AFAI®

Pour des systèmes d'information
de confiance et créateurs de valeur

Cartographie des risques informatiques : exemples, méthodes et outils

8 avril 2010

Gina Gullà-Ménez,
Directeur de l'Audit des Processus et des Projets SI,
Sanofi-Aventis

Vincent Manière
Consultant

Construction d'une cartographie des risques : quel modèle proposer ?

Agenda

- Introduction - Présentation du groupe de travail
- Eléments génériques sur les risques
- Retours d'expérience
- Enseignements
- Conclusions

Introduction

- Dans le cadre des activités de l'AFAI :
  - Publier les bonnes pratiques professionnelles
    - **catalogue d'une douzaine d'ouvrages, issus du partage d'expérience au sein de groupes de travail constitués de professionnels expérimentés**
  - Faciliter l'échange et l'élaboration collective
    - **des échanges professionnels approfondis**
    - **des groupes de travail constitués à l'initiative des membres**
      - ***Définir un objectif (un livrable sous 18 mois maximum) : ouvrage, article, enquête…***
      - ***Obtenir l'accord du CA***
      - ***… et engager les travaux***

OBJECTIFS DU GROUPE DE TRAVAIL « Cartographie des risques informatiques »

- Etudier les avantages à élaborer une cartographie des risques informatiques.
- Mettre en évidence les différentes approches pratiques, en fonction des objectifs poursuivis et du point de vue de l'utilisateur de la cartographie (Management, Audit interne, Direction de projet, …)

ORGANISATION/PARTICIPANTS

- Le groupe de travail était composé de membres permanents issus des grandes entreprises, des cabinets d'audits, de consultants, exerçant des métiers différents :
  - Responsable d'audit
  - Risk manager
  - Responsable sécurité informatique
  - Responsable méthode
  - …

- Il a bénéficié de la présence d'invités, qui ont apporté un angle de vue particulier ou un témoignage de leur expérience.

DÉROULÉ/MODE DE FONCTIONNEMENT

- Témoignages anonymes ayant pour objectif
  - Restituer de façon standardisée les présentations-témoignages pour faciliter la perception par le lecteur ;
  - Fournir un cadre structuré pour les participants appelés à témoigner.
- Structure de la fiche Témoignage:
  - **Objectif de la cartographie**
  - **Résultats obtenus**
  - **Acteurs**
  - **Démarche**
  - **Avantages**
  - **Inconvénients et difficultés**
- Faire ressortir des enseignements et des facteurs clés de succès pour réussir une démarche cartographie.

Construction d'une cartographie des risques : Quel modèle proposer ?

Agenda

- Introduction - Présentation du groupe de travail
- Eléments génériques sur les risques
- Retours d'expérience
- Enseignements
- Conclusions

Des définitions multiples

- De nombreuses définitions existent qui combinent :
  - Probabilité
  - Impact
  - Vulnérabilité
  - Menace

Origine Bernoulli

- "Le risque est l'espérance mathématique d'une fonction de probabilité d'événements". En termes plus simples, il s'agit de la valeur moyenne des conséquences d'événements affectés de leur probabilité d'occurrence. Ainsi, un événement e1 a une probabilité d'occurrence p1 avec une conséquence probable C1 ; de même un événement en aura une probabilité pn et une conséquence Cn, alors le risque vaudra R = p1.C1 + p2.C2 + ... + pn.Cn. Un produit pi.Ci est appelé valeur de l'aléa i.

Origine IFACI

- Risque **:** possibilité que se produise un événement qui aura un impact sur la réalisation des objectifs. Le risque se mesure en termes de conséquences et de probabilité.

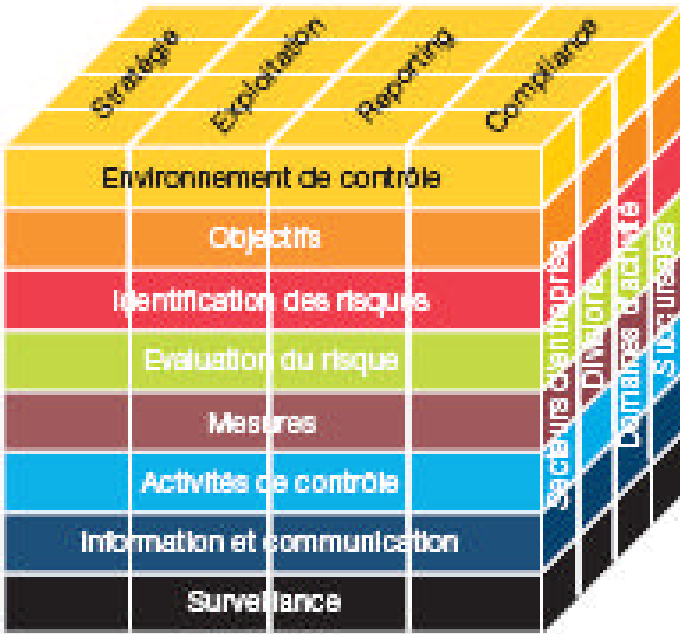
- Cartographie des risques : positionnement des risques majeurs selon différents axes tels que l'impact potentiel, la probabilité de survenance ou le niveau actuel de maîtrise des risques. Son objectif est de permettre d'orienter le plan d'audit interne et d'aider le management à prendre en compte la dimension risque dans son pilotage interne.

Eléments génériques sur les risques

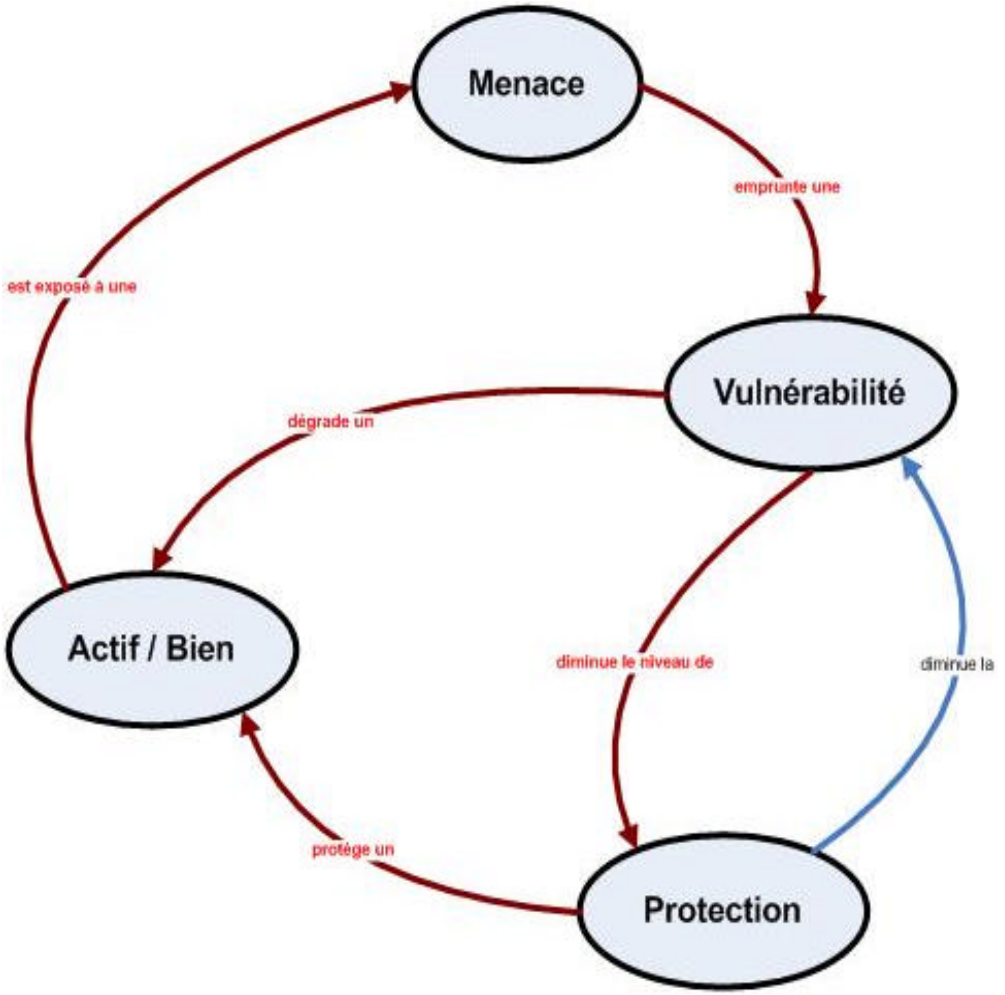
- Deux tendances principales se dégagent de « l'histoire du risque » :
  - Approche mathématique
    - **Blaise Pascal et Pierre de Fermat en 1654**
    - **Loi des grands nombres**
    - **Bernoulli en 1738**
    - **Théorie des Jeux en 1944**
  - Approche « management par les risques »
    - **Apparue en fin des années 1950 aux Etats-Unis**
    - **Gouvernement d'entreprise et obligation de contrôle des risques**
    - **COSO II**

Eléments génériques sur les risques
Tendance COSO II

- Le «cube COSO» visualise la gestion du risque en trois dimensions : du point de vue des objectifs de l'entreprise tel le contrôle interne, les composantes de la gestion du risque à l'échelle de l'entreprise et l'organisation de l'entreprise.



Tendance ISO 2700x



Le risque informatique est-il spécifique ?

- Dans Risk IT (ISACA) :
  - Le risque informatique peut être désigné comme le risque « métier » associé à l'utilisation, la possession, l'exploitation, l'implication, l'influence et l'adoption de l'informatique dans une organisation.
- Exemples et Lien risques métiers
  - Interruption des activités d'une entreprise en raison d'une indisponibilité du SI :
    - **panne d'un composant du réseau (par exemple un routeur)**
    - **incendie de la salle machine**
    - **intrusion d'un pirate et destruction des bases de données**
    - **plan de secours n'ayant pas suivi les évolutions récentes des systèmes**

Le risque informatique est-il spécifique ?

- Exemples et Lien risques métiers
  - Fraude sur les systèmes de paiement :
    - **accès inapproprié aux données : possibilité d'intervention directe sur les fichiers d'interface, sans supervision**
    - **absence de contrôles au sein des processus achats : « 3-way match principle »**
    - **anomalies de séparation des tâches au sein de la communauté d'utilisateurs : le demandeur n'est pas l'acheteur**
    - **pas d'outil de détection d'anomalies en place sur les données : modification des données fournisseurs**
    - **capacité des équipes informatiques à intervenir sur le code source des applications et à mettre en production sans point de contrôle**

Construction d'une cartographie des risques : quel modèle proposer ?

Agenda

- Introduction - Présentation du groupe de travail
- Eléments génériques sur les risques
- Retours d'expérience
- Enseignements
- Conclusions

Retours d'expérience

- Structure des retours d'expérience selon la fiche témoignage :
  - Contexte de la cartographie
  - Objectif de la cartographie
  - Acteurs concernés
  - Démarches
  - Représentations

Retours d'expérience
- Contexte de la cartographie

- Une réponse à la montée des exigences règlementaires concernant les risques
- Démarche de sécurisation des actifs SI
- Volonté de la Direction Générale
- Structuration des démarches de gestion des risques et de contrôle interne
- Management opérationnel par les risques

Cartographie des risques – Etat de l'art

4 types de cartographies identifiés

- cartographie des risques Groupe
  - pour décision et action de gestion du responsable du risque
  - pour suivre la maîtrise des principaux risques de l'entreprise
- cartographie des risques pour construction du plan d'audit
  - pour identifier l'exposition au risque et définir le plan d'audit
- cartographie des risques Sécurité de l'information
  - pour protéger au plus efficient les actifs du SI au regard des menaces qu'ils encourent
- cartographie des risques propres à la Fonction SI
  - pour piloter les processus, la fonction SI, et la réussite des projets

Retours d'expérience - Acteurs concernés

Ce sont toujours les mêmes, mais plus ou moins impliqués selon les contextes :

- La fonction SI
- La filière Sécurité
- L'Audit Interne
- Les Métiers
- La Gestion des Risques
- Le Contrôle interne
- La Direction Générale

Retours d'expérience - Démarche (1/3)

- Les démarches sont souvent structurées et formalisées,
- Plusieurs démarches peuvent co-exister au sein d'une organisation, mais elles restent généralement indépendantes,
- Différents impacts liés aux risques SI sont traités : opérationnels, financiers, réglementaires,
- Des approches Top-Down (pour la DG, pour le réglementaire) ou Bottom-Up (pour la sécurité, le pilotage SI),

Retours d'expérience - Démarche (2/3)

- Des « inputs » de plus en plus nombreux
  - Menaces, incidents, résultats d'audits internes et externes, dires d'experts, statistiques
- L'évaluation de l'impact financier est rare,
- Les risques bruts (ou inhérents) et les risques nets (ou résiduels) sont généralement pris en compte,
- Méthodes et référentiels : on retrouve les standards du contrôle interne SI et de la sécurité
  - Cobit, COSO, ISO 27xxx, …
- Mais également des méthodes internes,

Retours d'expérience - Démarche (3/3)

- Un outillage divers, plus ou moins sophistiqué
  - Questionnaires, tableurs, listes de risques, progiciel de gestion des risques
- La charge de travail initiale dépend du périmètre de l'analyse, mais elle est généralement conséquente
  - par exemple, 20-25 jours par branche pour une cartographie Direction Générale
- La fréquence de mise à jour est souvent annuelle pour les cartographies Groupe et Audit interne et peut-être trimestrielle pour les cartographies opérationnelles

Retours d'expérience - différentes représentations (1/4)

- Par exemple :

  Schéma générique

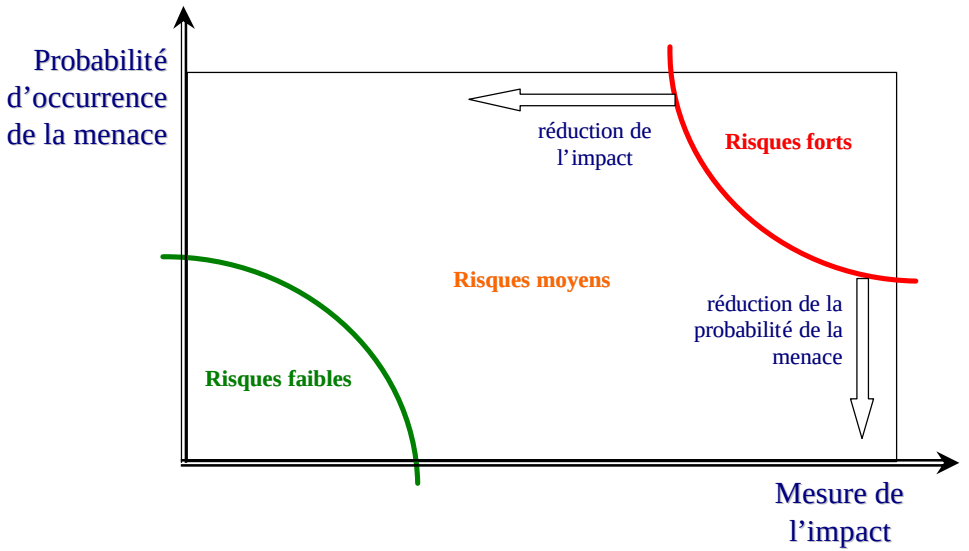
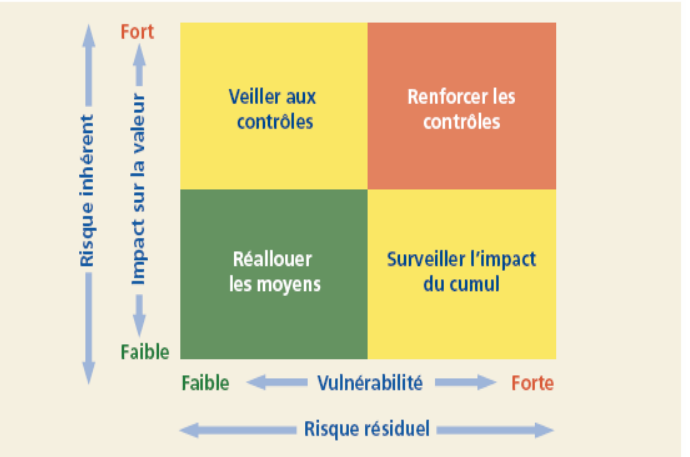
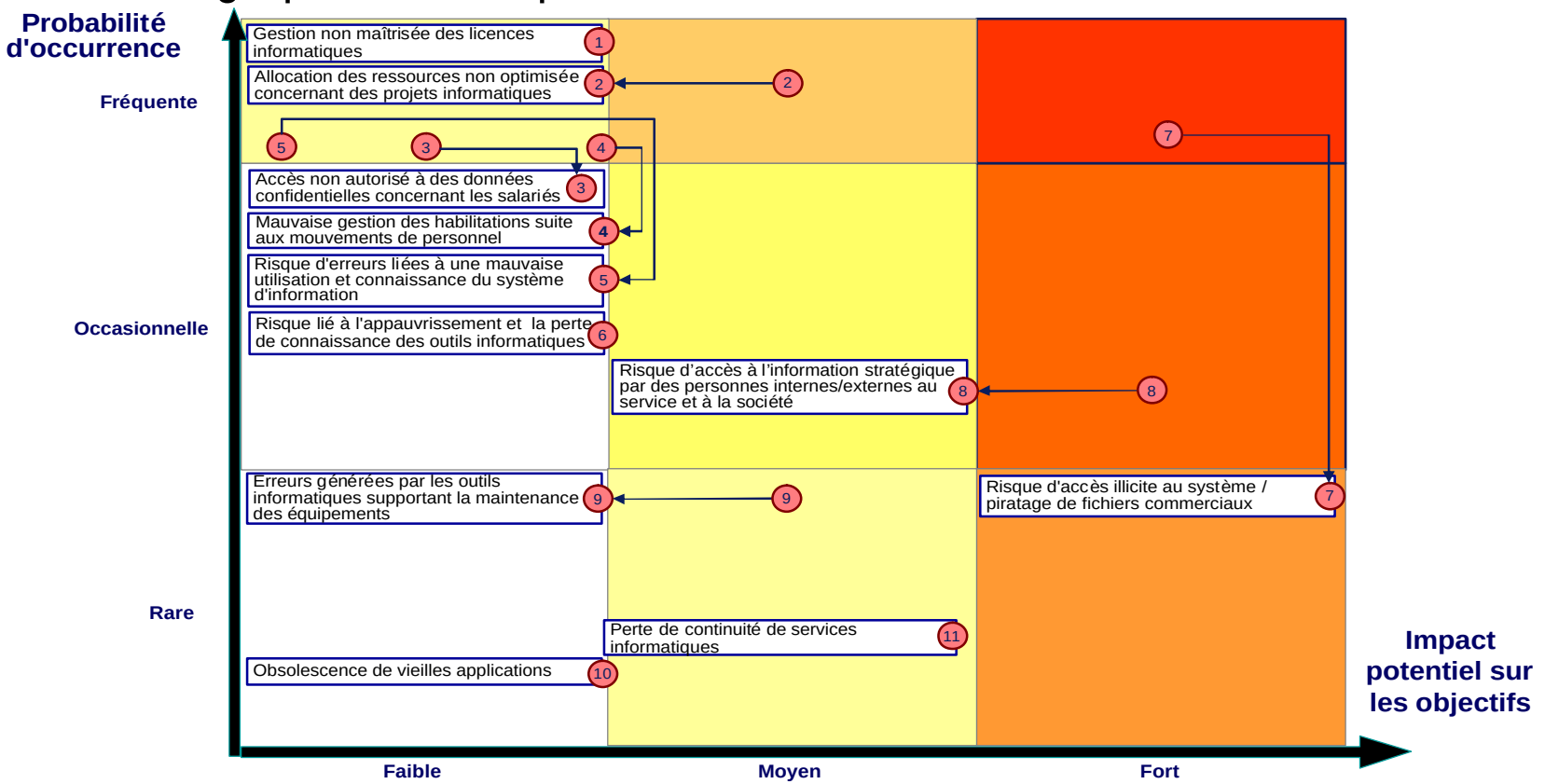


  Schéma Contrôle Interne



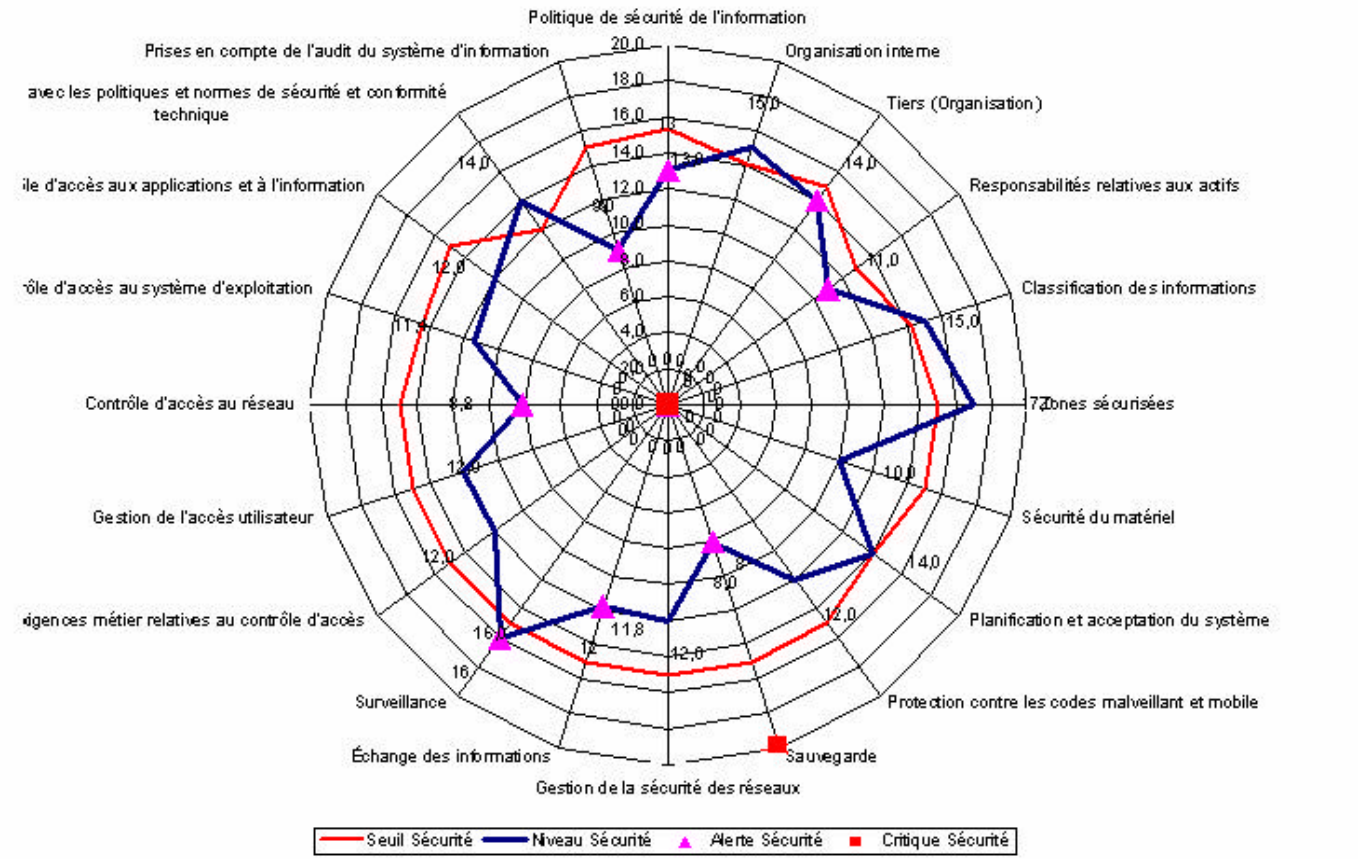
Retours d'expérience - différentes représentations (2/4)

- Cartographie des risques SI



Retours d'expérience
- Différentes représentations (3/4)

- Représentation en rosace



Retours d'expérience
- Différentes représenta

- Quantification

Menaces		Actifs: Matériel transportable	Matériel fixe	Support de stockage dynamique	Supports de stockage statique	Logiciel de service, de maintenance, d'administration ou système d'exploitation	Application métier	Architectures et applications réseaux	L'organisme SI	Activités métiers	Sous-traitant/Fournisseurs/Industriels	Personnes	Certification, Image de marque de la Dsi	Périmètre physique	Service et moyens en énergie et utilitaires	Données / Informations
		31	6	16	20	29	41	44	16	30	1	30	31	37	0	151
Perte ou altération des preuves empêchant toute investigation	6			1		1							3			1
Désaccord, sanction des autorités de tutelle ou sanction pénale	25							1	4	1	1	5	6			7
Perte de certification	16						1		4	4			6			1
Intrusion de personne	16	1			1							2		10		2
Menaces physiques (Incendies, inondations, tremblements de terre…)	13	1	1		1							1		8		1
Défaillance des prestations de tiers	18		1	1			4	1	3	4			1			3
Interruption des activités métiers	11						3			6						2
Accès non autorisé	72	3	1	2	2	6	12	6		7		3	1	11		18
Abus de droits	15					1	3		2	2		1	2			4
Reniement d'actions	12			1		2	2					2	2			3

Construction d'une cartographie des risques : Quel modèle proposer ?

Agenda

- Introduction - Présentation du groupe de travail
- Eléments génériques sur les risques
- Retours d'expérience
- Enseignements
- Conclusions

ENSEIGNEMENTS (1/2)

- Difficulté de compréhension par les métiers de certains critères de l'information, notamment Efficacité et Fiabilité
- Pas d'évaluation scientifique
- Subjectivité dans l'identification et l'évaluation des risques
- Hétérogénéité et granularité des risques

ENSEIGNEMENTS (2/2)

- Consolidation difficile
- Niveaux de maturité ou de sensibilité différents
- Périmètre de la démarche
- Mobilisation des ressources
- Vocabulaire : pas de définition unique d'une entreprise à une autre et au sein d'une même entreprise : Menace, risque de sécurité, risque métier, risque opérationnel …

- Constat général :

  Il n'y a pas de cartographie unique et il apparaît que cela n'aurait pas forcément de sens.

Construction d'une cartographie des risques : Quel modèle proposer ?

Agenda

- Introduction - Présentation du groupe de travail
- Eléments génériques sur les risques
- Retours d'expérience
- Enseignements
- Conclusions

Conclusions (1/2)

« Concilier diversité et cohérence d'ensemble »

- **Effectuer un travail amont de clarification du vocabulaire et des notions retenus**
- **Conserver les initiatives locales répondant à des besoins spécifiques de management opérationnel : sécurité, audit interne, contrôle interne, DSI, Métiers**
- **Mais, mettre en place un pilotage global de la gestion des risques informatiques**
  - **vision globale des initiatives, maintien de la cohérence et pertinence, optimisation des moyens, maîtrise de la communication et du reporting en matière de risque**

Conclusions (2/2)

« Concilier diversité et cohérence d'ensemble »

- **Etablir un référentiel des risques informatiques**
- **Choisir un outil afin de faciliter le partage et la consolidation des risques**
- **Avoir une vision intégrée des démarches connexes propres à l'informatique : Qualité, ITIL, Gouvernance, Sécurité, …**
- **Etablir la contribution de la gestion des risques informatiques à la gestion globale des risques de l'entreprise**

Annexe. Actualité des associations professionnelles

- AMRAE : Association pour le management des risques et des assurances de l'entreprise
  - Groupe de travail « Cartographie des risques » - ouvrage publié en 2007

- AFAI : Association Française de l'Audit Informatique
  - « Baromètre » - enquête qui établit un état des lieux de la gestion des risques informatiques dans les entreprises, leurs perceptions et les actions entreprises pour les maitriser
  - Groupe de travail « Cartographie des risques »
    - **Témoignages et publication d'un ouvrage méthodologique courant 2008**
- IFACI
  - Enquête
  - Cahier de recherche « Cartographie des risques » publié en 2003

Backup

DÉROULÉ/MODE DE FONCTIONNEMENT

- Guide de constitution de l'ouvrage :
  - Introduction : lancer le sujet et notamment le positionner par rapport à la cartographie globale des risques d'une organisation
  - Pourquoi la cartographie
  - Justification
  - Définition
  - Méthode
  - Quels acteurs ?
  - Comment réaliser la cartographie ?
  - Quelle démarche ?
  - Quels outils mettre en œuvre ?
  - Mise à jour et périodicité
  - Témoignages
  - Fiche selon format ci-après
  - Glossaire
  - Bibliographie

Le risque informatique est-il spécifique ?

- Existe-t-il / Faut-il des catégories de risques informatiques
  - Recours à des catégories facilite le travail sur les risques
    - **guide pour le recensement**
    - **communication sur les risques informatiques dans un cadre partagé**
  - exemple : catégorisation du modèle Risk IT de l'ISACA
    - **les risques portant sur la fourniture du service, liés à la disponibilité et la performance des systèmes au quotidien ;**
    - **les risques portant sur la livraison des nouvelles solutions aux utilisateurs, et notamment les projets ;**
    - **les risques portant sur les opportunités (et notamment les opportunités ratées) de rendre plus efficaces les processus métiers en s'appuyant sur les évolutions de la technologie.**

Conclusion

- Élaborer une cartographie des risques informatiques est possible et les bénéfices sont réels.
- Toutefois, quand des risques ont été exprimés et partagés au sein d'une organisation, on ne peut plus ne rien faire.
- L'enjeu réel porte donc plus sur l'utilisation de la cartographie que sur la cartographie elle-même.
- Les risques sont dynamiques (surtout sur un sujet technologique) et la vision que l'on en a doit l'être aussi.
- C'est donc tout un processus de gestion des risques informatiques qui doit donc être mis en œuvre.