SSTIC06
Les limites de la sécurité

De l'intérêt du « risk management » en SSI

1er Juin 2006

Sylvan Ravinet – chargé de mission

Vazrik Minassian – directeur associé

Adenium SAS

SOMMAIRE

SOMMAIRE

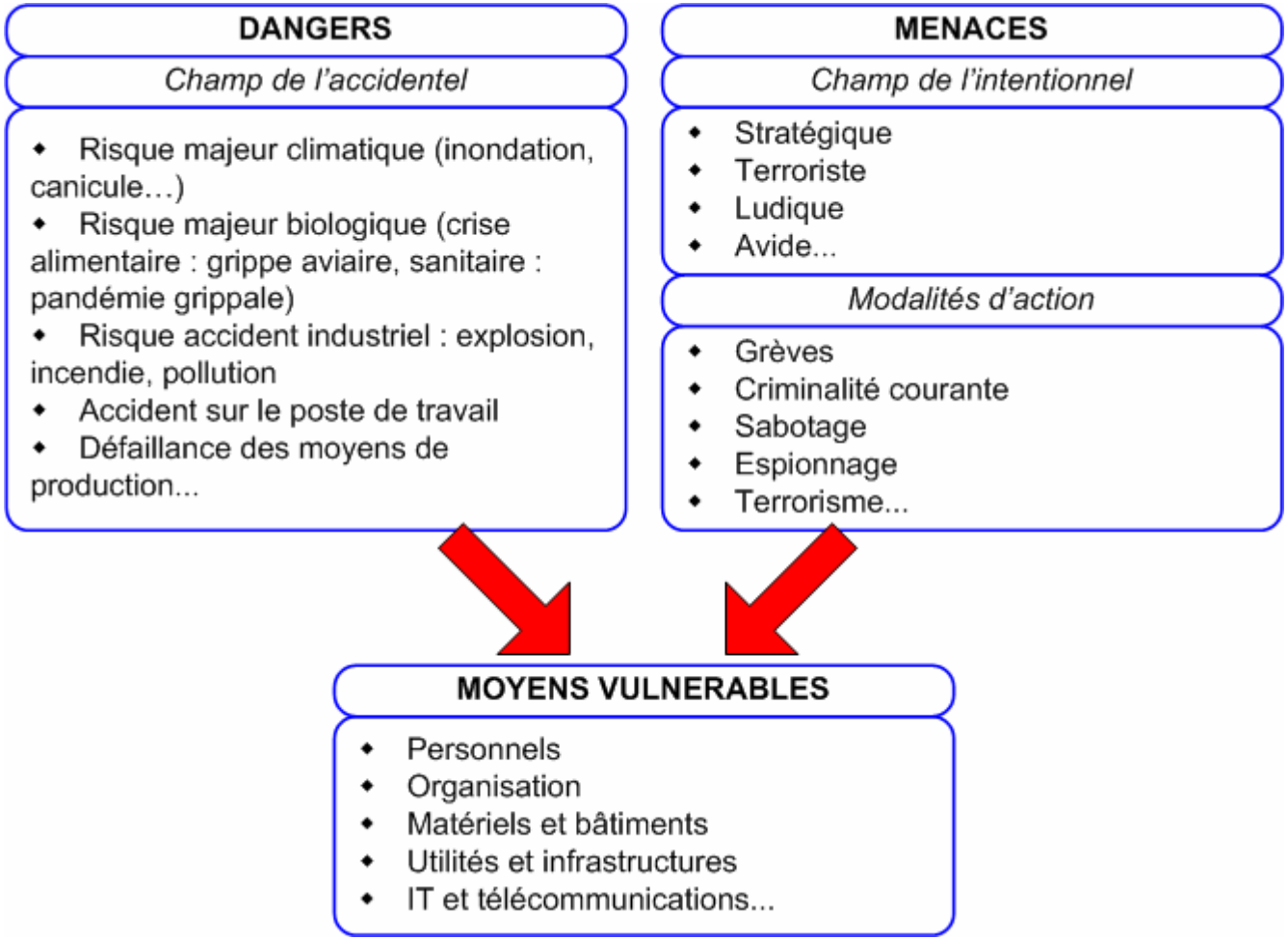
1 > LES DEFIS DU MANAGEMENT DE LA SSI

-Les risques sont très divers

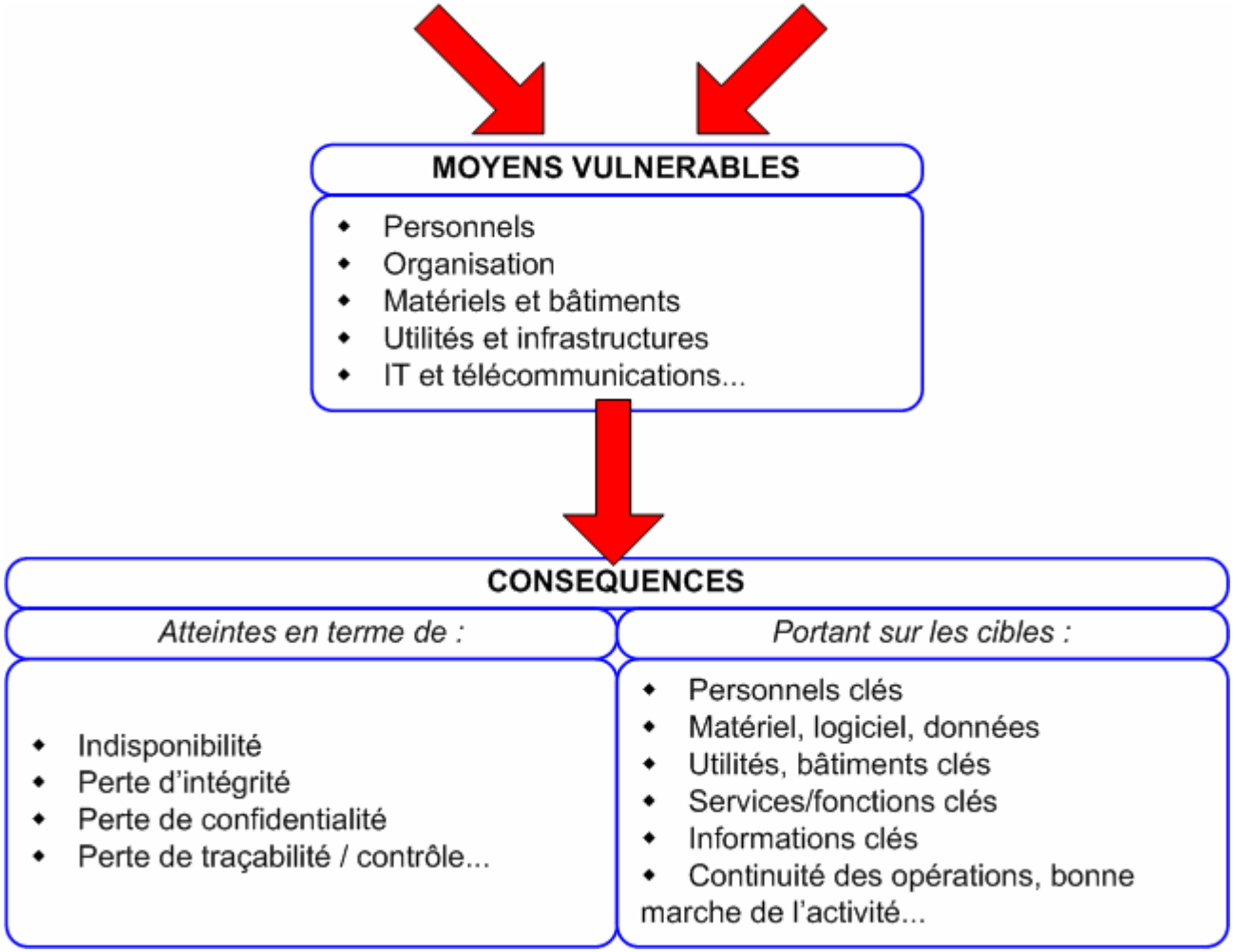
-Une grande variété d'acteurs

-Les outils du management sur étagère…

LES RISQUES A TRAITER SONT DE NATURES TRES DIVERSES (1/2)

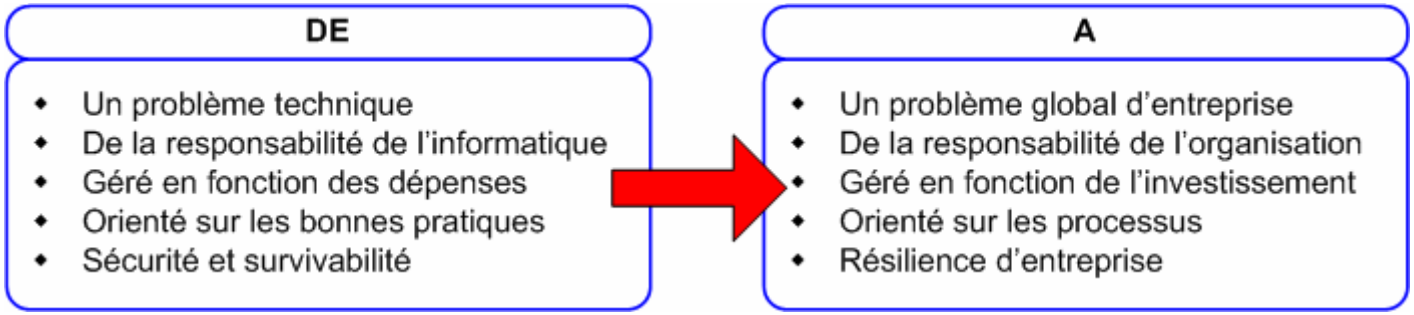


LES RISQUES A TRAITER SONT DE NATURES TRES DIVERSES (2/2)



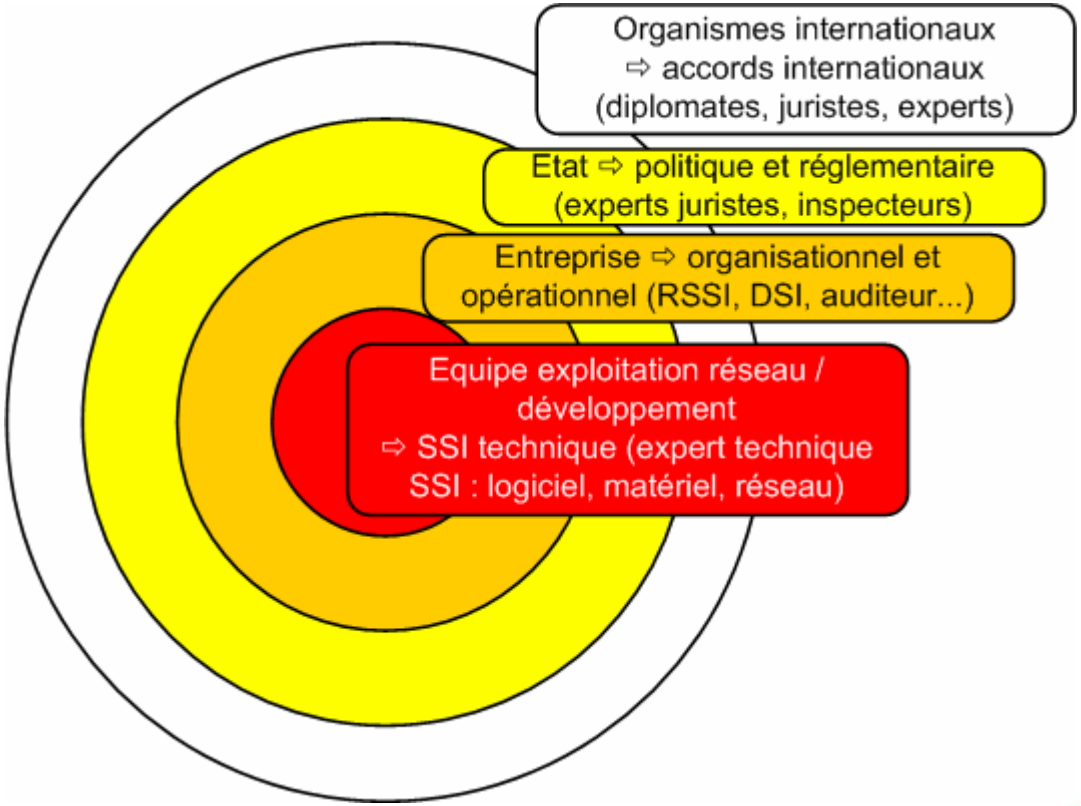
LA SSI NE SE LIMITE PAS A LA TECHNOLOGIE (1/2)

✓**Le CERT, institution technique de référence, a redéfinit sa notion de la sécurité (2005).**



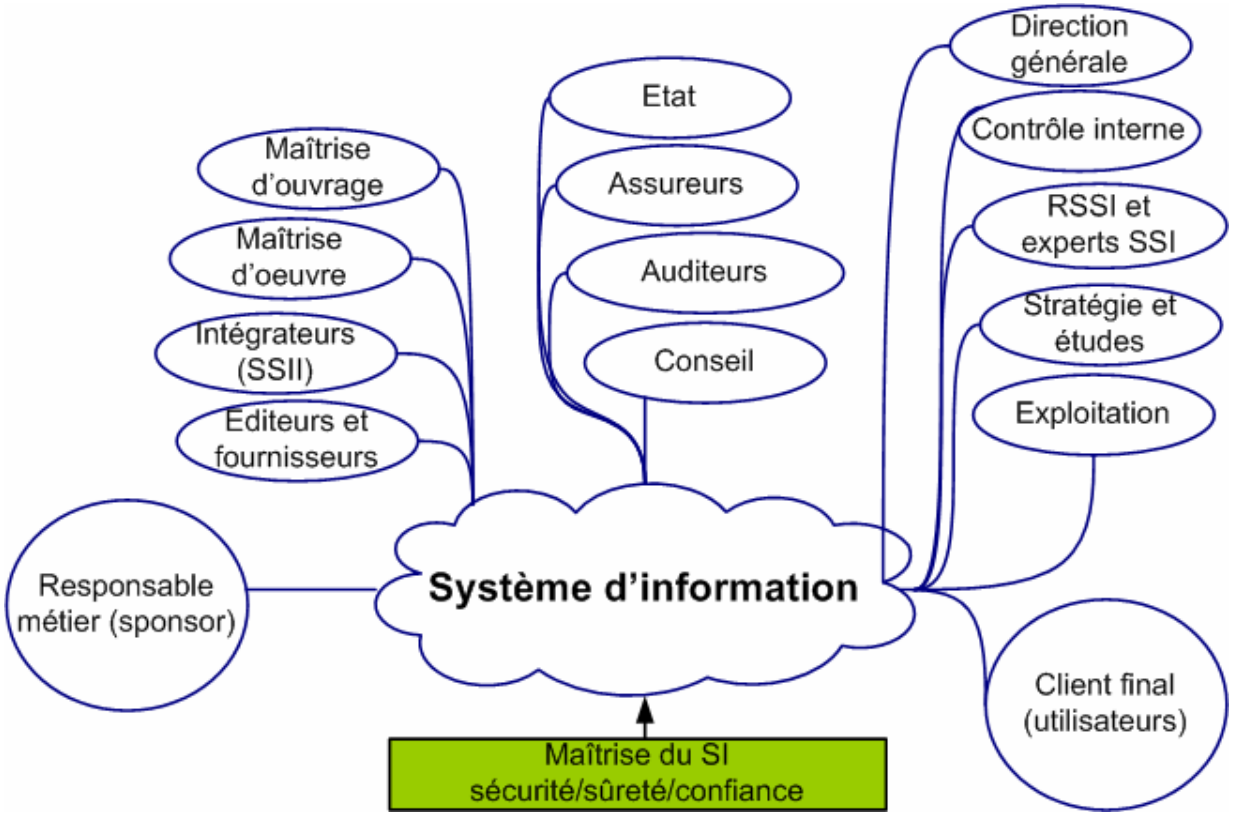
LA SSI NE SE LIMITE PAS A LA TECHNOLOGIE (2/2)

✓ **Les entités concernées par la SSI sont d'origine et de culture très diverses :**



AUTOUR DES SYSTEMES, LES ACTEURS EN SSI SONT MULTIPLES

✓ **Une grande diversité d'acteurs interviennent au chevet des SI :**



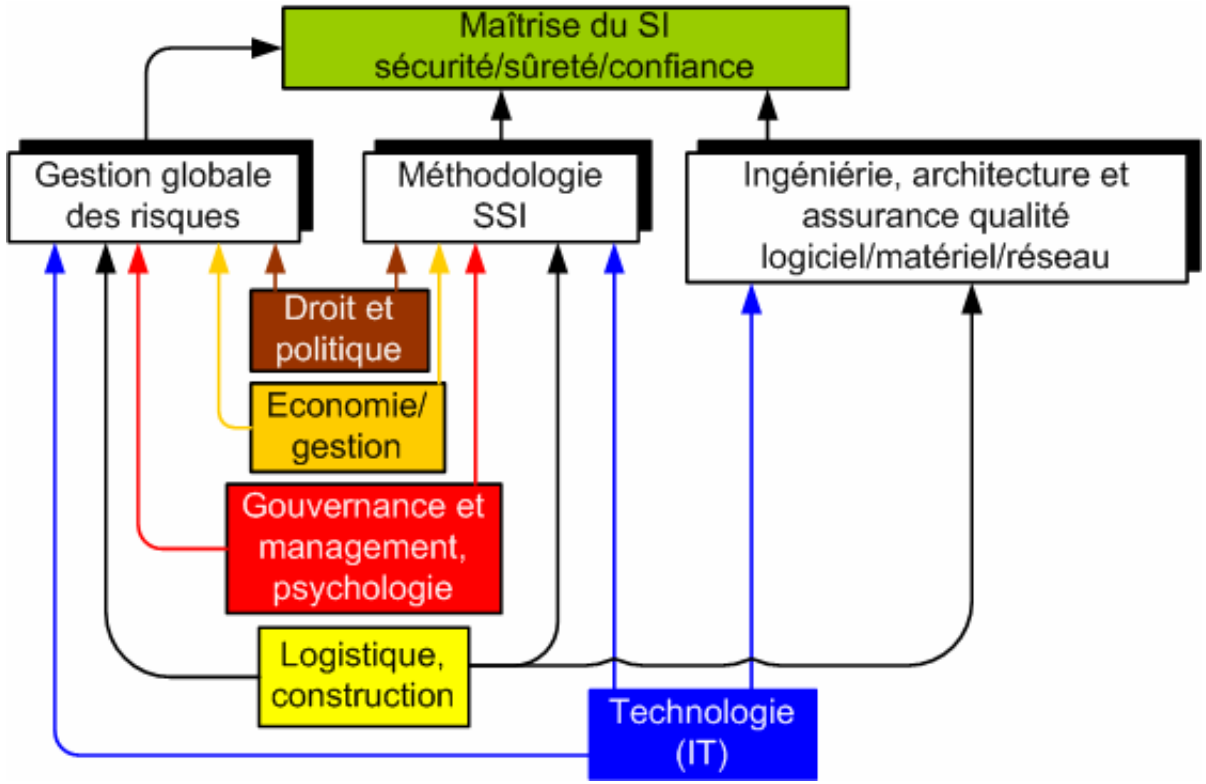
LES OUTILS STANDARDS SONT UTILES… MAIS INSUFFISANTS

✓ **Les outils du management « sur étagère » sont des normes :**

Sujet	*Objectifs*	*Sources et références*	*Standard ISO/IEC*
Evaluation de systèmes de sécurité	Critères d'évaluation de la sécurité des produits	Critères communs	ISO/IEC 15408
Référentiel de bonnes pratiques SSI	Guide de mise en place de contre-mesures ; Evaluation de la performance SSI	BS7799-1 CobiT (sections) ITIL (sections)	ISO/IEC 17799:2005 (ISO/IEC 27002:2007)
Analyse et réduction des risques SSI	Prioriser les risques à traiter	BS7799-3 Octave (CMU), EBIOS (DCSSI), Mehari (Clusif)	ISO/IEC 27005:?
Maturité de la SSI	Evaluer le niveau de maturité SSI d'une organisation	CMMI SCAMPI (CMU)	ISO/IEC 21827 (SSE-CMM)
Système de management de la SSI	Coordonner les actions SSI	BS7799-2 ISO19011, ISO 9001 ISO14001	ISO/IEC 27001:2005

LES OUTILS STANDARDS SONT UTILES… MAIS INSUFFISANTS

✓ **Les domaines de pratique et les méthodes sources de la SSI sont plus larges :**



2 > L'ANALYSE DES RISQUES, LANGAGE COMMUN AUX ACTEURS EN SSI

-La démarche de réduction des risques

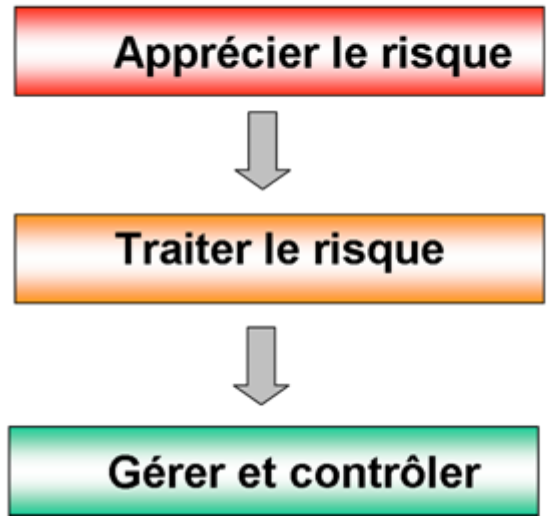
-Analyser les risques pour identifier les priorités

-S'organiser pour gérer la crise SSI

UNE DEMARCHE DE REDUCTION DES RISQUES EST INDISPENSABLE

✓ **La démarche de réduction des risques :**

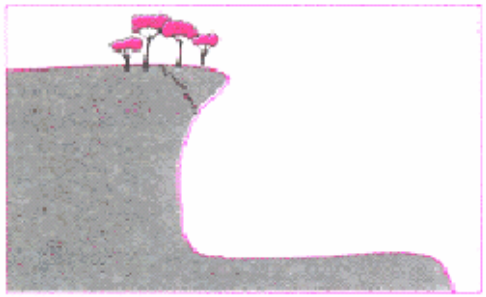
DEMARCHE GENERALE DE REDUCTION DES RISQUES



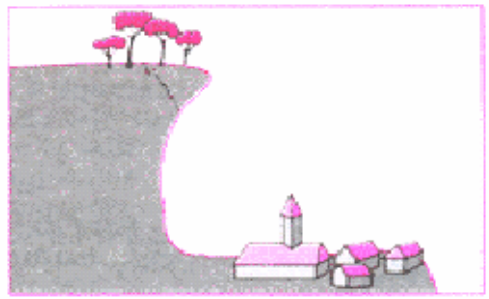
2 – L'ANALYSE DES RISQUES, LANGAGE COMMUN

UNE DEMARCHE DE REDUCTION DES RISQUES EST INDISPENSABLE

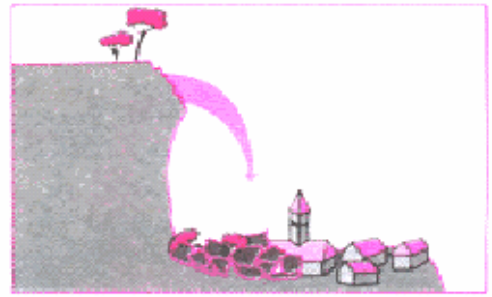
" Un risque se définit comme tout événement, action ou inaction de nature à empêcher une organisation d'atteindre ses objectifs "



L'aléa
"Le danger"



Les enjeux
"L'organisation"



L'événement redouté
"Le risque majeur"

<u>Signal faible</u> :
Évènement perçu ou non
Intégré ou non intégré dans le cadre de la prévention des risques

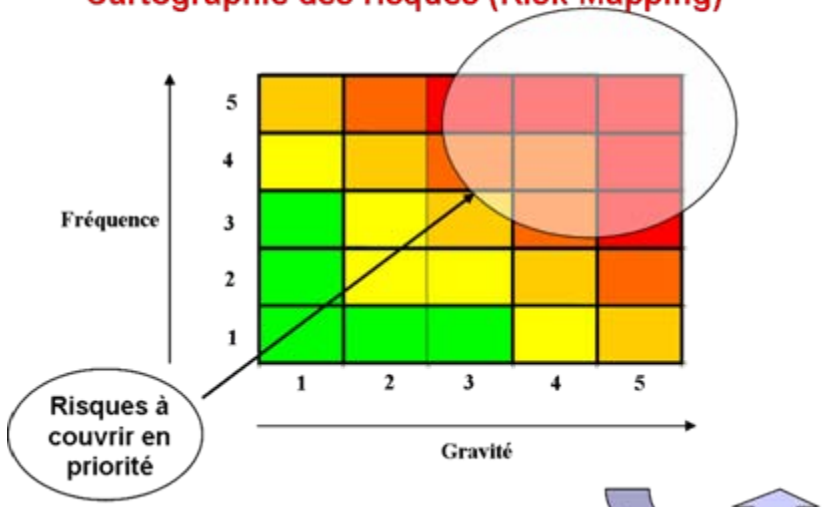
2 – L'ANALYSE DES RISQUES, LANGAGE COMMUN

UNE DEMARCHE DE REDUCTION DES RISQUES EST INDISPENSABLE

✓ **La méthode d'évaluation des risques (risk mapping) :**

La Méthode d'évaluation

Cartographie des risques (Risk Mapping)



FRÉQUENCE DE SURVENANCE DU RISQUE
1: Improbable - 1 x / 100 ans
2: Rare - 1 x / 10 ans
3: Occasionnel - 1 x / 3 ans
4: Probable - 1 x / an
5: Fréquent - 1 x / semaine

GRAVITÉ DE L'IMPACT DU RISQUE
1: Négligeable
2: Mineur
3: Majeur
4: Critique
5: Catastrophique

2 – L'ANALYSE DES RISQUES, LANGAGE COMMUN

UNE DEMARCHE DE REDUCTION DES RISQUES EST INDISPENSABLE

- ✓ La méthode d'évaluation des risques (risk mapping) :

2 – L'ANALYSE DES RISQUES, LANGAGE COMMUN

FACE AUX NOUVELLES MENACES, IMPREVISIBLES, S'ORGANISER ET GERER LA CRISE

✓ **La SSI est alors une modalité de gestion de crise, autour de 3 étapes, le management étant utile à chacune :**

Prévention	◆ Préparation : plans et tests, formation ◆ Prévention : signaux faibles, sensibilisation ◆ Dissuasion : information, communication ◆ Entrave : dispositifs, contrôle d'accès
Gestion de l'urgence	◆ Détection : moyens ◆ Alerte : chaîne d'alerte, moyens ◆ Réaction : intervention et secours
Gestion de crise	◆ Dévolution : organisation de crise ◆ Continuité : mode dégradé ◆ Restitution : mode nominal
Management	◆ Vision stratégique et tactique ◆ Architecture : compartimentation, homogénéité ◆ Leadership, coordination, autonomie ◆ Contrôle, retour d'expérience, gestion compétences

3 > QUESTIONS / REPONSES

MERCI POUR VOTRE ATTENTION