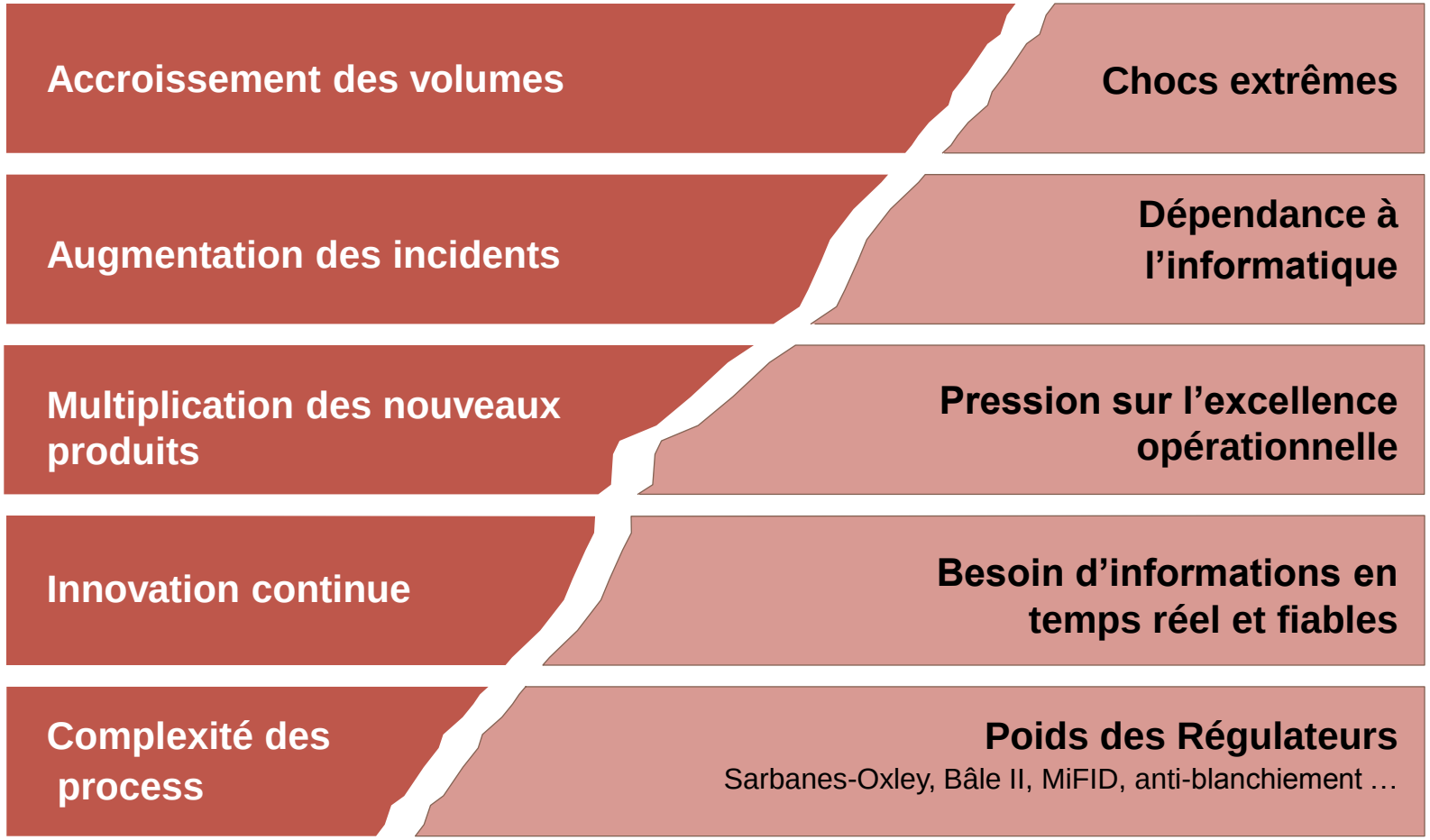
GESTION DES RISQUES OPÉRATIONNELS

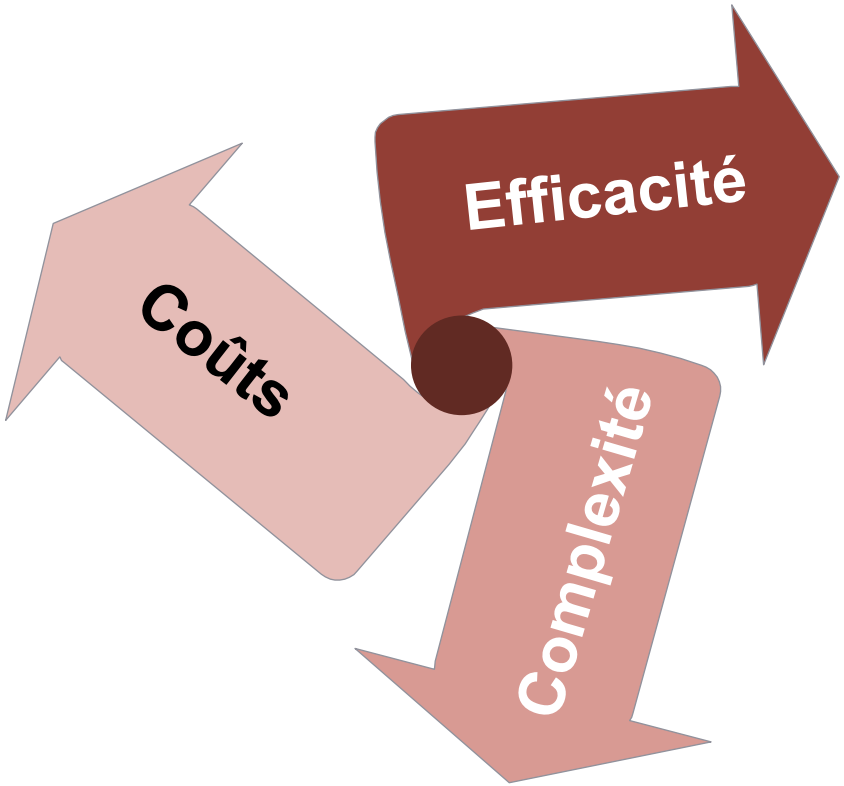
Xavier Genet

CONTEXTE

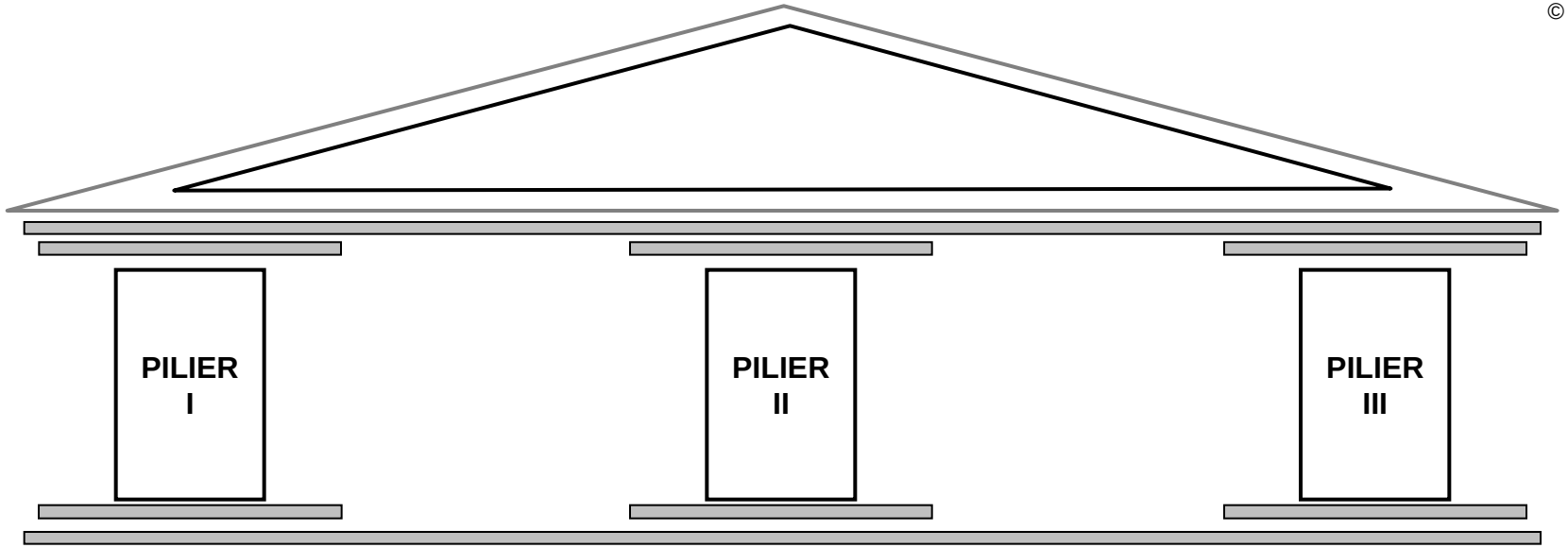


IL Y AURA TOUJOURS DES RISQUES …

Protéger l'organisation
… en définissant un niveau de risque acceptable
… en permettant aux métiers d'opérer dans un environnement sécurisé
… suivant des coûts adéquats



LA RÉFORME DE BÂLE 2 : LES TROIS PILIERS



EXIGENCES MINIMALES EN FONDS PROPRES

- Risque de crédit
- Risque opérationnel
- Risque de marché

PROCESSUS DE SURVEILLANCE PRUDENTIELLE

Le régulateur pourra exiger un ratio de solvabilité supérieur au minimum réglementaire en fonction de son appréciation sur la qualité :

- Des risques pris, notamment taux et liquidité
- Du Risk Management, du contrôle interne et du reporting de l'établissement
- De l'allocation des fonds propres

DISCIPLINE DE MARCHÉ

« Transparence vers l'extérieur » :

- Composition des fonds propres
- Allocation des fonds propres aux divers risques
- Composition (géographique, sectorielle …) des portefeuilles de crédit
- Système de notation interne

AGENDA BÂLE 2

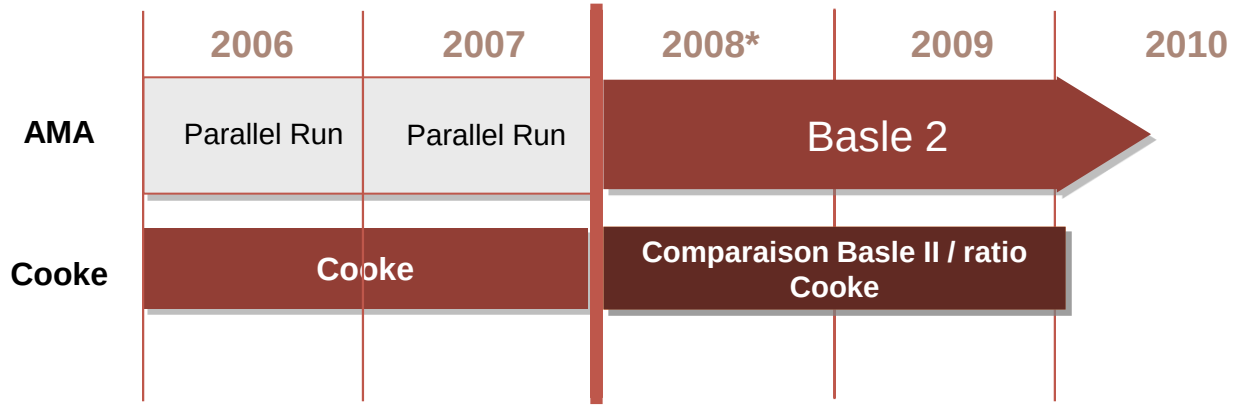
Certification

2007-2008 : la Commission Bancaire audite les banques pour la validation AMA (Advanced Measurement Approaches) dans le cadre des accords de Bale II.

Principes

1. **Quantitatif :** Le capital réglementaire est calculé grace à un modèle statistique interne.
2. **Qualitatif** : Les banques doivent mettre en place une organisation indépendantes de gestion des risques opérationnels (prévention, mesure, pilotage, implication du Management, ressources dédiées)

Plan d'implementation



PILIER 1 : RISQUES OPÉRATIONNELS

- Ils sont définis comme « les risques de pertes résultant d'une inadéquation ou d'une défaillance attribuable à des procédures, à des facteurs humains, à des systèmes ou à des événements extérieurs ».

- Ils englobent l'ensemble des risques inhérents à l 'activité de l 'établissement.

- Cette définition inclut le risque juridique mais exclut les risques stratégiques et les risques d'image.

- Dans le document de janvier 2001, le comité de Bale s'attendait à ce que les risques opérationnels représentent 20% de l'exigence en FP. Il a changé sa position depuis : les risques opérationnels ne devraient représenter qu'environ 12% des FP.

LES RISQUES OPÉRATIONNELS EN IMAGES

“Rogue trading”

IT

Litiges clients

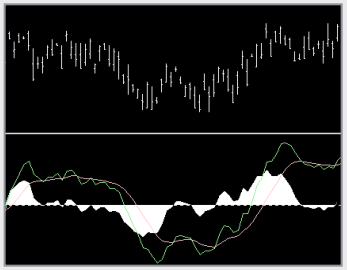
Fraude

Terrorisme

Innondation

Litiges / autorités

Erreur de pricing



RISQUES OPÉRATIONNELS

- **Le risque opérationnel n'est pas un risque nouveau et il est présent depuis longtemps dans les banques**

- **Il a pris une importance croissante en raison de la modification du cadre et de la conduite des activités bancaires (globalisation des marchés, essor des technologies, complexification des produits)**

- **Son univers est particulièrement large :**
  - Risques difficiles à identifier : une imbrication des causes, des événements et des effets, imbrication avec le risque de crédit et de marché (risques frontières)
  - Risques difficiles à mesurer : profil de pertes atypiques, coexistence de pertes directes et indirectes, insuffisance des historiques de données
  - Risques difficiles à surveiller et contrôler : coexistence de causes internes et externes, une occurrence et une sinistralité variables

RISQUES OPÉRATIONNELS

Les événements récents renforcent cette tendance :

- **Scandales financiers,**
- **Fraudes importantes dans le domaine bancaire**
- **11 Septembre,**
- **Coupures d'électricité (Etats Unis, Canada, Italie)**
- **SRAS, Grippe aviaire**
- **…**

RISQUES OPÉRATIONNELS

- **Bâle 2 répartit les sinistres par ligne métier (8 lignes métier) et catégories d'événements.**

- **Catégories d'événements :**

  - Internal fraud
  - External fraud
  - Employment practices and workplace safety : pertes dues au non respect des lois et des conventions protégeant les employés (sécurité, santé, …)
  - Clients products and business practices : pertes dues au non respect (involontaire) d'obligation vis à vis d'un client
  - Damage to physical assets : pertes dues à un endommagement des actifs physiques à cause des catastrophes naturelles
  - Business disruption and system failures
  - Execution delivery and process management : pertes dues au non respect des procédures liées à des transactions ou au management.

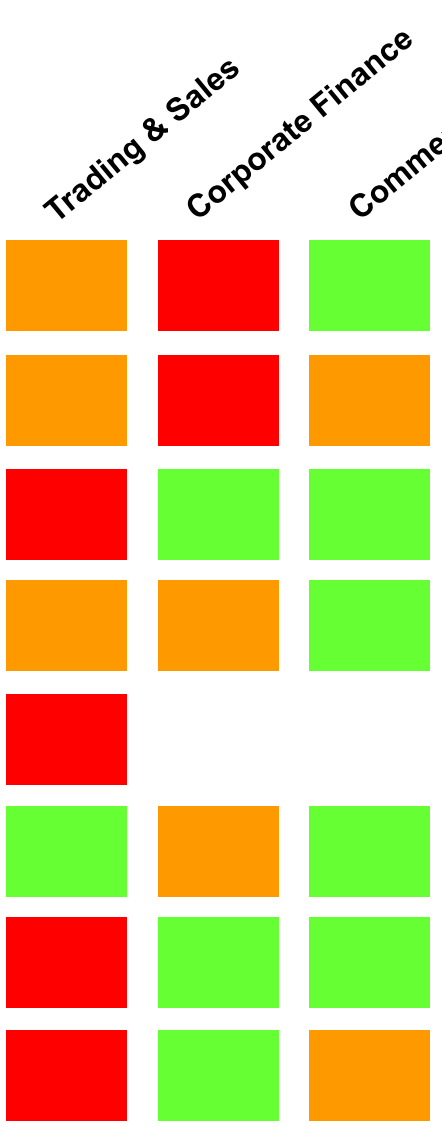
EXEMPLE DE CLASSIFICATION DES PERTES (8/49)

Commercial disputes	Disputes with authorities	Errors in pricing or risk evaluation	Execution errors	Fraud and other criminal activities	Rogue trading	Loss of operating environment/ capability	Systems interruptions
1. Disputes over advisory services provided	7. Breach of banking law	18. Deficiencies in the process for managing and monitoring limits and credit authorisations	22. Breakdown in settlements and or payments processes	33. Computer hacking and other malicious attacks on the bank's IT systems	39. Unauthorised activities on capital markets	40. Lack of personnel	44. Hardware failures
2. Improper business practices	8. Breach of diversity and discrimination laws	19. Non existent or inaccurate position (re)valuation	23. Confirmations failures	34. Other criminal activities against the bank's assets		41. Loss of data	45. Inconsistent data
3. Inadequacy of products offered	9. Breach of employment legislation	20. Poor market information	24. Errors arising in the general administration process over the tenor of a transaction	35. Robbery/ swindles/frauds committed by external parties		42. Loss of facilities	46. Poor management of projects
4. Inadequate customer care	10. Breach of environmental legislation	21. Pricing/valuation model errors	25. Errors in capture	36. Theft by internal parties(staff/ contractors engaged by the bank)		43. Loss of services	47. Software failures
5. Other disputes over third party agreements	11. Breach of requirements/ rules of organised markets		26. Inaccurate management information	37. Transactional fraud by staff or with its help			48. Weak logical environment
6. Unenforceable contract or transaction terms	12. Breach of health and safety standards		27. Inadequate exception reporting	38. Unauthorised use/misuse of proprietary or confidential information			49. Weak physical environment
	13. Breach of other statutory requirements		28. Inappropriate organisational structure/poor general control environment				
	14. Breach of regulatory requirements		29. Lack of safe custody relating to documents and/or valuable assets held on behalf of third parties				
	15. Breach of statutory accounting and disclosure requirements		30. Outsourcing/third party service delivery failures				
	16. Breach of tax legislation		31. Reconciliation failures				
	17. Money laundering and financial crime		32. Unapproved access given to customer accounts				

EXEMPLES EN BANQUES D'INVESTISSEMENT

Des risques nombreux et variés touchant la plupart des activités

- Litiges Commerciaux
- Litiges avec les autorités
- Erreur de pricing ou d'évaluation du risque
- Erreurs d'exécution
- "Rogue Trading"
- Fraude et activité criminelle
- Perte des moyens d'exploitation
- Interruption des systèmes



PILIER 2 : PROCESSUS DE SURVEILLANCE RENFORCÉ

- **Les banques doivent disposer de procédures d ’évaluation de leur FP en conformité avec leur profil de risques**

- **Les banques doivent mettre en place des procédures permettant d ’identifier, de mesurer, de piloter et de contrôler tous les risques qu’elles prennent.**

- **Les superviseurs doivent évaluer ces procédures et prendre les mesures nécessaires si elles ne leur semblent pas satisfaisantes**

- **Les superviseurs doivent pouvoir intervenir rapidement afin d ’éviter que le niveau de FP ne devienne inférieur au minimum requis**

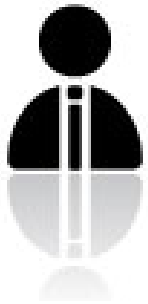
LES RÉGULATEURS

Rôle de la Commission Bancaire :

- Contrôler le respect des dispositions législatives et réglementaires
- Sanctionner les manquements constatés
- Examiner les conditions de leur exploitation et veiller à la qualité de leur situation financière
- Veiller au respect des règles de bonne conduite de la profession

Rôle de l'AMF :

- Régularité des opérations sur titres faisant appel public à l'épargne



LE 97-02 – RÔLE DU CONTRÔLE INTERNE

- **Vérifier que l'organisation et les procédures internes sont conformes aux dispositions de nature législative ou réglementaire, aux normes professionnelles et déontologiques ou aux instructions internes.**

- **Vérifier que les procédures de décisions de prise de risques et les normes de gestion fixées (notamment sous forme de limites) sont strictement respectées.**

- **Vérifier la qualité de l'information comptable, financière, des systèmes d'information et de communication**

- **Vérifier les conditions d'évaluation, d'enregistrement, de conservation et de disponibilité de cette information, notamment en garantissant l'existence d'une piste d'audit**

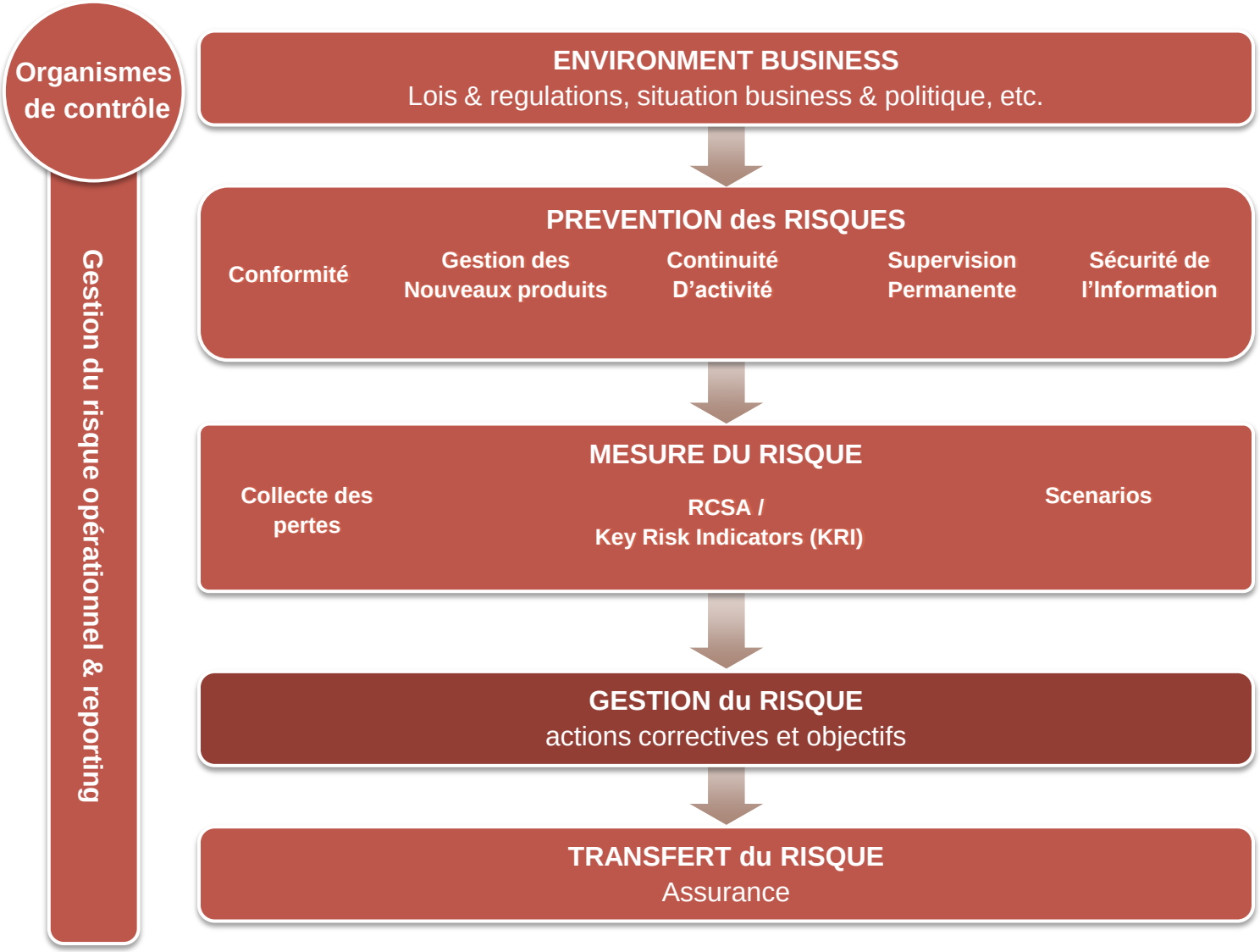
MISE EN PLACE D'UN DISPOSITIF DE GESTION DES RISQUES OPÉRATIONNELS

ETAT DES LIEUX

La plupart des banques ont développé un dispositif de gestion des risques afin de satisfaire aux exigences réglementaires :

- **Politiques et directives**
- **Collecte des pertes**
- **Identification et analyse des risques**
- **Allocation de capital en fonds propres**
- **Dispositif de réduction des risques et de suivi des plan d'action**
- **Contrôle & mesure**
- **Reporting**

EXEMPLE DE CYCLE DE GESTION DES RISQUES OPERATIONNELS



PRÉVENTION : SUPERVISION PERMANENTE

- **Objectif : système de contrôles formalisés, de règles, méthodes et procédures utilisées afin d'assurer la sécurité, la validité et l'efficacité des opérations.**

- **Une Supervision Permanente efficace :**
  - Sécurise les activités quotidiennes
  - Met en œuvre les contrôles adéquats
  - Analyse les dysfonctionnements et permet le lancement d'actions correctrices.

- **Une responsabilité à tous les niveaux de la structure sous la responsabilité du Management**

PRÉVENTION : CONTINUITÉ D'ACTIVITÉ (PCA)

Objectifs :

- Protéger les employés, préserver la réputation, s'assurer de la continuité des process clés, des produits et des services.
- Une capacité de réponse aux désastres, crises et incidents
- Une obligation réglementaire

Un plan de continuité efficace est :

- **Opérationnel** : il marche et peut être invoqué à tout moment
- **Extensible** : Il peut être invoqué pour tout ou partie des scénarios
- **Complet** : Les fonctions clés de l'entreprise sont couvertes en un temps minimum
- **Cohérent** : Il est mis en place en accord avec les normes et les meilleures pratiques en vigueur
- **Mis à jour** : Toutes les informations sont à jour et répercutées dans le plan
- **Documenté** : Toutes les procédures sont entièrement documentées
- **Testé** : Le plan est régulièrement testé en grandeur nature

Chaque entité / département est responsable et définit son plan de continuité en s'assurant de la cohérence avec les objectifs et la stratégie de l'entreprise.

MESURE : COLLECTE DES PERTES OPÉRATIONNELLES

Objectifs

- Mettre en place une structure de remontée des pertes opérationnelles quasi temps-réel
- Permettre l'explication, l'analyse et la catégorisation de chaque perte
- Mettre en place un reporting précis par Business, Département, catégorie de perte …
- Permettre la constitution de statistiques de distribution de pertes afin d'alimenter le calcul du capital RO
- Lancer des actions correctrices immédiates afin d'éviter la récurrence d'une même perte.
- Satisfaire à une exigence réglementaire (historique min. de 5 ans)

Critères d'un process efficace de collecte :

- Rapidité et fluidité : Chaque perte doit être reportée immédiatement par le réseau de correspondants
- Qualité : Les saisies doivent être factuelles, référencées et accompagnées de toutes les pièces justificatives
- Exhaustivité : Tous les incidents doivent être remontés

MESURE : RISK & CONTROL SELF ASSESSMENT ET KRI

Objectifs du RCSA

- Evaluer l'exposition de l'entreprise aux risques opérationnels d'un point de vue qualitatif
- En utilisant un outil de supervision pour les "Risk Managers" et la Direction destiné à alimenter pour chaque activité son profil de risque, identifier les zones les plus risquées et mettre en place des actions préventives et correctrices.
- Utilisé annuellement, via une série de questionnaires auto-déclaratifs

Mise en place d'indicateurs de risque (Key Risk Indicators)

- Permettre une gestion proactive des risques grâce à une mesure précise
- Analyser l'évolution des risques et pouvoir se comparer
- Satisfaire une exigence réglementaire

MESURE : ANALYSE DE SCENARIOS

Qu'est ce qu'un scénario ?

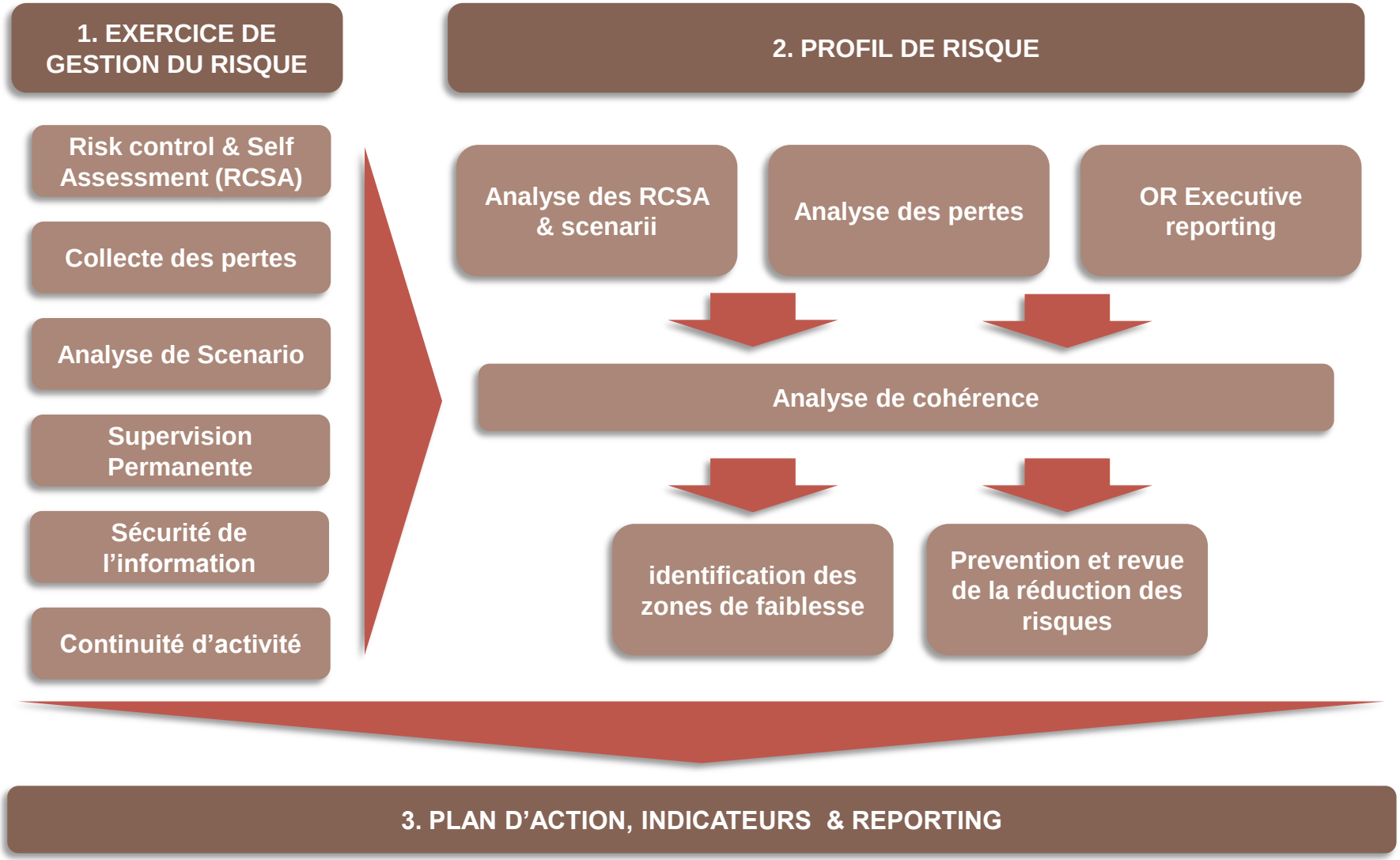
- Un scénario est un évènement imaginaire de risque extrême ou non (encore) avéré.
- Il est analysé en terme de potentialité, d'impact tant humain que financier

Objectifs :

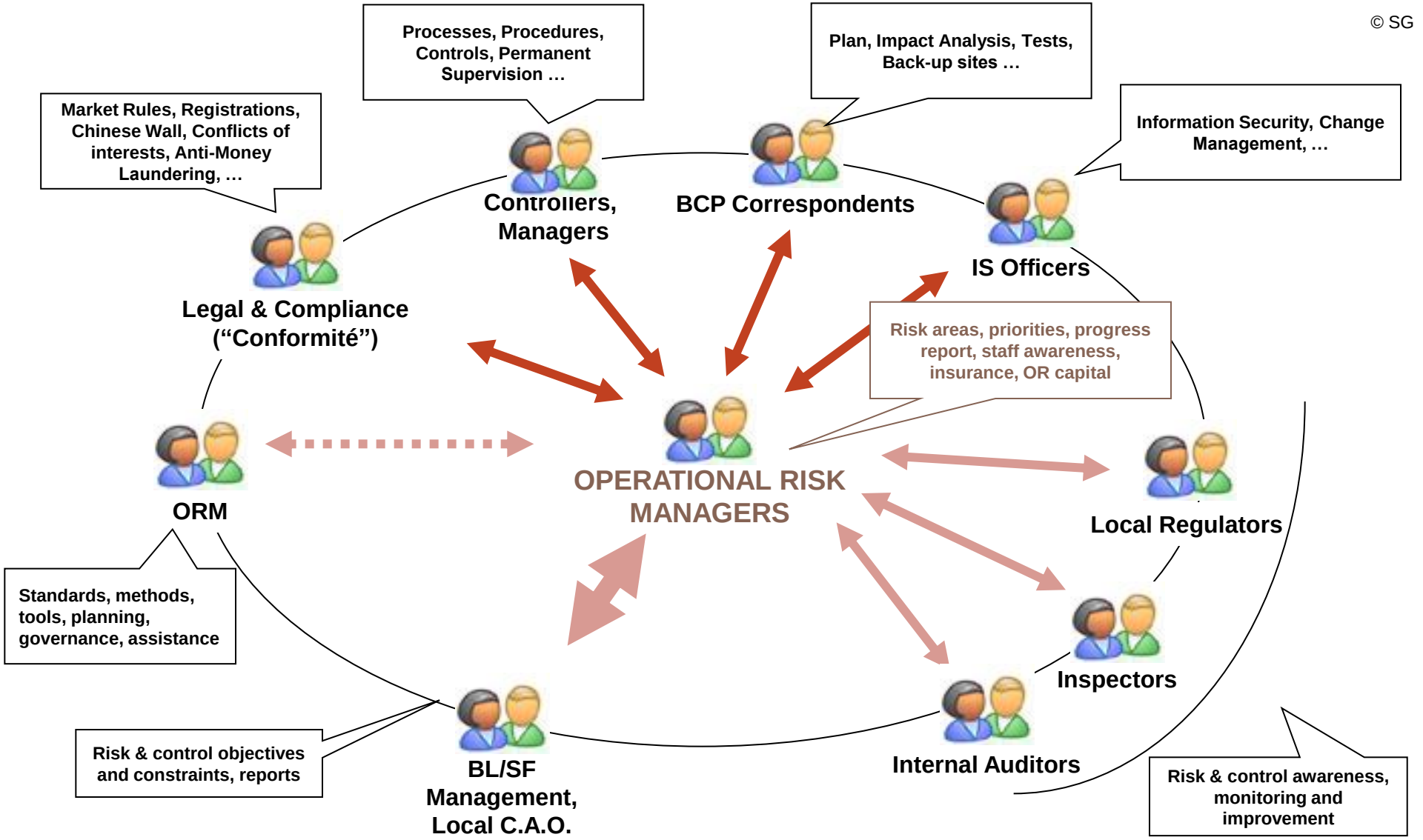
- Evaluer l'exposition de l'entreprise aux risques extrêmes, en accord avec les régulateurs
- Disposer d'une base de scénarios pour compléter les études effectuées avec la base de collecte des pertes
- Mettre en place un outil d'analyse permettant aux managers de tester leur environnement de contrôle, évaluer leur risques opérationnels et définir des plans d'action préventifs.

Un scénario peut avoir un impact sur l'allocation en fonds propres au titre du risque opérationnel

CONSTRUCTION D'UN PROFIL DE RISQUE



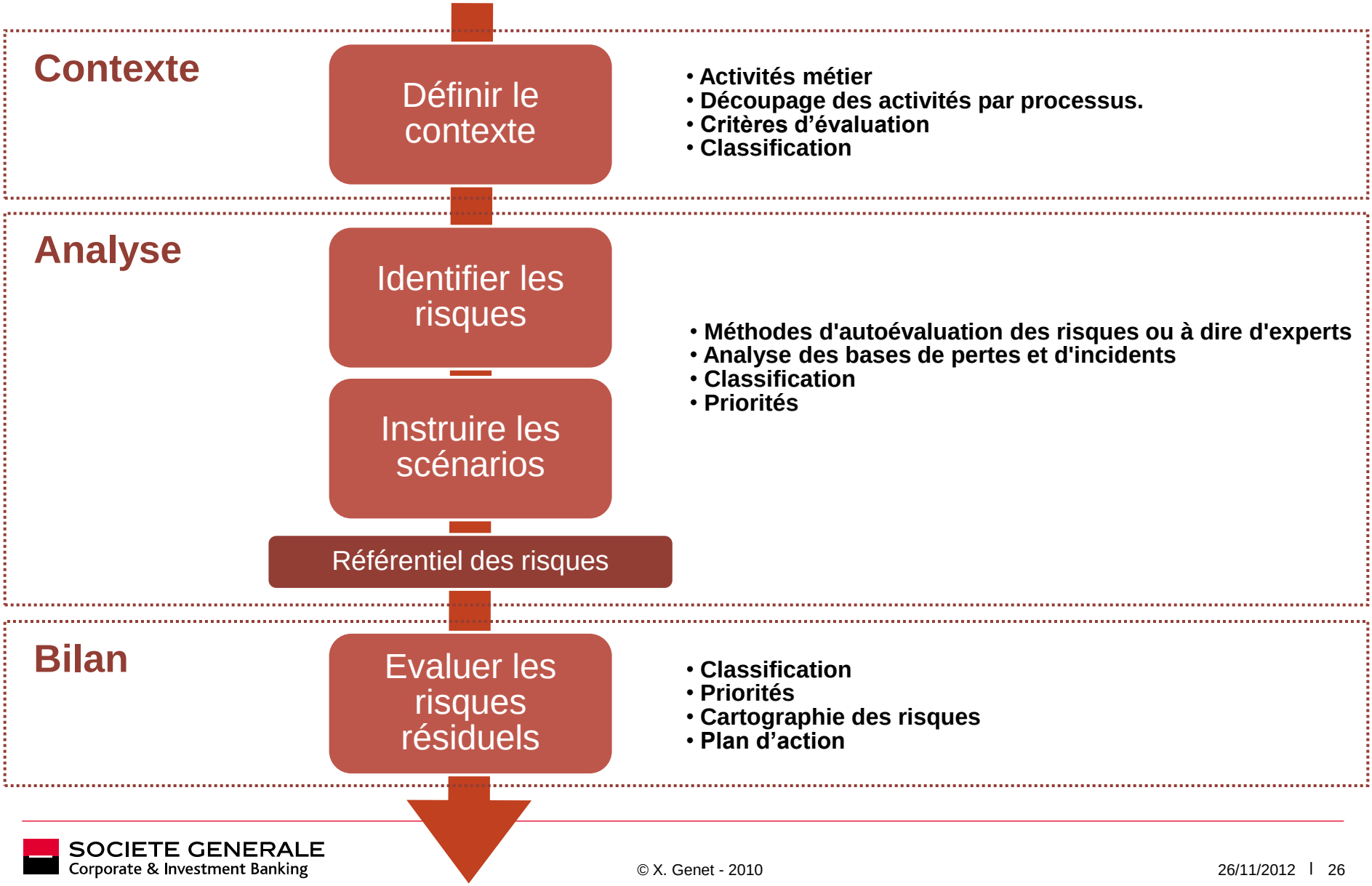
ORGANISATION DE LA GESTION DES RISQUES OPERATIONNELS



RISK MANAGEMENT

Penser à l'impensable …

LES ÉTAPES CLÉS D'UNE ANALYSE DE RISQUES



GRAVITÉ DES SCÉNARIOS

Potentialité	
4	Très probable (court terme)
3	Probable (long terme)
2	Possible bien que peu probable
1	Très peu probable
0	Impossible

Impact	
4	Catastrophique
3	Très grave
2	Grave
1	Moyen
0	Nul

- **La mesure du niveau de gravité se fait en attribuant à chaque scénario:**
  - Sa potentialité
  - Son niveau d'impact résiduel sur les activités
  - La gravité est ensuite déterminée à l'aide d'une grille d'aversion des risques

Grille d'aversion des risques

P \ I	0	1	2	3	4
4	0	1	2	3	4
3	0	1	2	3	4
2	0	1	1	3	4
1	0	0	1	2	3
0	0	0	0	0	0

Gravité	
4	Stratégique
3	Critique
2	Important
1	Moyen
0	Nul

METHODOLOGIES DE RISK MANAGEMENT

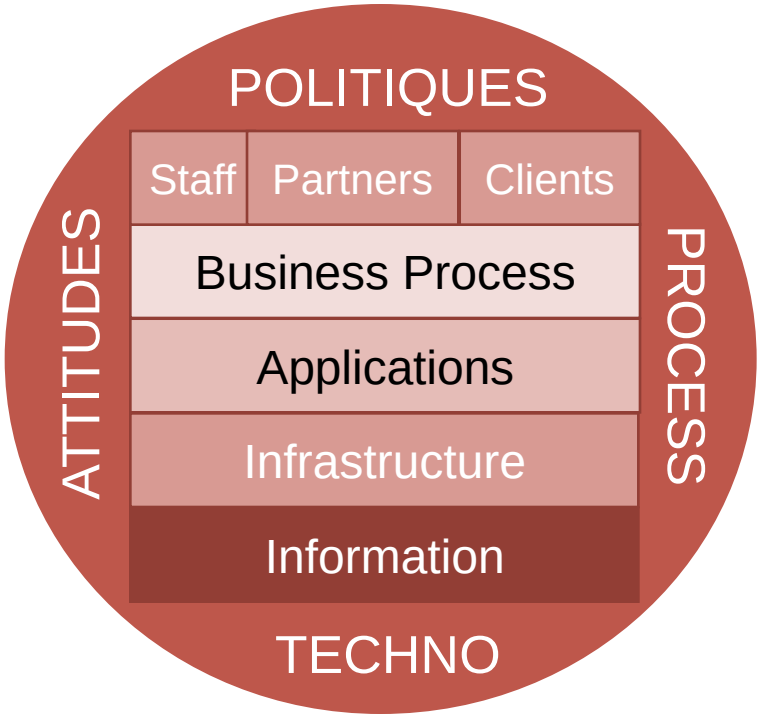
- **Des centaines de méthodologies existent, optimisées par métiers et types de risques.**

- **Methodologies les plus courantes :**

  - COBIT
  - OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)
  - NIST – 800-30, Risk Management Methodology
  - COSO – Enterprise Risk Management Framework (PwC)
  - SAS Risk Management
  - IRMF - Integrated Risk Management Framework
  - FRAP – Facilitated Risk Analysis Process
  - DRAM – Delphic Risk Assessment Methodology
  - Mehari …

RISK MANAGEMENT : UN COMPOSANT À PART ENTIÈRE DU BUSINESS

- **Le “Risk management” ne peut pas seulement être efficace avec de la technologie ou de la gestion de process. C’est un des fondamentaux de la culture d’entreprise.**
- **Il nécessite des changements culturels et d’organisation à tous les niveaux.**
- **100% de mitigation du risque est impossible. L’objectif est d’investir à des niveaux adéquats.**
- **Le “Risk management” doit accompagner le Business, pas le freiner …**



CONCLUSION

"We've considered every potential risk except the risks of avoiding all risks."

BANQUES : UN CONSTAT MITIGÉ

- **Approche souvent trop réglementaire**
- **Environnement de contrôle trop fragmenté**
- **Corrélation et communication diffuse**
- **Rôles et responsabilités vagues**
- **Difficulté à obtenir une vue intégrée des risques**
- **Génération d'un sentiment de sécurité factice**
- **Approche réactive plutôt que proactive**
- **Sensibilisation déficiente**

La plupart des dispositifs de gestion des risques opérationnels ne peuvent pas protéger les banques de risques extrêmes.

DE NOUVELLES PRIORITÉS …

- **Contrôles : moins de contrôles MAIS de meilleurs contrôles tout en accompagnant le business**
- **Proactivité vs Réactivité : traiter les incidents avant qu'ils ne deviennent des problèmes.**
- **Integration vs segrégation: convertir les signaux faibles en alertes concrètes.**
- **Culture & Responsabilisation : Rendre chaque employé responsable et attentif**
- **Organisation : renforcer les changement structurels afin de réduire les risques opérationnels.**

5 COMMANDEMENTS *

- **Il n'y a pas de bonne maîtrise des risques, sans vision prospective**
- **Il n'y a pas de gains sans prise de risques**
- **Le traitement d'un risque crée souvent un autre risque**
- **Plus on complexifie, plus on crée des risques**
- **L'homme est au cœur du système**

* d'après les propos d'Alexandre Tedeschi Administrateur du CNISF et Spécialiste en gestion des risques

QUESTIONS

OPERATIONAL RISK CASE STUDY

Rogue Trading at Société Générale Management

ROGUE TRADING MOST FAMOUS CASES

Barings, Singapore, Index derivatives.
Loss : $1.3 billion
February, 1995

Allied Irish Bank, New York, FX Forwards.
Loss : $691 million
2002

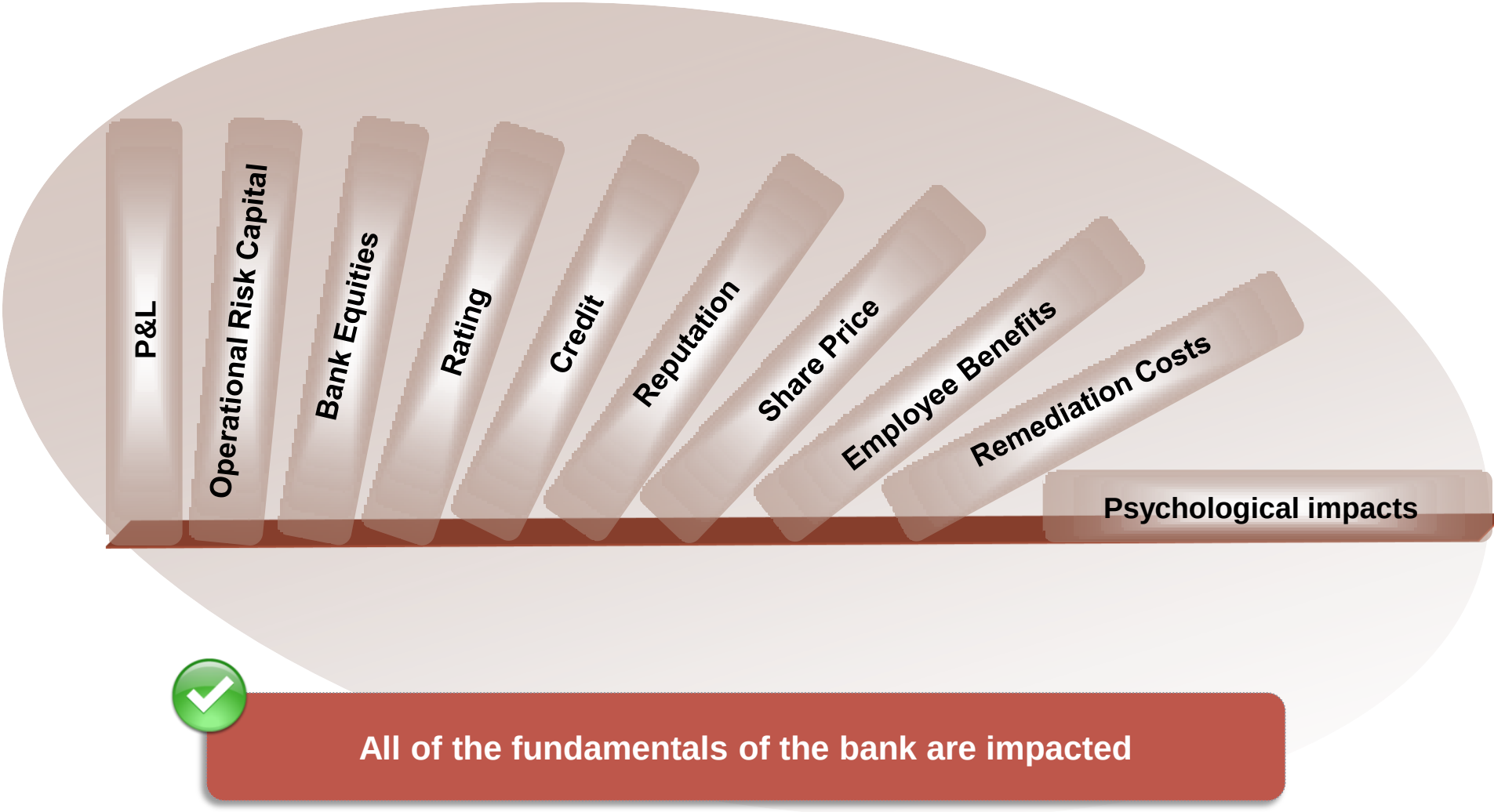
CALYON, New York, credit market indices.
Loss : €250 million
September 18, 2007

Sumitomo Corp
Loss : €1,75 Billion
1996

Daiwa Bank,
Loss : €743 Million
1996


INTERNATIONAL
Herald Tribune
Société Générale loses $7 billion in trading fraud

LOSS IMPACTS



All of the fundamentals of the bank are impacted

ROGUE TRADING DEFINITION

- **Definition : Rogue trading is “Unauthorized employee activities on capital markets”**

- **Rogue Trader literally means “unscrupulous trader”.**
  - Manipulating Position
  - Manipulating PnL

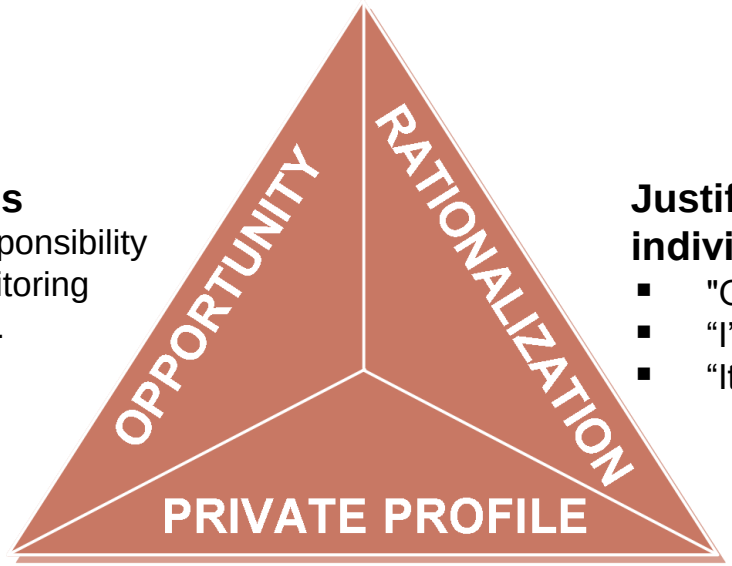
- **Different from others kinds of fraud :**
  - Theft, money laundering, misappropriation of funds , …

ROGUE TRADING CONDITIONS

OPPORTUNITY

Weak internal controls

- Lack of clear lines of responsibility
- sufficient employee monitoring
- Segregation of duties…).



Adapted from AICPA, 2006

RATIONALIZATION

Justification according to the individual's own code of ethics

- "Others are doing it"
- "I'll beat my colleagues/competitors"
- "It is for a good purpose" …

PRIVATE PROFILE

From the employee's personal life

- Ego, Psychological profile
- Low income, Personal financial problems, etc…

When all three of these forces are present, then risk of rogue trading is very high. Financial institutions should effectively act upon all three.

PREVENTION, AWARENESS, INFORMATION

JOB ENVIRONMENT SECURITY

DETECTION

PREVENTION : BEST PRACTICES TO CONSIDER

Why look at Prevention?

A solid prevention system focuses on rogue trading **mitigating factors**. Such prevention is **key to deterring rogue trading**

Transversal controls system

Exhaustiveness of internal controls

Staff management & education

Ethics Policy

Information System security

JOB ENVIRONMENT SECURITY : BEST PRACTICES TO CONSIDER

Why look at Environment?

A secured environment **mitigates the opportunity** to commit rogue trading

Segregation of duties

Management oversight

Team work to prevent isolated traders

Effective worldwide monitoring

DETECTION : BEST PRACTICES TO CONSIDER

Why look at Detection?

Fast and appropriate detection measures will **prevent** rogue trading as well as **lower** its impact

PNL Justification

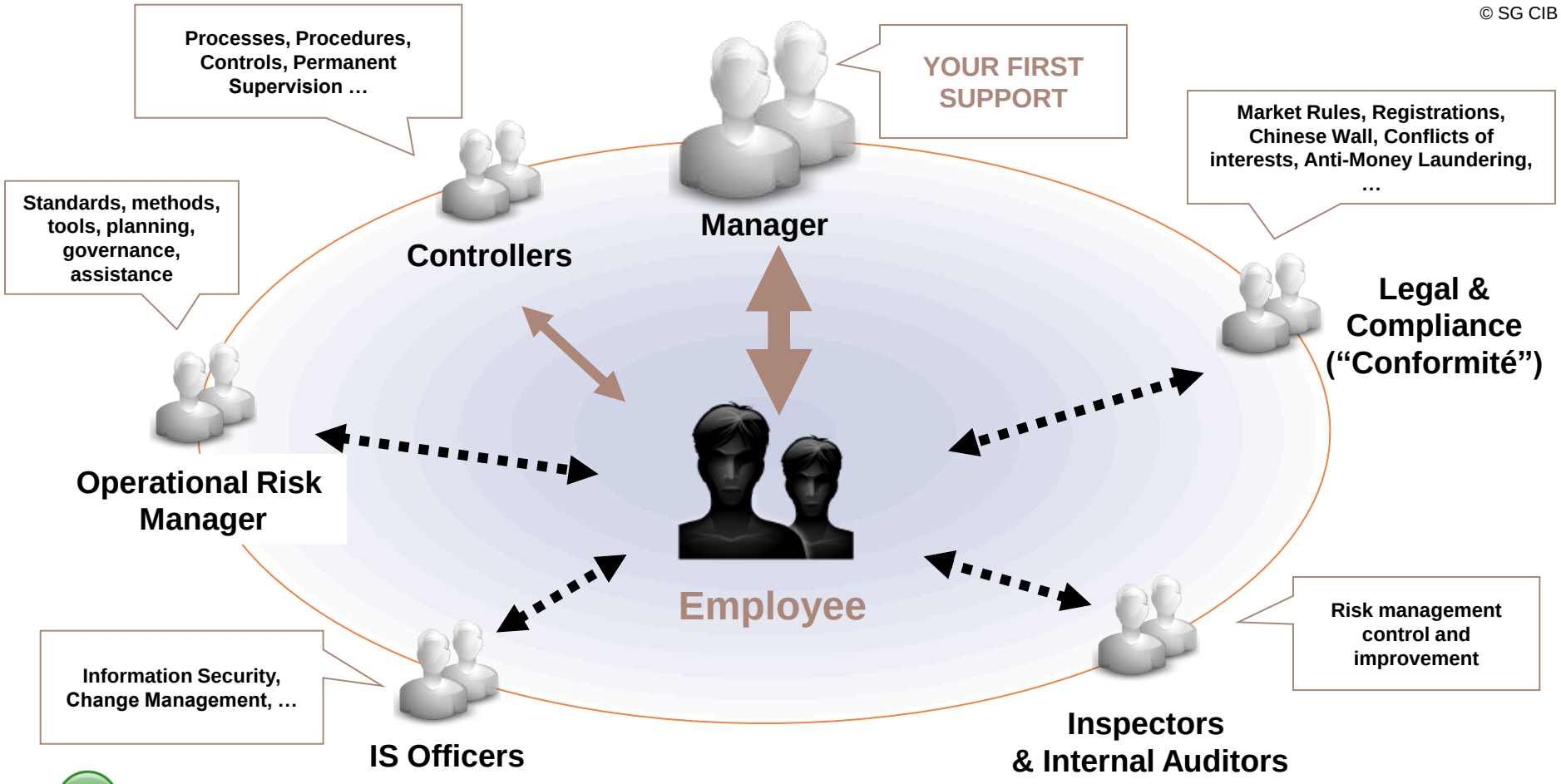
Limit monitoring

Hotline & whistle blowing

Transversal interpretation of alerts

Un-reconciled databases

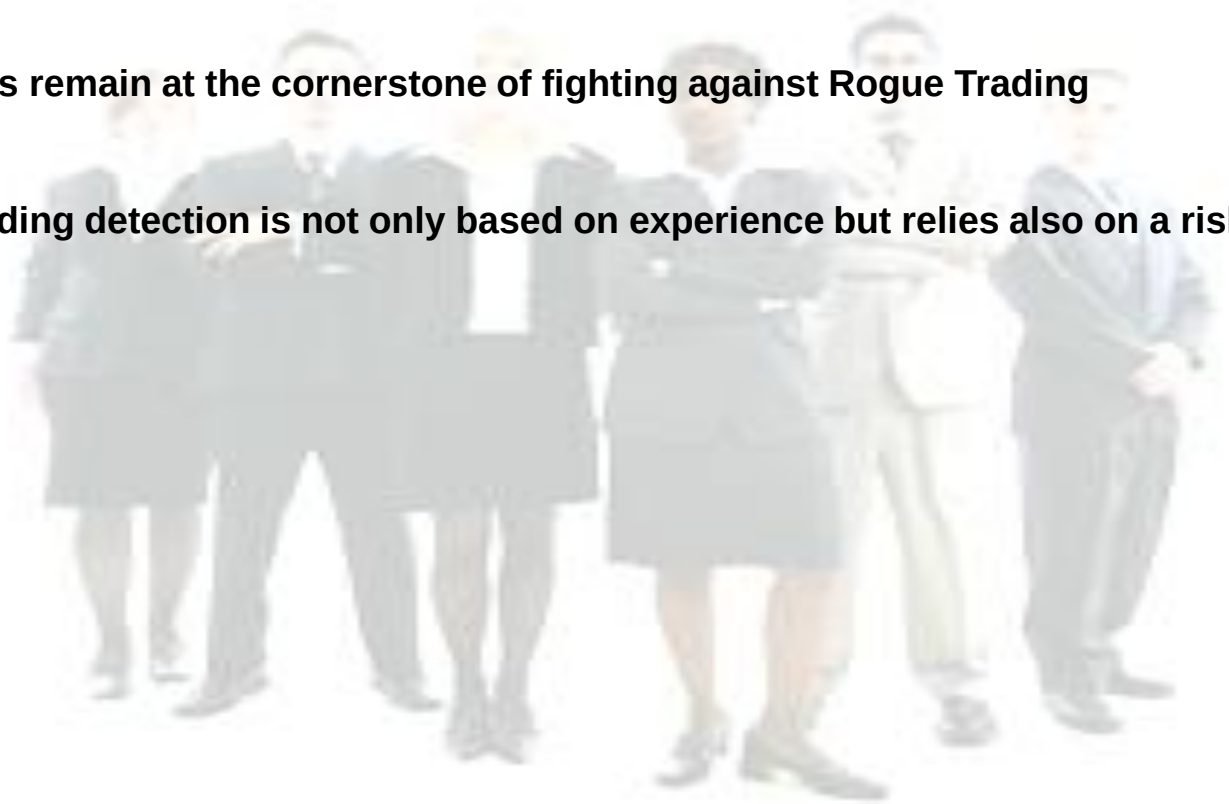
STAFF : CORNERSTONE TO FIGHT ROGUE TRADING



Reporting to direct management in case of anomalies is the first action, but dedicated specialists are here to help too.

LESSONS LEARNT

- **HUMAN FACTOR is the only common element to all studied cases**
- **Employees remain at the cornerstone of fighting against Rogue Trading**
- **Rogue trading detection is not only based on experience but relies also on a risk culture**



Risk culture provides the best conditions to detect rogue trading.
This culture should be owned by each individual and promoted by management.

QUESTIONS