux) relatifs au(x) PCA(s) et portant sur : -La mise en œuvre des procédures d'urgence -La reprise technique (informatique) -La reprise fonctionnelle (métiers) -La mobilisation des moyens de secours logistiques (sites de replis, intervention de prestataires, ...)	... / ...	
Réaliser le programme glissant de tests de la mise en œuvre des procédures d'urgence liées au(x) PCA(s) Elaborer et mettre en œuvre les plans de progrès issus du programme de tests des procédures d'urgence	<ul style="list-style-type: none"> •Contrôle du respect de la conduite des tests vis-à-vis des programmes prévus (conditions de déclenchement, mobilisation des ressources, chronologies des tâches,...) 	<ul style="list-style-type: none"> •Contrôle de l'existence d'un plan d'action actualisé de mise à jour des actions de progrès du(des) PCA(s) liées à : <ul style="list-style-type: none"> -La mobilisation des moyens logistiques de secours -La sollicitation des prestataires de secours -Le secours et de reprise technique des infrastructures de production -La reprise d'activité métiers •Contrôle de l'évolution dans le temps du stock d'actions inscrites au plan de progrès identifiées dans le cadre des tests du(des) PCA(s)
Réaliser le programme glissant de tests de reprise technique liés au(x) PCA(s) Elaborer et mettre en œuvre les plans de progrès issus du programme de tests de reprise technique	<ul style="list-style-type: none"> •Contrôle de l'exhaustivité et de la qualité de l'enregistrement des anomalies et incidents constatés 	
Réaliser le programme glissant de tests de reprise fonctionnelle liés au(x) PCA(s) Elaborer et mettre en œuvre les plans de progrès issus du programme de tests de reprise fonctionnelle	<ul style="list-style-type: none"> •Contrôle de l'exhaustivité de la prise en considération des anomalies et incidents constatés dans le cadre d'un plan de progrès 	
Réaliser le programme glissant de tests de mobilisation des moyens de secours logistiques (sites de replis, intervention de prestataires, ...) liés au(x) PCA(s) Elaborer et mettre en œuvre les plans de progrès issus du programme de tests de mobilisation des moyens de secours logistiques	<ul style="list-style-type: none"> •Contrôle de l'existence et de la tenue d'une réunion de débriefing (destinée notamment à la mise à jour du plan de progrès PCA) à l'issue de chaque test 	
	... / / ...

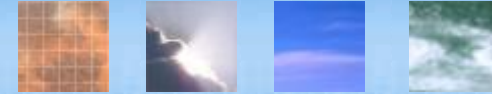


IV – Applications



- Organisation SSI et conduite du changement
 - Intégration de la SSI dans les processus opérationnels de l'entreprise (Globalement ou sur un périmètre spécifique)
 - Organisation des missions / rôles des entités opérationnelles à l'égard de la sécurité
 - Organisation du contrôle permanent
- Pilotage SSI
 - Pilotage opérationnel des processus SSI
 - Evaluation partielle ou globale de la qualité du SMSI
 - Evaluation du niveau de maîtrise des risques majeurs

Dans le respect des meilleures pratiques issues de normes effectives ou « de fait »



**MERCI DE VOTRE
ATTENTION !**