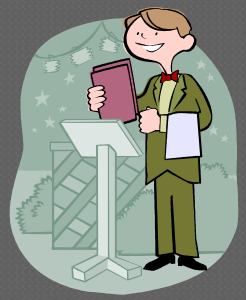
COMMENT INDUSTRIALISER LE PROCESSUS DE GESTION DES RISQUES

JEAN LARROUMETS
Co-fondateur FIDENS
Consultant en Sécurité des Systèmes d'Information

fidens
Sécurité des Systèmes d'Information

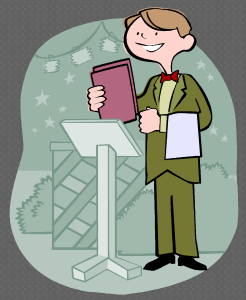
Jean Larroumets

- Consultant sécurité des SI et Co-fondateur de Fidens
  - Chef de produit logiciel EGERIE Risk Manager SIO27005
  - Certifié Lead Auditor ISO27001 (BSI)
  - Formateur Agréé LSTI
    - Risk Manager ISO27005 / LA_ISO27001/LI_ISO27001
  - Membre du club EBIOS (V2 / V2010)
  - Membre du Clusif
  - Membre du Club ISO27001



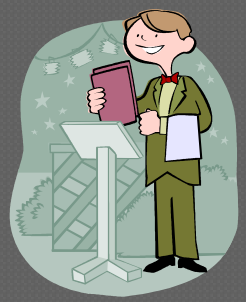
Plan

- Introduction
- Réglementation
- Norme ISO27005
- Constats et approches observées
- Industrialisation du Risk Management
- Retour d'expérience
- Conclusion



Plan

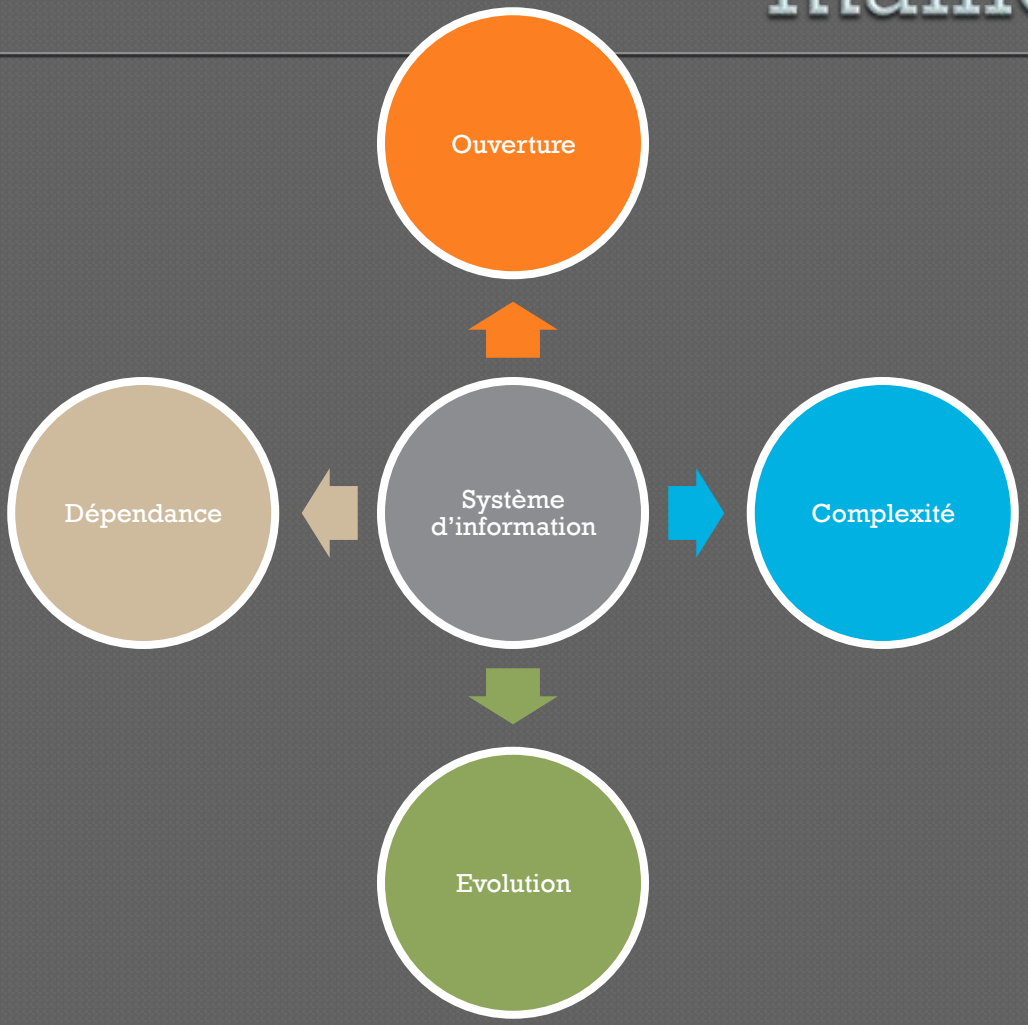
- Introduction
- Réglementation
- Norme ISO27005
- Constats et approches observées
- Industrialisation du Risk Management
- Retour d'expérience
- Conclusion



Constat

Les risques informatiques évoluent constamment, les bonnes pratiques ne sont pas toujours respectées et, s'il peut paraître difficile de procéder à une analyse de ses risques ; il l'est plus encore de maintenir celle-ci à jour…

Le Système d'information : le maillon faible



Management par le risque

Créer et préserver la valeur

- les actifs et la réputation de la société

Sécuriser la prise de décision

- les processus de la société, pour favoriser l'atteinte des objectifs

Favoriser la cohérence des actions

- avec les valeurs de la société

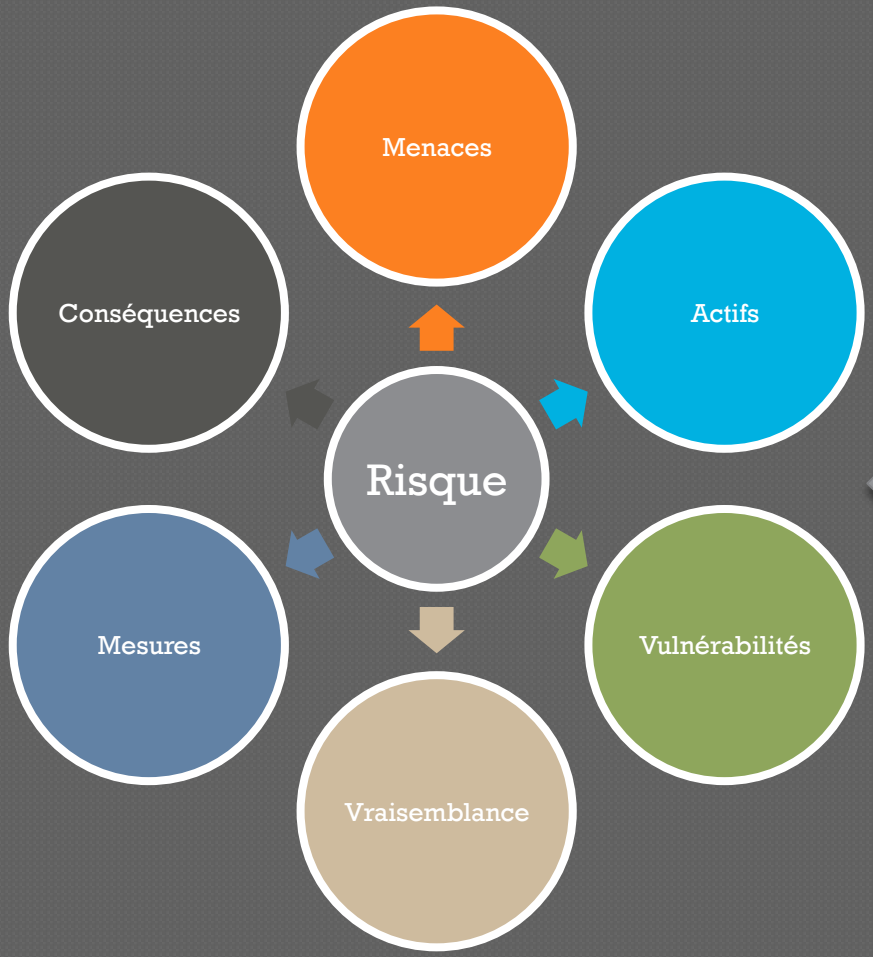
Mobiliser les collaborateurs et direction

- autour d'une vision commune des risques

Management par le risque

- Développer une culture sécurité raisonnée

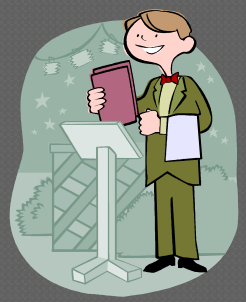
Risque (ISO27005)



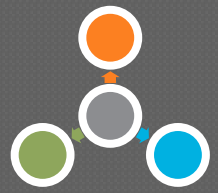
- Identifier les risques
- Estimer les risques
- Evaluer les risques
- Traiter les risques
- Accepter les risques

Plan

- Introduction
- Réglementation
- Norme ISO27005
- Constats et approches observées
- Industrialisation du Risk Management
- Retour d'expérience
- Conclusion



Les règlementations



- Administrations françaises
  - Référentiel Général de Sécurité
    - Publié le 18 mai 2010 (application définitive le 17 mai 2013)
    - Article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005
    - Relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
- Secteur Banque / Assurance
  - Bâle III /SOLVABILITY II
    - BIII (Publié le 16 décembre 2010) /SII (voté le 22 avril 2009)
    - Proposition de réglementation bancaire/assurance suite à la crise financière de 2007
    - Gestion des risques opérationnels (y compris SI)
    - S'assurer que la compagnie est bien gérée et est en mesure de calculer et maîtriser ses risques

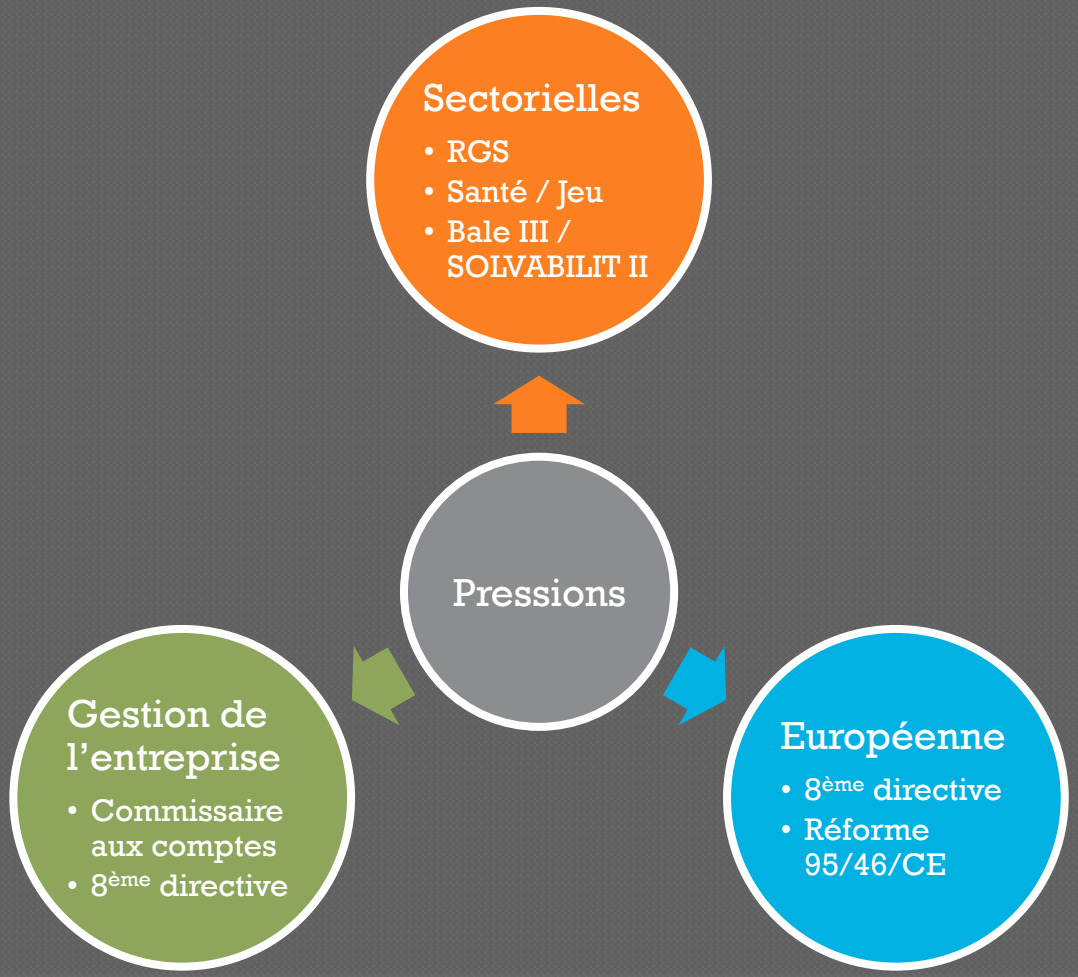
Les règlementations

- Directives européennes
  - Loi du 3 juillet 2008 et l'ordonnance du 8 décembre 2008 ont transposé en droit français les directives européennes
    - Directive européenne audit légal 2006/43/CE (dite 8ème directive) (article 41)
      - qui imposent de nouvelles obligations aux sociétés cotées en matière de gestion des risques (contrôle légal des comptes)
  - Projet de réforme de la Directive européenne n°95 /46/CE (article 33 du projet)
    - Rend obligatoire la réalisation l'analyse et la gestion des risques par l'entreprise sur la protection des données à caractère personnel

Les règlementations

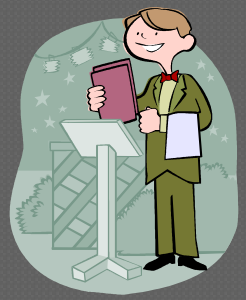
- Données personnelles
  - CIL (CNIL) / Futur DPO (Data Protection Officer)
    - Evolution de la fonction : « Tenir la liste des traitement » à être « Responsable de traitements » de données à caractère personnel
- Données classifiées et homologation
  - IGI 920 / IGI 1300
  - Homologation de système sur la base d'une analyse de risque (FEROS)
- Autres Réglementations
  - Santé, Jeu, Sarbanes-Oxley, Loi de Sécurité Financière, Loi sur les Nouvelles Régulations Economiques, …

La pression règlementaire s'accentue



Plan

- Introduction
- Réglementation
- Norme ISO27005
- Constats et approches observées
- Industrialisation du Risk Management
- Retour d'expérience
- Conclusion



Normes et méthodes de management du risque

Management du risque

- **ISO 31000 (2009)** — Management du risque
- **ISO 31010 (2009)** — Management du risque : Guide
- **ISO Guide 73 (2009)** — Management des risques : Vocabulaire
- **ISO 13335 (2004)** — IT – Security Techniques

IT

Sécurité des Systèmes d'information

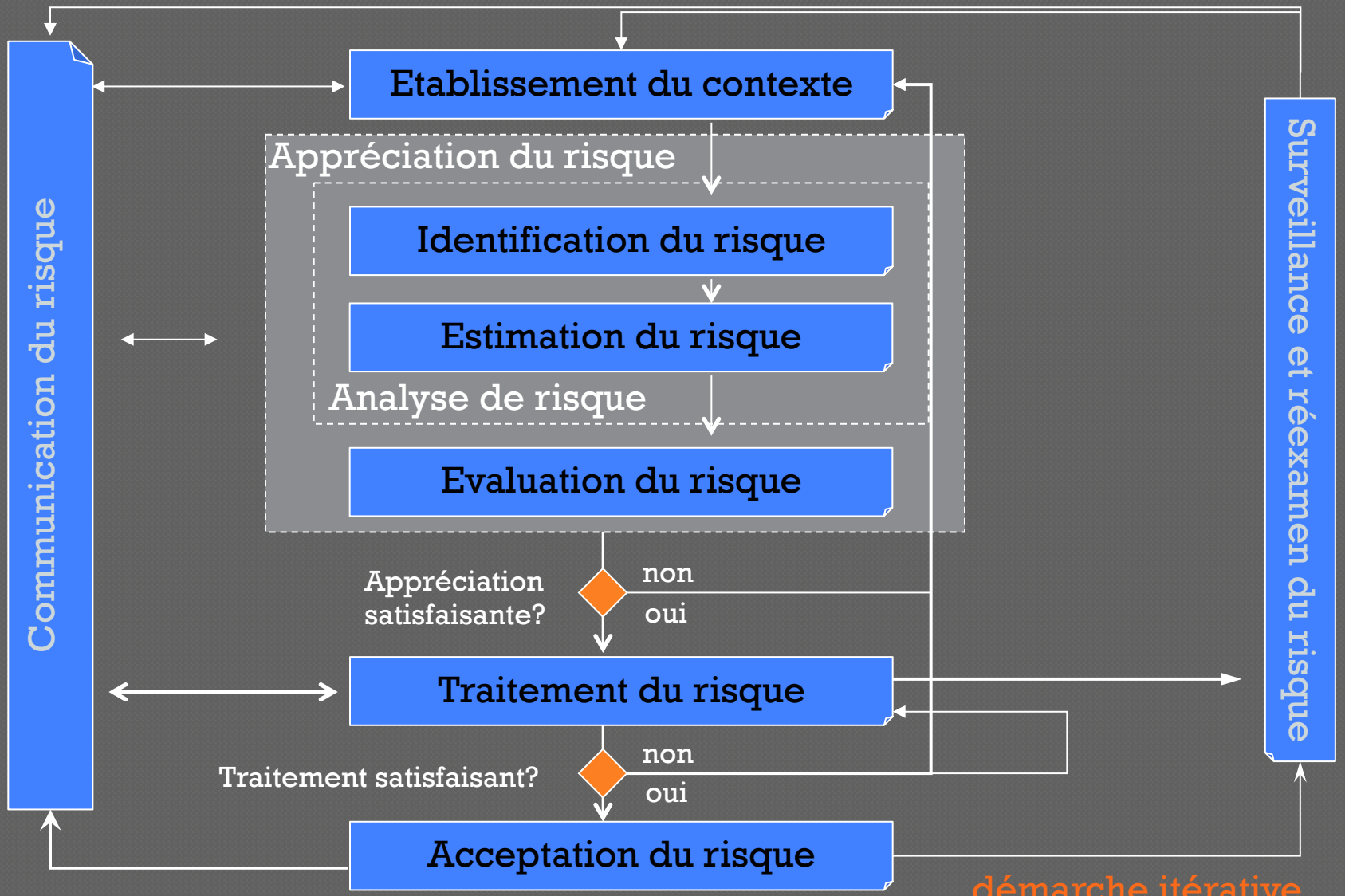
- **ISO 27001 (2005)** — SMSI : exigences et guides
- **ISO 27005 (2008/2011)** — Gestion du risque en sécurité de l'information

Méthodes

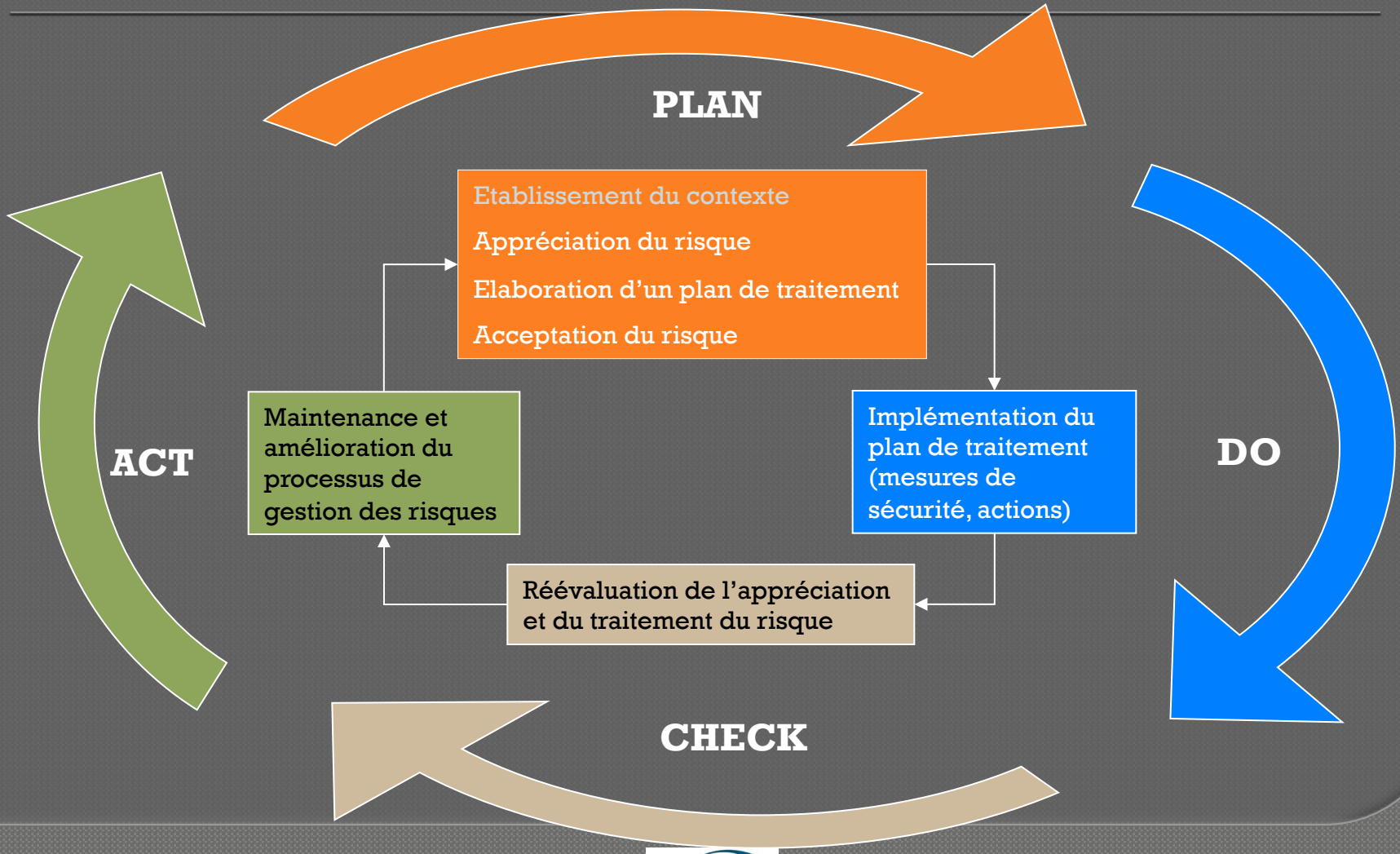
- **CRAMM (2005)**
- **EBIOS (2010)**
- **MEHARI (2010)**
- **OCTAVE (2007)**

Norme ISO27005

- Définir une démarche de gestion de risques appropriée à la mise en place d'un SMSI
  - Participation française (SGDSN) importante
  - Delta entre démarche et méthode (EBIOS)
  - Base GMITS, puis ISO 31000 et ISO 13335
  - 1ère version en 2008, mise à jour en mai 2011
- Répond directement aux exigences de la norme ISO 27001 (certifiante)
  - 4.2.1 c) d) e) f) g) h) i) j)
  - Garantit de reproductibilité des résultats
  - Alimente les comités de direction



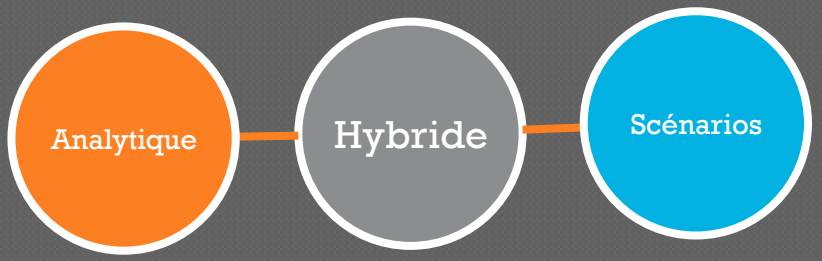
Norme ISO27005 (Alignement vision SMSI)



Contributions de l'ISO27005

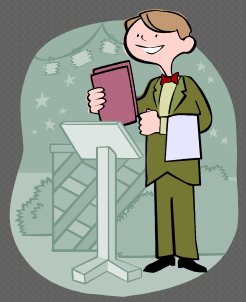
Choix d'une méthode

- Méthode analytique (EBIOS)
  - Entités unitaires assemblées
    - Menaces – Actifs en support – Vulnérabilités – Actifs primordiaux – Impacts
- Méthode par scénarios (Mehari)
  - Liste de scénarios
- Méthode hybride
  - Base : analytique
  - Outillage : scénarios



Plan

- Introduction
- Réglementation
- Norme ISO27005
- **Constats et approches observées**
- Industrialisation du Risk Management
- Retour d'expérience
- Conclusion



Constat - Ce que disent nos clients

- Difficultés dans l'appréciation des risques
  - Compétences / Méthodes
  - Focalisation sur le rapport (DS / FEROS)

- Pas ou peu de mutualisation
  - « From scratch » pour chaque projet
  - Difficultés dans le partage de la méthode et des référentiels
  - Multiplication des coûts (7 à 20K€ par projet)

Constat - Ce que disent nos clients

- Difficultés dans la gestion des risques
  - Pas de mise à jour et maintien des risques
  - Peu d'indicateurs
    - Notamment d 'évolution
  - Difficultés pour arbitrage et la réactivité
  - Implication de la direction

- Absence d'outil
  - Excel, excel, excel, excel, …

Approches observées

Approche (par périmètre)

- Cartographie globale des risques
- Cartographie sur un périmètre règlementé
- Système existant

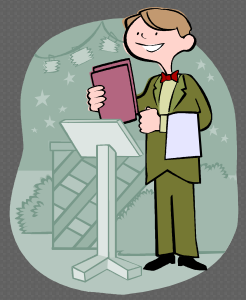
Approche (par processus de rénovation)

- Cartographie consolidée sur la base de la prise en compte de la sécurité dans les projets
- Système à concevoir ou rénover

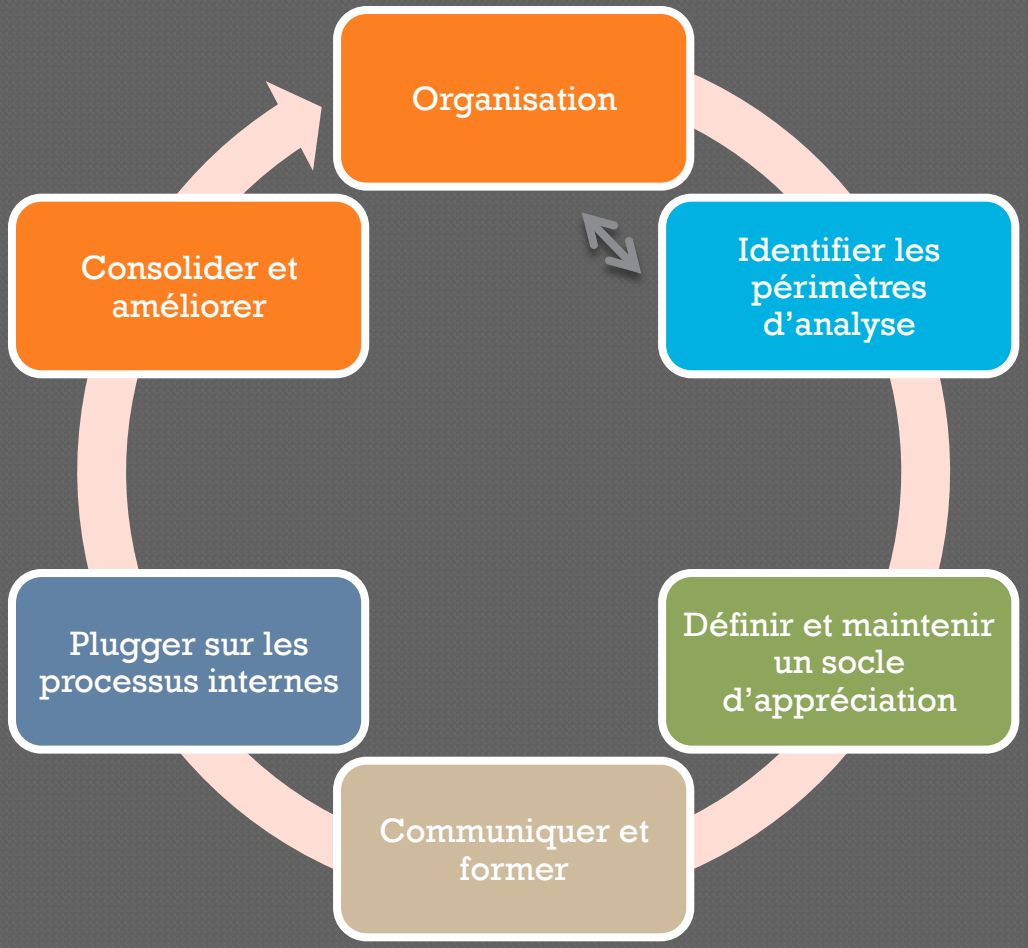
Approche combinée

Plan

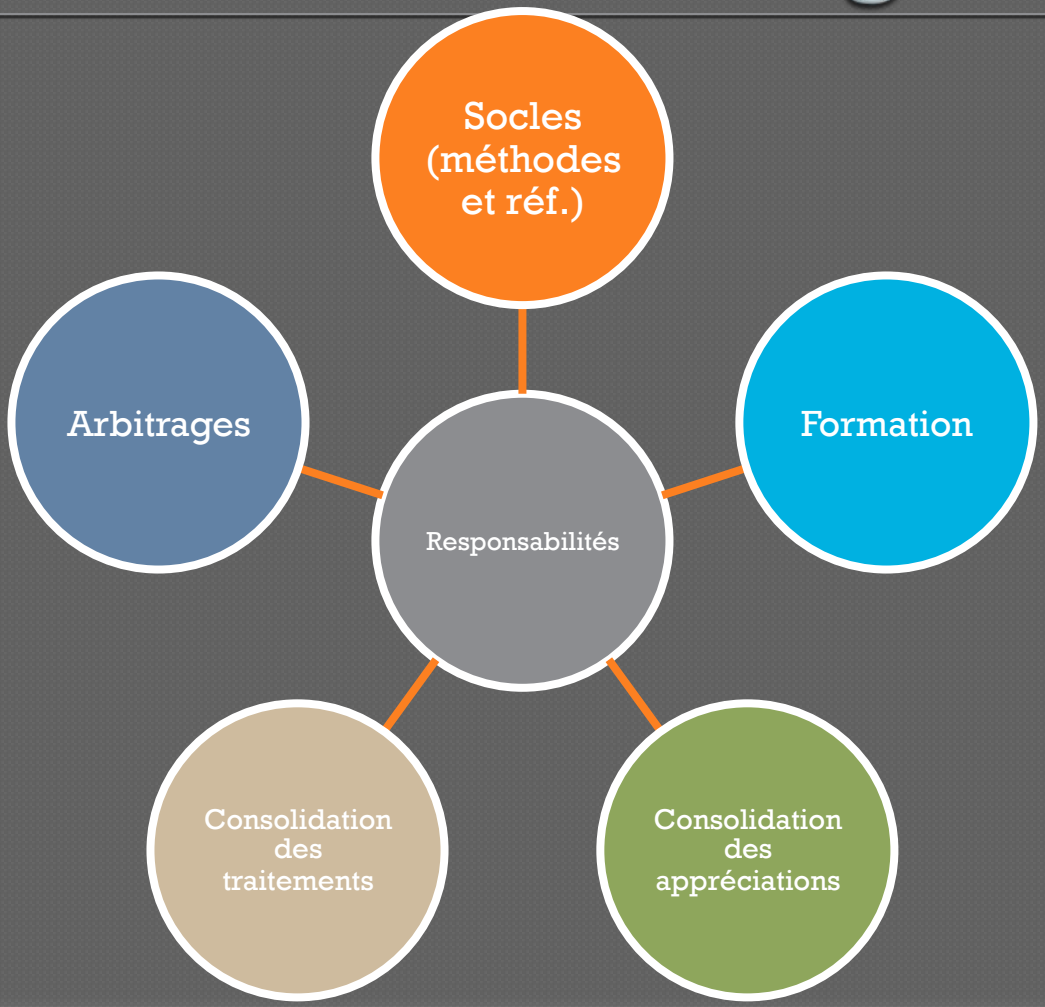
- Introduction
- Réglementation
- Norme ISO27005
- Constats et approches observées
- **Industrialisation du Risk Management**
- Retour d'expérience
- Conclusion



Comment industrialiser le processus de gestion des risques



Organisation



Organisation

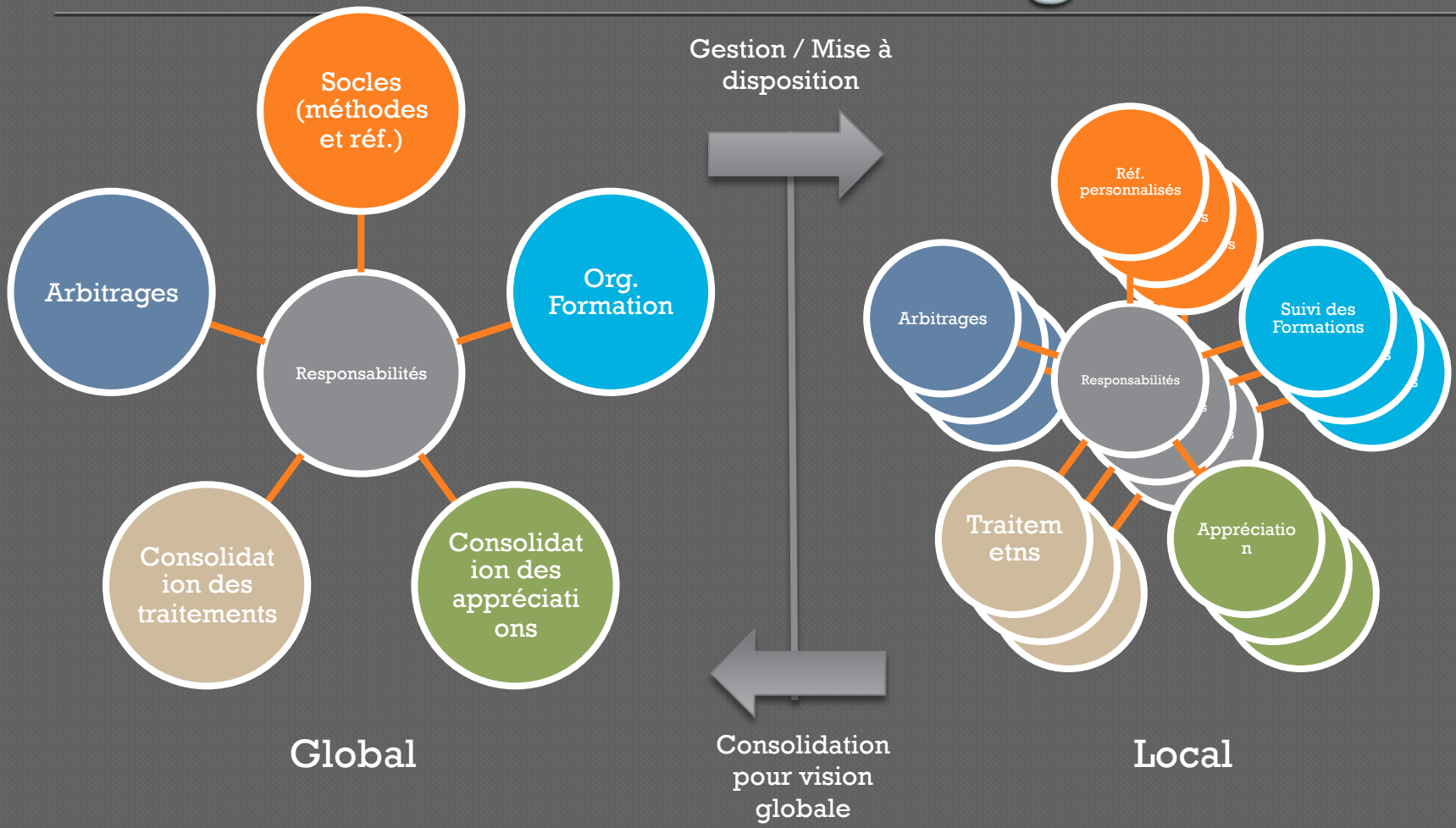
- Maintien du socle d'appréciation
  - Risk Manager (méthode / métrique)
  - RSSI / Cellule sécurité (référentiels)
- Appréciation
  - RSSI / Cellule sécurité
  - Equipes Projets
- Arbitrages
  - Direction générale / CoDir
  - Sponsor du projet / directeur de projet
- Traitement
  - DSI
  - Equipe sécurité
- Formation
  - Risk Manager
  - Service formation
- Consolidation
  - Risques : Risk Manager
  - Traitements : RSS / DSI
- Amélioration
  - Direction générale
  - Risk Manager
  - RSSI

Identifier les périmètres de gestion des risques

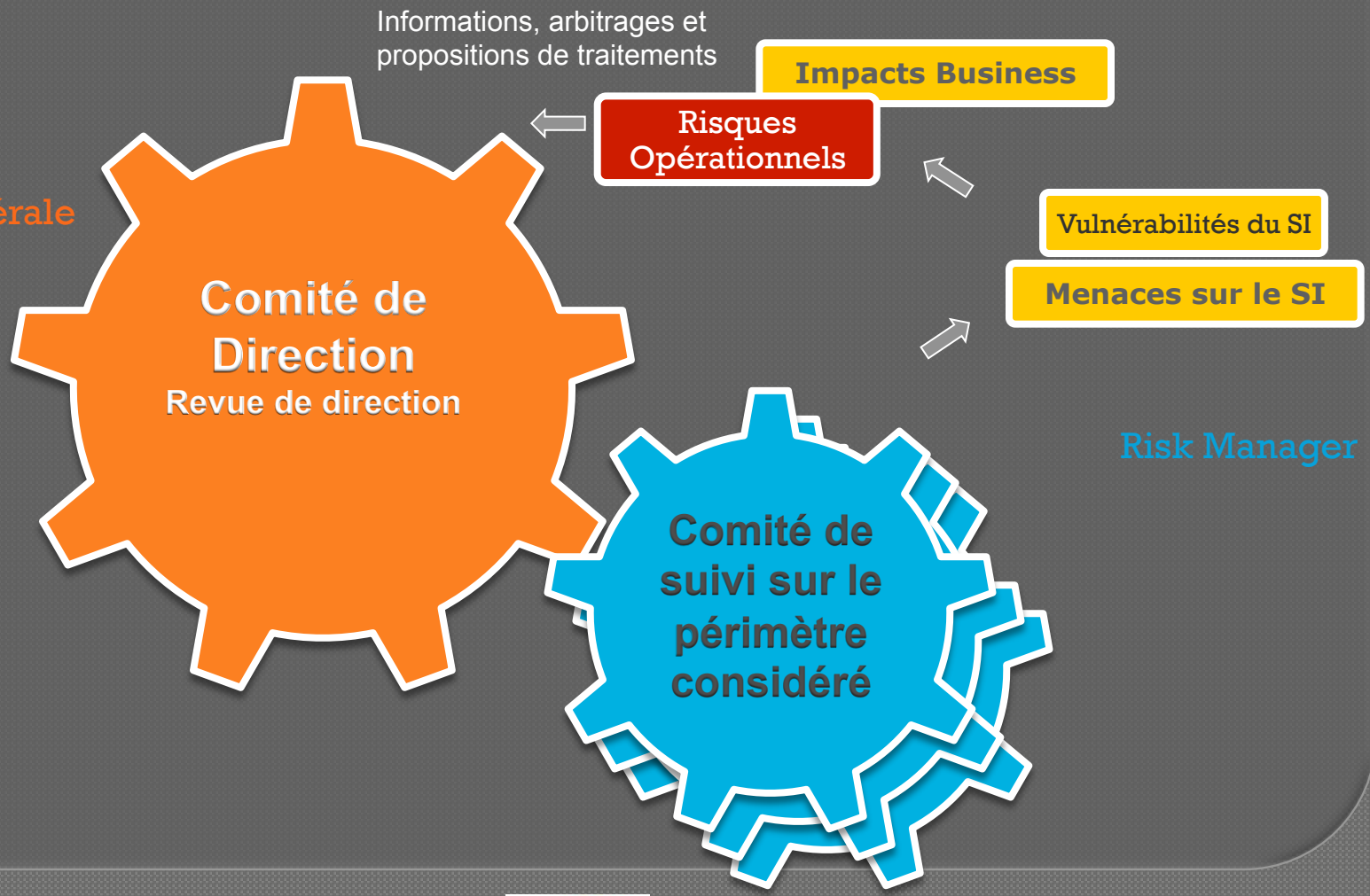
- Périmètre global
- Par filiale
- Par zone géographique
- Par processus métier
- Par Service / Département

- Il faut alors décliner l'organisation au niveau du découpage considéré

Organisation

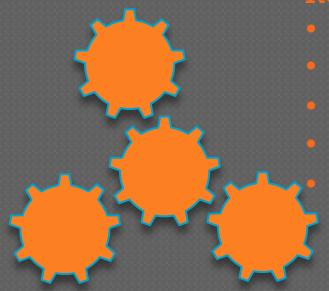


Organisation (Approche par périmètre)



Socle d'appréciation

- Méthode et calculs
  - Choix de la méthode
  - Stabilisation des métriques et méthodes de calcul
    - Impacts / vraisemblance / DICP / matrice d'aversion / …
  - Seuil d'acceptabilité
- Mise à disposition des Référentiels
  - Simples d'utilisation
  - Portables
  - Adaptables
  - Améliorables (bijectivité)

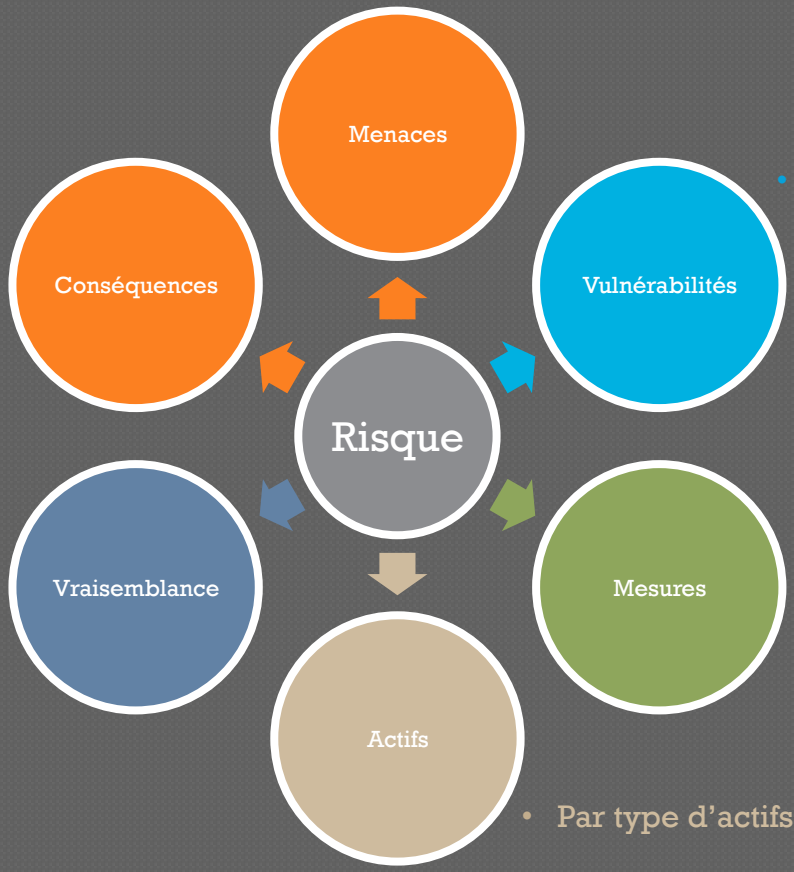


Référentiels :
- Menaces
- Vulnérabilité
- Mesures
- Actifs
- …

Référentiels

- Par type de menaces

- Métriques :
  - Type d'impact
  - DICP



- Par type d'actifs en support

- Métriques

- PSSI
- Par Services
- Par type d'actif

- Par type d'actifs

Communication et Formation

- Communication du socle
  - Partage de la méthode d'analyse et des référentiels
    - Bijectivité des référentiels
      - Gage d'amélioration
  - Organisation
    - Qui fait quoi et comment
- Formation
  - Certification Risk Manager ISO27005
  - Formation EBIOS / MEHARI / méthode interne
  - Formation à l'utilisation de l'Outillage

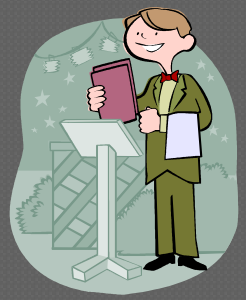
Plugger sur les processus internes

- Approche par périmètre
- Gestion des incidents
- Continuité d'activité
- Sécurité dans les projets
- Politique de sécurité

Industrialiser (approche globale)

Plan

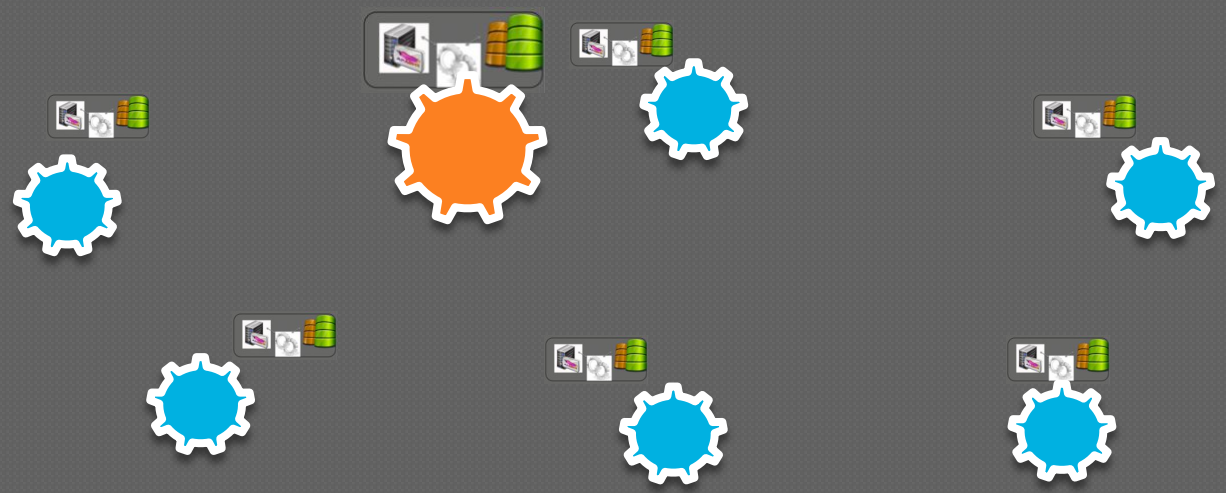
- Introduction
- Réglementation
- Norme ISO27005
- Constats et approches observées
- Industrialisation du Risk Management
- Retour d'expérience
- Conclusion



Retour d'expérience

- Industrialisation du processus de gestion des risques
  - Reprise de l'existant (méthodologique / organisation)
  - Mise en place d'un outillage
    - Déployer l'usage de l'analyse de risque (outil informatique)
    - Faciliter l'appréciation des risques (référentiels)
    - Faciliter et améliorer les arbitrages (indicateurs)
    - Gérer dans le temps (itérations)
    - Permettre l'amélioration (améliorer les ref.)
    - Disposer de résultats reproductibles (ISO27001)
      - À grande échelle

Retour d'expérience



- Référentiels transverses

Retour d'expérience

- Mise à disposition des instances logicielles
  - Cloud privé (in house)
- Définition et Gestion du socle d'appréciation
  - Méthode
  - Métriques
  - Référentiels
- Gestion des formations
  - Logiciel / méthodes internes

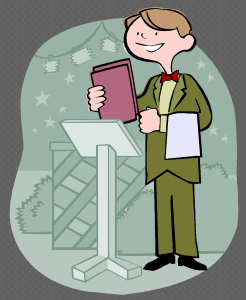
Retour d'expérience

- Responsable fonctionnel de l'instance
  - RSSI local ou Risk Manager local
  - Gestion des référentiels locaux
    - Imports / Export des référentiels transverses
    - Personnalisation des référentiels locaux
      - Langue par exemple
  - Gestion des utilisateurs locaux
    - Risk Manager pour chaque étude
    - Visiteurs pour chaque étude
  - Vision consolidée des analyses locales

Retour d'expérience

Plan

- Introduction
- Réglementation
- Norme ISO27005
- Constats et approches observées
- Industrialisation du Risk Management
- Retour d'expérience
- Conclusion



Conclusion

- Pression légale et règlementaire
  - Sectorielle et européenne
- Manager par le risque
  - Volonté des décideurs
  - Système maîtrisé par les Décideurs
    - Rôdés à la présentation et à l'exercice
    - Terrain familier
- Facteurs de succès
  - Indicateurs actualisés et actualisables
  - Analyses et méthodes encadrées
  - Partage et amélioration continue

Conclusion

- Industrialisation (inévitable)
  - Outillage (nécessité)
    - Décision
    - Accompagnement
- Chemin à parcourir
  - Dépend de la maturité de l'organisme
- Accompagnement au changement / aide au déploiement
  - Mode manuel ou excelisé
  - Mode outillé

Questions

Jean Larroumets

+33 (6) 87 40 51 30

jean.larroumets@fidens.fr