# FORMULATING INFORMATION SYSTEMS RISK MANAGEMENT STRATEGIES THROUGH CULTURAL THEORY

## I- Le processus de risk management selon ISO 27001(2005), NSIT : 8000 (2002) et Frosdick (1997) :

Ce processus inclut 3 étapes : -l'initiation
-l'analyse de risque
-l'atténuation du risque

**1) l'initiation :** son objectif est de :
- définir le contexte du processus de management du risque
-fixer l'étendu de l'analyse
- constituer l'équipe responsable de la gestion du risque
→C'est aussi dans cette étape que la méthodologie de gestion du risque sera fixée

**2) l'analyse du risque :** cette étape inclut 3 sous-processus :
- identification du risque
- estimation du risque
- évaluation du risque

**a) identification du risque :** c'est le processus d'identification des risques constituant des menaces aux actifs qui ont besoin d'être protégés.
Il est donc nécessaire d'identifier les actifs à protéger, leur associer des risques potentiels et identifier leurs vulnérabilités.

**b) l'estimation du risque :** c'est le processus de quantification des risques identifiés. Cela passe, en général, par le calcul de la probabilité d'occurrence (P) et l'estimation de l'impact ou coût (T) → ***risk (R)= P x C***

**c) l'évaluation du risque :** durant se processus on détermine le seuil de tolérance et on identifie les options de traitement du risque [Transfert du risque chez un tiers, acceptation du risque (ne pas le contrôler), prévention du risque (si elle est appliquée, l'actif n'est plus exposé au risque), réduction du risque (sélection des mesures de contrôle appropriées)].

**3) atténuation du risque :** selon l'ISO 27001, ce processus inclut 3 étapes :
-le design
-l'implémentation ; et
-le suivi (monitoring)

**a) le design :** c'est la spécification des objectifs de sécurité, l'élaboration des politiques de sécurité et des processus relevant du contrôle de risques (les contre-mesures et les politiques) avec l'établissement d'un plan temporel pour l'implémentation.
Dans le cas où d'autres risques apparaissent, d'autres mesures de contrôle doivent être spécifiées et conçues accompagnées, bien sûr, du plan temporel d'implémentation.

**b) l'implémentation :** elle implique l'application des mesures et procédures de contrôle choisies, la gestion des ressources nécessaires à l'implémentation (personnel, temps, moyens financiers et opérations). Il faut aussi prévoir, dans cette étape, des programmes de

sensibilisation à la sécurité dans le but de promouvoir une culture appropriée du risque et de la sécurité.

**c) le suivi** : l'objectif de ce processus est de s'assurer de l'efficacité des mesures prises. Il inclut :
- des processus de détection rapide des erreurs et incidents.
- des mécanismes qui vérifient si les procédures documentées sont suivies.
-des révisions visant à évaluer l'efficacité des contrôles implémentés, et
-la réévaluation du niveau de risque résiduel, en tenant compte les changements possibles dans les processus organisationnels ou les objectifs business.

## II- Importance du rôle des perceptions des actionnaires pour le processus de risk management :

En général, utilisateurs finaux de la sécurité de l'information sont inconscients des mesures de sécurité. Pour la majorité d'entre eux, c'est un outil pour accomplir leurs responsabilités de la manière la plus efficace possible, mais la sécurité de l'information est perçue plus comme une entrave qu'une nécessité.
Pour atteindre la conformité des parties prenantes aux mesures de sécurité prises, il est primordial d'introduire des programmes de sensibilisation à la sécurité et de formation des employés. Mais ces deux mesures ne sont pas les seuls facteurs sociaux influant sur la perception des menaces chez les parties prenantes. En effet, différentes personnes (utilisateurs finaux, parties prenantes, etc...) mettent l'accent sur des risques différents. Leurs préoccupations peuvent avoir comme sources leur expérience personnelle, ce qu'ils ont entendu ou vu dans les médias,… plusieurs facteurs peuvent avoir une influence sur la manière de percevoir le risque dont la familiarité avec les sources de danger et l'aptitude à contrôler les situations dangereuses.
Aussi, les individus ont-ils tendance à faire différentes estimations du même risque selon qu'il soit pour eux ou pour des tiers. C'est pour cette raison que la classification des menaces par des tiers peut être différente de celle des professionnels de la sécurité→ d'où son importance.

## III- le modèle théorique de risk management : (la théorie culturelle)

Cette théorie a été proposée par Douglas(1978) et Douglas & Wildavsky (1982).
Son postulat principal est que la manière d'interaction sociale entre les individus empiète sue les systèmes de symboles qu'ils utilisent pour comprendre le monde. Autrement dit, les concepts que les gens utilisent pour comprendre le monde sont reliés contraintes ou structures sociales auxquelles ils sont confrontés (préjugés culturels).

→Cette théorie explique comment et pourquoi les individus formulent leur perceptions de certains concepts tels que le risque ou la menace.
1) les perspectives de la théorie culturelle :
- la stabilité
- la mobilité

**a) la perspective de stabilité :** elle suppose que les individus sont constants dans un préjugé culturel. Ils ont tendance à s'attacher à des structures sociales avec le même type de préjugé culturel, dans tous les domaines de leur vie. Cela implique que ces individus se conforment, toujours, à ce préjugé quelque soit le contexte social→ on pourra donc mesurer le préjugé culturel d'un individu indépendamment du temps et du contexte.

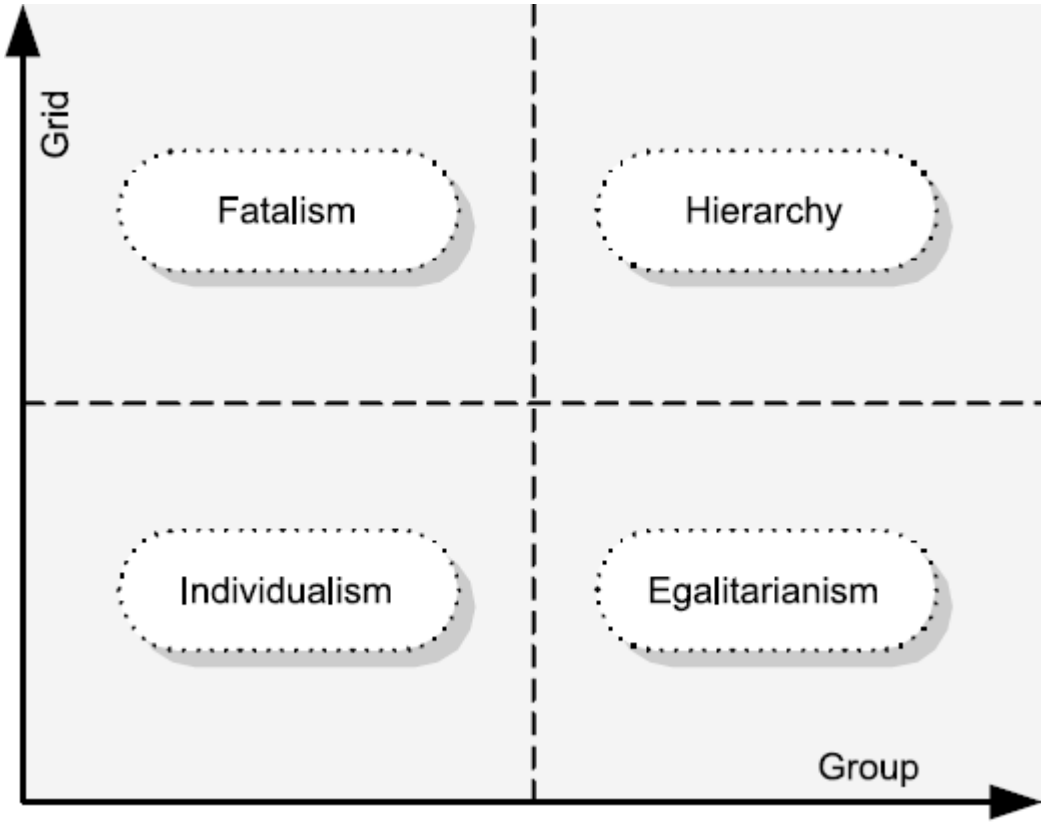
**b) la perspective de mobilité :** cette perspective suppose que les individus peuvent s'attacher à des structures culturelles avec différents types de préjugé culturel dans différents domaines de leur vie. Cela implique que ces individus peuvent se conformer à différents préjugés culturels en fonction du contexte ou adopter différents préjugés culturels au cours du temps.
→ On ne peut, alors, mesurer les préjugés culturels sans faire référence à un contexte et un espace temporel spécifiques. On doit, donc, appliquer des méthodes quantitatives telles que les observations ou les groupes de discussion.

2) **la typologie grille/groupe :** cette typologie fournit un dispositif heuristique permettant l'application de la théorie culturelle et a eu une grande influence dans différents contextes et différents niveau d'agrégation.
Elle se base sur une distinction entre le concept de préjugé culturel et celui de relation sociale. Cette typologie identifie 4 groupes culturels différents ayant des trains de vie différents. Elle comprend 2 dimensions : la grille et le groupe

a) **la dimension « groupe »** : Elle montre si un individu est membre d'une unité sociale fermée, à quel point les activités du groupe ont une influence sur l'individu et à quel point les frontières du groupe constituent une contrainte à la liberté d'agir des individus dans et en dehors du groupe.

b) **La dimension « grille »:** elle montre le degré de régulation et de restriction du contexte social à l'égard des comportements individuels.

Ces deux dimensions fournissent un modèle à 4 « visions du monde » :
-la hiérarchie
-l'égalitarisme
-le fatalisme
-l'individualisme.



Les « hiérarchistes » sont caractérisés par des frontières du groupe très solides et par des prescriptions contraignantes. La position d'un individu dans le monde est définie par une classification établie basée sur des critères tels que l'âge, le sexe ou encore la race
La culture hiérarchique insiste sur l'importance de l'établissement et la préservation de l'ordre naturel de la société→ pour cette raison, les « hiérarchistes » ont peur de tout ce qui peut perturber cet ordre social et accordent une grande confiance aux experts. → ils s'adaptent difficilement au changement et sont dépendant des moyens réguliers de faire les choses.

Les « égalitaires » sont aussi caractérisés par des groupes importants, mais leur vie n'est pas guidée par la différentiation des rôles. Aussi supposent-ils qu'un individu doit négocier sa relation avec les autres de façon que l'autorité d'une personne ne soit par la résultante de sa position → un fort sens de l'égalité d'où leur peur du développement qui peut conduire à une inégalité sociale et une faible confiance accordée aux experts.

Les « individualistes » ne sont tenus ni par l'appartenance à un groupe ni par les rôles prescrits, ils suggèrent que toutes les frontières soient sujettes à la négociation. Ils se sentent responsables envers les autres membres de la société et préconisent une allocation du pouvoir indépendante de la position sociale ou du statut. → Ils n'acceptent pas les règles basées sur le passé et hésitent à accepter les lois et les instructions surtout lorsque ces dernières constituent une barrière à leur autonomie.

Les « fatalistes » croient que leur autonomie est limitée par les distinctions sociales, mais ne se sentent pas membres des institutions qui établissent les règles (ils se sentent toujours comme des outsiders). Aussi ils croient que la classification sociale doit être basée sur l'ascendance.

## IV- les stratégies de risk management dans le domaine des SI en fonction de la théorie culturelle :

Le système d'information est constitué par :
- l'information stockée et transformée
- le hardware et le software utilisés pour transformer l'information
- un système social formé par les actions et les relations entre les utilisateurs du SI

→ le contexte social est un aspect critique du SI qui ne peut pas être ignoré par le processus de risk management
La théorie culturelle a été beaucoup utilisée dans les études sur la perception du risque et préconise que les manières dont le risque est perçu sont enracinées dans le contexte social.

**1) l'impact des 4 dimensions sociales sur le risk management** :

| | Types of cultural bias | | | |
|---|---|---|---|---|
| Initiation tasks | Hierarchy | Egalitarianism | Individualism | Fatalism |
| Selection of risk management method | Selection of methods based on experts decisions and widely accepted security standards (Lima and Castro, 2005; Marris *et al.*, 1996) | Selection of methods that encourage stakeholders' participation (Marris *et al.*, 1996) | Selection of methods based on cost-benefit analysis (Marris *et al.*, 1996; Langford *et al.*, 2000) | Users tend to accept whatever is imposed on them (Torbjorn, 2004; Marris *et al.*, 1996; Langford *et al.*, 2000) |

| Risk analysis tasks | Types of cultural bias | | | |
|---|---|---|---|---|
| | Hierarchy | Egalitarianism | Individualism | Fatalism |
| Risk identification<br>Risk estimation<br>Risk evaluation | Threats with regard to social order prevail for users (Torbjorn, 2004; Marris *et al.*, 1996; Langford *et al.*, 2000) | Users mostly fear threats related to their sense of equity or threats that may increase inequalities (Torbjorn, 2004; Marris *et al.*, 1996; Langford *et al.*, 2000)<br>Users expect to be informed about risk analysis (Finucane and Holup, 2005)<br>Level of tolerance against threats can be negotiated | Users mostly fear threats to their personal freedom (Torbjorn, 2004; Marris *et al.*, 1996; Langford *et al.*, 2000)<br>The level of tolerance against possible threats is expected to be justified by using cost-analysis criteria | Users do not pursue awareness of risk (Torbjorn, 2004) |

| Risk mitigation tasks | Types of cultural bias | | | |
|---|---|---|---|---|
| | Hierarchy | Egalitarianism | Individualism | Fatalism |
| Design | Security experts should select countermeasures and policies that do not alter the users' standard workflow | Security experts should expect resistance to controls that result from their analyses | Security experts should expect reluctance to accept rules from the users' side | Security controls should be embedded in users' tasks |
| Implementation | Informative awareness programs should be designed | Awareness programs should place emphasis on the justification of security measures.<br>Awareness programs should be based on the appropriate communication means | Awareness programs should emphasize on positive incentives to promote users' compliance with security rules and policies | Awareness programs should seek to bolster users' commitment to the organisation |
| Monitoring | Security experts should anticipate a tendency to cheat as a group in an orderly, disciplined and co-ordinated way from the users (Mars, 1996) | Security experts should expect limited adherence of rules from users who feel threatened by security controls | Security experts should expect a higher predisposition to risk taking procedure bypassing from the users' side users are expected to choose short-term personal advantage over long-term corporate benefit (Mars, 1996) | Security experts should expect limited breach of security |

**2) Formulation de stratégies de risk management sensibles au contexte :**
L'expert en sécurité doit étudier le contexte culturel du système d'information, decider quelles dimensions sociales il doit prendre en considération et, finalement, ajuster le risk management en fonction de ces dimensions.
A partir de cela, on peut identifier 4 stratégies de risk management distinctes. Ces stratégies seront développées en se basant sur les différents préjugés sociaux que les utilisateurs de Si peuvent partager (typologie grille/groupe)

| Types of Cultural bias | Risk Management stages | | |
|---|---|---|---|
| | Initiation | Risk Analysis | Risk Mitigation |
| Hierarchy | ○ Methods based on experts decisions and widely accepted security standards should be employed. | ○ Hierarchists strongly fear risks that threat social order. Stakeholders expect low tolerability to relevant risks. | ○ Countermeasures and policies should not radically alter the standard workflow.<br>○ Informative awareness programs are suggested.<br>○ During the monitoring stage the security experts should bear in mind that stakeholders tend to cheat as a group. |
| Egalitarianism | ○ Methods that encourage stakeholders' participation should be employed. | ○ Stakeholders are expected to consider threats to their sense of equity as most severe. Security experts are required to treat these risks with low tolerability.<br>○ Stakeholders are characterized by a desire to have all the information to make their own risk analysis.<br>○ They expect to negotiate tolerability levels. | ○ Stakeholders are expected to resist to various controls introduced as result of security experts' analysis.<br>○ During awareness and training programs the justification of security policies is recommended.<br>○ Security experts should expect incompliance to controls that may generate inequalities or to controls whose purpose isn't clear to stakeholders. |
| Individualism | ○ Methods based on cost –benefit analysis are considered as more appropriate. | ○ This type of cultural bias is characterized by fear to whatever threats the stakeholder's personal freedom. Stakeholders expect low tolerability to relevant risks.<br>○ The usage of cost-benefit criteria to define tolerability levels is recommended, since these are considered more valid. | ○ Stakeholders adopting this type of cultural bias are generally reluctant to accept rules.<br>○ Awareness programs should emphasize on economic rewards of compliance to rules.<br>○ During the monitoring stage security expert should be aware that these stakeholders have a predisposition to risk-taking, cheating and bypassing procedures. They also prefer short-term personal advantage over long term corporate advantage. |
| Fatalism | ○ Given that fatalists accept whatever is imposed on them and tend to be indifferent to the selection of risk management methods, all types of methods could be applied. | ○ Stakeholders are likely to consider risk analysis as meaningful, since they perceive risks as unavoidable. | ○ Security controls should be applied as a routine of stakeholders' job.<br>○ Security expert should propose awareness programs that enhance stakeholders' commitment to the organization.<br>○ During the monitoring stage security experts should bear in mind that stakeholders are not expected to infringe security controls for their personal gain. |