Chapitre 1 : Gestion des Risques : Déf, Typologie, et Composants.

I/ Définition générale du risque :

- le risque est une composante inhérente à la vie de toute l'entreprise qui œuvre dans un environnement dynamique. Ces risques sont liés aux facteurs sociaux, économiques, écologiques, politiques, juridiques, légals, et technologiques. Cette notion de risque compte 2 composants :

→ le degré d'incertitude (la probabilité) : le risque se rapporte à l'incertitude qui entoure des événements et les Rts futurs → l'objectif de l'Ese est de diminuer l'incertitude (Probabilité) de ces événements.

→ l'ampleur des conséquences : il s'agit du degré des dommages causés à l'Ese.

⟹ l'objectif de la gestion de risque ne pas de supprimer la totalité de risque pour atteindre le risque ozéro ; mais de déterminer les risques que l'Ese pourra assumer en fonction de sa stratégie et d'évaluer (minimiser) les éventuels des conséquences.

II. les Attributs d'un risque : Caractéristiques

a/ l'incertitude : Probabilité.

b/ le coût de risque : l'accumulation de conséquence : Matérielles, financières immatérielle).

c/ l'information : c'est un élément clés dans le processus de la gestion du risque par conséquence la mission de l'Ese à nos jours ne limite plus à la maximisation des profit mais plutôt elle a la mission immatérielle à savoir la collecte, l'exploitation, et la protection de l'information (c'est la mission de l'unité de l'intelligence).

d) le facteur temps.

e) la perception.

III/ la mesure du Risque :

- Deux Approches :

A/ Approche théorique : Elle se base sur 2 facteurs : a F1 : La Probabilité
b F2 : La gravité.

- Cette approche théorique compote 2 présentations de gestion de risque qui sont basés sur 2 principaux facteurs à savoir la probabilité (incertitude) et la conséquence (l'impact / gravité). Ces deux présentations se schématise comme suit : Conception 1: Présentation de Risque selon la fréquence et la gravité

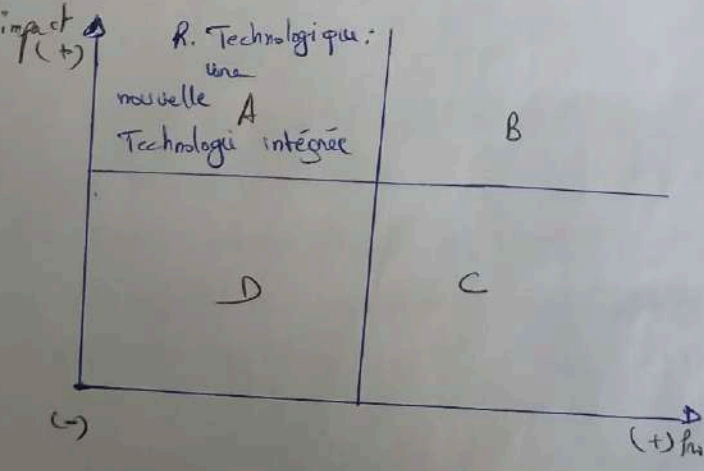
Fréquence / Gravité	Peu fréquent 0	moyenne fréquent 1	fréquent 2	très fréquent 3
0 Mineur				
1 Moyenne				Risque opérationnel
2 Majeure				
3 Critique	R. incendie			

échelle de Likert

- Conception 2 : le modèle Min / Max : st un modèle de hiérarchisation de risque en fonction de la conjugaison de deux composants : Fréquence d'occurance et gravité. Son objectif st de faciliter l'étude des risques et essayer par la suite de mobiliser (utiliser) les outils de l'IE afin de minimiser la réalisation des risques.

- Carré A : représente Le classement de risque qui ont un impact très fort sur l'organisation et dont la probabilité st faible.

- Carré B : représente le classement de risque qui ont un impact très fort sur l'activité de l'ES et une probabilité d'occurance très fort.



Modèle de hiérarchisation des risques.

- utilité : Aide le manager de Risque à mieux analyser la priorité des Risques.

B/ Approche sociale :

* l'approche sociale est basée sur un classement des risques selon 3 zones d'acceptabilité :

Tableau : Acceptabilité des risques :

Zone d'inacceptabilité : l'impact de risque est non acceptable socialement (cout sanitaire par exp) risque d'explosion nucléaire.

Zone de Tolérance : elle plus acceptée par la société.

Zone d'acceptabilité : l'impact mineur.

=> D'une façon générale la première approche théorique, elle se base sur la fréquence et la gravité et l'approche la plus utilisée par les E^ts vu son objectivité dans l'estimation et la gestion de risque, par ailleurs l'approche sociale est destinée plus pour les ministères dans la classification des risques d'ordre politique, naturelle, légale.

Mesure du risque

IV 1. Profil du risque :

- l'évaluation du contexte (Risque) requiert (nécessite) un traçage de profil de risque basé sur l'information qui va faciliter au risque manager d'identifier le risque potentiellement dans

Approche théo
- pour les entreprises
Qualit : prob
Impact
Quantitative : Calcul des Ratios (Risque)

App - sociale (Administrations ministères)
3 - zones.

⟶ le choix entre Approche théorique qualitative (Probabilité gravité) ou Quantitative (Calcul des ratios) n'est pas standard En effet, il dépend de perception et du nombre des informations (l'accès à l'info, fiabilité) collectées.

* Les 4 principaux caractéristiques qui identifient le profil de risque sont :

✓ le type de risque : Technologique, politique, contractuel, financière ...

✓ la source de risque : lié de l'environnement externe (économique, sociale, politique ..), interne (départements, manque de circulation d'info, lié à l'activité de département, gestion du Savoir, risque lié aux systèmes d'information).

✓ l'objet de risque : l'objet ou zone d'impact (personnels, réputation, En Terme matérielle, financière).

✓ le degré de contrôle du risque : la capacité de gérer le risque : Degré de contrôle soit élevé (le risque opérationnel), moyenne (Risque de réputation) ou faible (catastrophe).

IV / - Typologie des risques :

- Afin d'assurer une gestion efficace des risques, le manager des risques doit dresser une cartographie des Risques qui a pour objectif de mieux Comprendre les liens entre les différents risques et d'assurer une hiérarchisation de ces derniers. Plusieurs type de Cartographie sont utilisés par les E^ses.

Type 1 → Cartographie 1 :

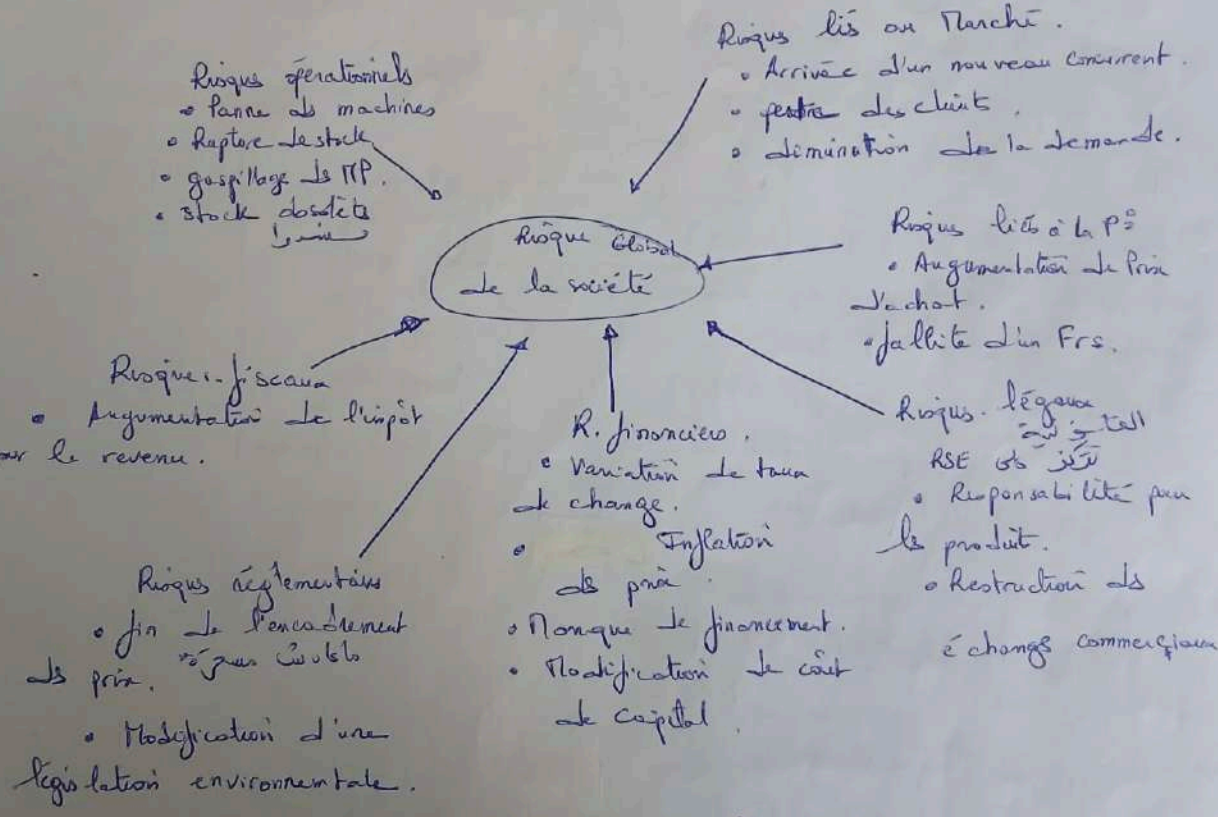
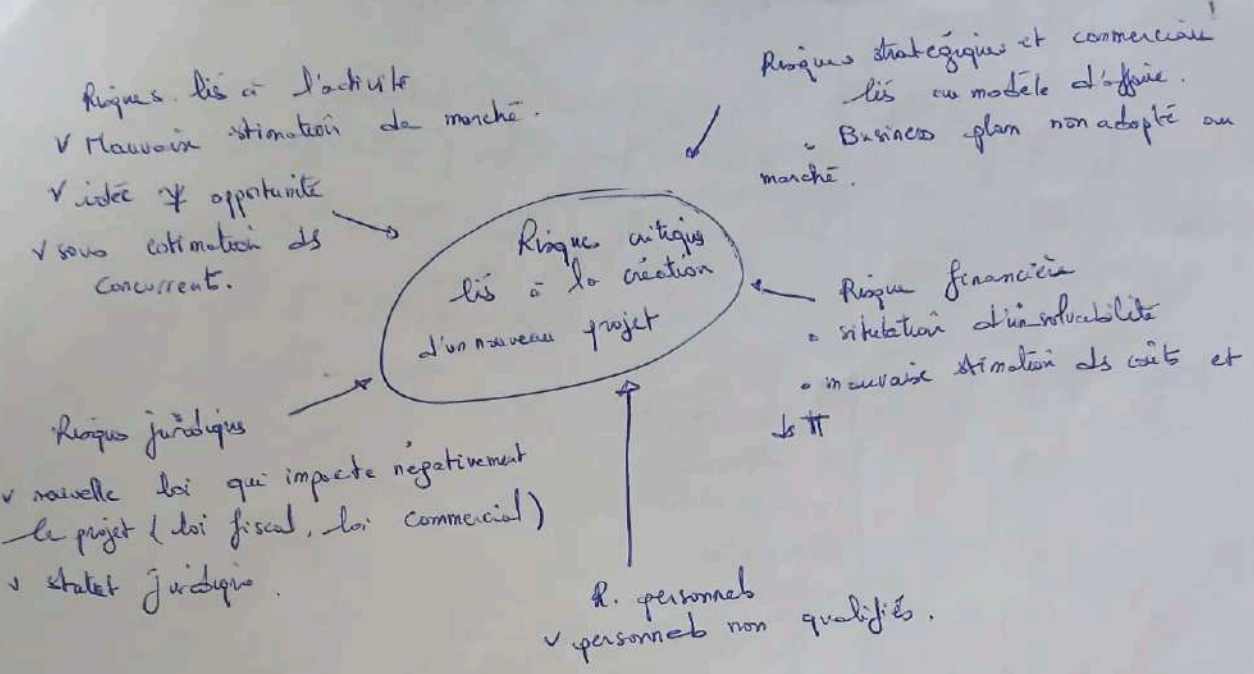


figure : Types des risques et leurs sources.

Type 2 : Cartographie des liés à la création d'une nouvelle entreprise (lancement d'un nouveau projet).



Type 3 : Cartographie exhaustive de risque :

famille de risques	Description
• Risques opérationnels	• Panne de ₦₦ • Panne de machines. • Rupture de stock • Risque logistique (Transport) • gaspillage de ₦₦Pfrts / Processus défectueux / dépendance à un seul frs. } il est lié aux activités d'exploitation de l'Ets
• Risques stratégiques	ils sont liés au modèle d'affaire de l'Ets dans le marché : • Risques liés aux Concurrents. (Forte concurrence dû à un avantage concurrentiel ; Mauvaise estimation de la dynamique de marché ; ₦ relation client (perte la capacité d'innovation). • Relation de confiance avec les investisseurs • Relation avec les employés.
• Risques financiers	• Cessation de paiement (insolvabilité) • Manque de liquidité. • La diminution de valeur en bourse. • Clients débiteurs. • variation de taux de change (En banques, en bourse)
Risques informationnels	lié à l'information : • Risques liés aux ressources = bien • la perte d'information stratégiques • la corruption de l'information. • La perte des données.

Risques Technologiques	+ Apparition des nouvelles Technologies non adaptées par l'Ets. + Risques liés aux Technologies de l'information. + Accident industriel (système erroné).
Risques fiscaux	liés à la politique fiscale du pays en vigueur. → Augmentation de taxe. + Mauvaise application de la loi fiscale.
Risque pays	+ guerre. + crise sanitaire. + Tolérisme. + corruption o Lié + révolution + conflits armés. + le réglement institutionnel. . Risque lié à la législation politique.
Risques environnementaux	→ Concerne l'écologie, protection de l'environnement, L'OMG,

VI). La gestion intégrée des risques : Outils pour une bonne prévention des crises :

L'objectif de cet outil est la prévention de tout évènement susceptible d'influencer négativement l'activité de l'Ets et de proposer des solutions pour diminuer la probabilité de réalisation des risques.

La gestion intégrée des risques doit faire partie intégrante de la stratégie globale de l'organisation. Cet outil est expliqué en 4 étapes :

E_1 : Identification et préanalyse : Cette étape vise à analyser et évaluer Tous les évènements susceptibles d'entrainer un préjudice ou une perturbation pourrait être à l'origine de l'état de crise.

E_2 : l'analyse détaillée et la quantification : cette étape vise à analyser les évènements perturbateurs potentiellement dangereux pour l'organisation. Cette analyse passe par 3 sous-étapes : ✓ évaluation (connaissance) du profil des risques. ✓ la mesure de risque selon une approche Théorique ou sociale ✗ en effet le manager de risque pourra étoffer le modèle min / max pour éliminer la gravité des facteurs ainsi que la probabilité d'occurance. ✓ Cartographie : Regrouper les risques pour hiérarchiser en fonction de leur impact et de leur tolérance (c'est urgent ou pas) et ce en dressant une cartographie des risques.

E_3 : Choix des solutions de traitement : Choisir un outil de L'IE

E_4 : le suivi (contrôle) : On contrôle si les solutions bien limiter les conséquences. / que les mesures prises fonctionnent et réduisent les risques.

* Chapitre 2 : Gestion des risques et IE : Relation de complémentarité.

I 1. Définition de l'intelligence économique (IE) :

- L'IE est un outil d'aide à la prise de décision : elle repose sur la collecte des informations pertinentes qui constituent une ressource stratégique pour l'entreprise.
→ l'IE est en soi un outil qui (vise) permet de saisir la réalité sur l'environnement de l'entreprise afin de réduire l'incertitude y afférente et par la suite diminuer la probabilité et l'impact du risque sur le bon déroulement de l'activité de l'Ese.

II 1. Interaction entre gestion des risques et Intelligence économique :

1/ IE : Trois Niveaux d'étude : Macro - Micro - Méso (économique)

- Les acteurs et les finalités sont différents selon que l'IE est utilisée et mise en place comme une politique publique (الدولة), comme un maillage Territorial ou comme une stratégie de protection de l'Ese.
- Les enjeux et les risques ne sont pas eux non plus identiques. Il aboutit à la mise en danger de la survie de l'Ese, à la pérennité du secteur ou à la maintien de la puissance d'un Etat.

Niveau d'étude	Niveau des risques	Niveau d'IE : Autorités compétentes intervenus.
Macro-économique (pays, بين الدول)	- Risque sécuritaire - R. Terroriste - R. pays. - R. monétaire - R. économique - R. politique	- Ministres - Hauts fonctionnaires : كبار المسؤولين - Conseillers ministériels. المستشارين الوزاريين
Méso-économique (بين القطاعات)	- Risque sectoriel - R. Territorial. - R. Technologique	- Conseillers régionaux. - Les administrations. - Chambre de Commerce. - Les syndicats. - Responsable de pôle administratif.
Micro-économique (في المؤسسة) = بين العمال	- R. opérationnels - R. informationnels - R. Technologiques - R. Concurrentiel - R. financiers. - " réglementaire - " stratégique. - R. politique ...	- Directeur de système d'information. - Responsable IE. (département gestion des risques) - Les directeurs des départements

2/ Lien entre les finalités de l'IE et les risques encourus par l'Ets :

- Les finalités (objectifs) de IE sont largement relié aux risques encourus par les entreprises :

Les finalités de l'IE		Risque associé.
La définition et la détention (assurer) d'un avantage Concurrentiel par la clarité de positionnement	la stratégique.	Risque stratégique.
l'anticipation législatifs et	des changement réglementaires.	Risque réglementaire.
La facilitation de culture fondée sur l'écoute et le partage. et la mise en place d'un adéquat.	de la création organisationnelle style de management	Risque d'inertie (asymétrie) manque de circulation de l'information
- la prévention inhérente	des suites ignorante à la mise en cause de l'image de marque de l'Ets.	Risque d'image.

III 1. Processus de l'intelligence Economique (4 étapes requises) :

E1 : Collecter : mettre l'intelligence à l'écoute de autre :

- la veille est pratiquer en fonction de besoin en information qui sont très définit au sein de département. elle permet d'acquérir de la matière grise (Information) qui intéresse le savoir, les compétences, - Ces informations doivent être pertinents, fiables et collectés au temps opportun.

- l'aptitude de la veille doit être présente chez tous les collaborateurs de l'Ets et cela même si une cellule de veille est dédié à cette opération. (consacré)

E2 : Réfléchir, analyser et mobiliser : Traiter l'information collectées.

- Stocker l'information : étape technique passive pour l'Ets, sa collecte n'est efficace que si elle est Traitée par la cellule IE. Cette étape fait appel à l'analyse et à la hiérarchisation des risques dont l'objectif de la proposition

ds recommandations managériales qu'ils font appel aux innovations produits, procesus ds législations, ds comportements concurrentiels et stratégiques.
Dans ce cadre, on pourra faire appel au lobbying, bunchmarking, communication de crise.

E_3: Capitalisation sur les ressources et les compétences:
- l'un ds principaux enjeux de la (conception) intelligence de l'E^x et de faciliter l'enrichissement ds informations existants, de créer ds pôles de compétence internes mais également de partager et de développer ds capacités d'apprentissage. Dans le management dans le cadre de l'IE doit capitaliser les savoirs créés en vue d'anticiper et gérer les risques stratégiques futurs de L'E^x.

E_4: Structurer et protéger le capital informationnel:
- Structurer l'information est nécessaire à toute les entreprises; de protéger et une condition vitale de survie pour les secteurs dits sensibles (RD, innovation, brevet, licence, l'invention. Parmi ds techniques et le mode de management utilisés afin de structurer et de protéger SI, on propose:
+ il faut éviter la diffusion de tout à tous mais plutôt diffuser en fonction ds besoins très précis ce qui permet d'éviter les fuites de l'information.
+ instaurer une équipe (voir département) responsables aux systèmes informationnels.

II 1. Intelligence économique (IE) et gestion des risques informationnels:
I/- IE: Intelligence du management: nouvelle compétence de L'E^x:
- face à la complexité de l'environnement économique > Technologique, sociale et même politique, la nouvelle compétence de entreprise s'exercent au cœur d'une réalité économique de plus en plus immatérielle. dès lors le dirigeant doit tenir compte dans la finalisation de sa stratégie que "l'énergie matière" mute vers une nouvelle économie fonctionnant sur "énergie information" (immatérielle). Au regard, de ce nouveau défis, l'objectif poursuivi par l'entreprise est de détenir une triple capacité:
+ capacité à collecter ds informations pertinente et optimistes (opportunistes) sur les différents acteurs de l'environnement (PESTEL).
+ capacité à gérer et exploiter l'information dans l'objectif de la rendre utile non seulement pour le dirigeant mais aussi à toute les parties prenantes internes et externes qui ont un impact sur la stratégie (contribuent à la compétitivité de l'E^x.). Dans ce cadre, on évoque aussi

la capacité de l'E^{se} à influencer avec intégralité son environnement par des actions de communication et de lobbying.

* Capacité à sécuriser son patrimoine informationnel constitué non seulement d'infrastructure Technologique mais aussi d'information, de savoir et de connaissances.

2°/ IE d'E^{se} : Intelligence du Management = (Système d'information : SI adapté à la démarche de l'E^{se})

a/ Exemple de menace lié au SI :

- Ds multiples sources de vulnérabilité (pas de sécurité) pourrait mettre en cause le système d'information qui émanent : * De l'E^{se} elle même : externalisation de certains activité liés au SI.
  + Information non qualifié / + Absence de Traçabilité.
  * De l'individu : + Non respect de réglementation SI.
  + inadaptation des compétence à certaine fonction critique lié à l'analyse des données.
  + Sous estimation des risque informationnels.
  * lié au « logiciels : + complexité croissante de ses logiciels source d'erreurs difficilement détectable.
  + Un large réseau de communication : E^{se} étendu «.
  * l'écosystème informatique : + concurrence, dépendance vis à vis des solutions américaines.

Ainsi nous pouvons citer quelques risque informationnel :

- R. Humaines : usage abusive d'internet, fraude, virus ; rumeur : Traitement non déclaré personnel.
- R. physiques : syniste, incendie, hypnotisation, vole des matériel

introduction de nouvelles Technologique dont le personnel ne maîtrise pas / sabotage.

b/ Les pratique de protection du patrimoine informationnel :

- le risque informationnel est double : D'abord, la captation ou le détournement d'information stratégique et ensuite la probabilité d'une information susceptible de modifier ou d'influencer négativement l'image, le comportement et la stratégie de l'E^{se}. Dans ce contexte, l'IE met en œuvre plusieurs stratégie de protection du capital informationnel :

→ Une stratégie de sécurité de l'information (R risque physique) : ce qui fait appel aux aspects organisationnels liés

Par ~~exponentiel~~ exemple :

+ Un double archivage des données.
+ développer des logiciels.
+ Maitrise de la divulgation de ses propres données.
+ choix de prestataire de service de confiance.
+ Définition d'une charte d'usage des ressources informatiques.

→ stratégie de lobbying et de communication :
(marque // العمل السياسي)

- L'E^se pourra procéder a une démarche informationnel, défense active (gestion de la réputation) contre les informations afin d'éviter les problème de destabilisation et de rumeur qui nuisent à son image de marque.

Par ailleurs, l'E^se pourra passer à des actions de communication maîtrisé et de lobbying.

→ S. adapter une équipe de SI.

- la définition d'une ~~pol~~ politique optimale de SI ceci fait appel.

il ~~est~~ définit et piloté par un responsable de sécurité de SI (RSSI).

- elle implique aussi d'autre acteurs c'est à savoir :

✓ politique de sécurité SI : Définit et piloté par RSSI.

• Assistée par d'autres acteurs :

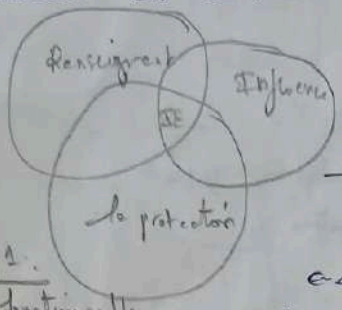
↓

- DSI
- Auditeurs interne.
- Risque manager.
- juriste.

-Chapitre III- Les outils de l'IE -

I/. Interaction entre la gestion de risque, IE et les outils de l'IE:

On peut considérer IE comme combinaison de Trois fonctions informationnelles: le renseignement, l'influence et la protection de l'information



» fig 1.
- Approche fonctionnelle de l'IE -

→ F1: (Fonction 1): la fonction de renseignement, elle sert à anticiper les menaces et les opportunités et à réduire l'incertitude liée à l'environnement. Par ce processus, elle cherchera à être mieux renseigné sur l'environnement que ses concurrents. l'objectif de la fonction de renseignement, l'asymétrie de l'information (عدم تناسق المعلومات) pouvant exister entre l'entreprise et ses concurrents au profit de la firme se renseignant sur les autres.

Il ne s'agit pas d'espionnage mais plutôt de renseignement économique légale.

→ Parmi les outils de l'IE qui vont permettre à l'ici de pratiquer la fonction de renseignement: le cycle de renseignement, la veille à travers ses différents types.

→ F2: L'influence: a pour vocation de modifier l'environnement par des pressions pour exercer cette fonction informationnelle. Parmi les outils de IE le plus connus on trouve le lobbying qui sont une pratique d'influence classique, exercée par des entreprises de forte pouvoir, et de ressources financières importantes.

→ F3: la fonction de protection: Elle sert à protéger les informations détenues par les entreprises. → Parmi les pratiques de la protection (voir paragraphe chapitre 2) le système d'information.

⇒ Par conséquence, l'IE est un mode de gestion et d'Asymétrie Informationnelle qui vise à augmenter cette asymétrie au profit de la firme qui la pratique qui lui confère ainsi une source d'avantage Concurrentiel.

(voir figure 1)

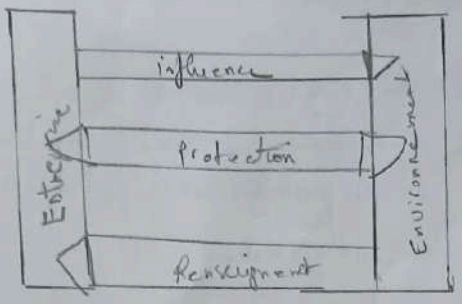


fig2: l'IE comme mode de management stratégique de l'information.

II- les outils de l'IE : (voir page 124)

1 - le cycle de renseignement : et une méthode de collecte et de gestion de l'information il est également un instrument d'audit puisqu'il permet de repérer les besoins critiques en information, les pistes d'[illegible] peut-être dangereux et par la suite permet de réduire l'incertitude à la prise de décision.

- il est structuré autour de 4 phases importantes :

① Expression du besoin :	② Recherche et collecte.
④ Diffusion de l'information :	③ Traitement / Analyse.

Tableau : cycle de renseignement.

→ Phase 1 : la première phase de cycle permet d'identifier les enjeux, les besoins en informations et en renseignements, elle traduit les axes de recherche, qui sont ensuite traduits en zones de recherche et en question opérationnel. Le besoin s'exprime ainsi généralement sous forme de liste de questions adressées aux agences de collecte des données.

→ la phase 2 : la recherche et la collecte définissent la période d'action de recensement ou de recueil des informations ainsi les unités de collecte identifient les sources légales et choisissent les moyens de collecte. il faut d'éviter l'espionnage.

→ Phase 3 : Traitement et analyse pendant cette phase les informations passent par un état de réflexion en vue d'élaborer des conclusions stratégiques en vue d'une prise de décision fiable. Ce qui nécessite un processus d'évaluation, d'interprétation et de synthèse. Ainsi, les informations sont traitées et gérées en fonction de leurs processus par des experts internes et externes.

→ finalement phase 4 : C'est la transmission des renseignements aux organes cibles responsables dans un format adapté à la confidentialité des données. L'objectif de cette étape est l'organisation de la mémoire collective de l'E[illegible] et la réorientation en fonction de conclusion de la première analyse ou bien l'élaboration d'une nouvelle stratégie

2/. Le Lobbying : a/ Définition : se présente souvent autour d'un groupe de pression, l'objectif est de défendre à un intérêt commun et de pouvoir économique face aux concurrents mais aussi des garanties des usages de pression face au gouvernement.

→ Une activité de lobbyisme est le fait de communiquer avec un Titulaire d'échange publique en vue d'influencer une décision à caractère législatif, réglementaire ou administratif.

b/ les acteurs de lobbying :

b1/ le lobbyiste : quelque soit leur titre ~~profit~~ professionnel le lobbyiste est personne qui en échange d'une contre partie pour le compte d'un client d'une entreprise ou d'une organisation communique avec les titulaires de charges techniques est vue d'influencer leurs décisions stratégiques.

Ex/ esp : les lobbyistes peuvent être : des responsables des relations gouvernementales, des consultant en relation publique, en communication stratégique ou

b2/ Titulaire de charge : qui a le pouvoir de prendre la décision.
- au niveau parlementaire : - de député et membre de leur personnel.
- " " gouvernementale : les ministres et les membres, employés de gouvernement.
- " " municipales : le maire, les conseillers municipaux.

b3/ Décision visée : Un l'activité de lobbyisme toute communication orale ou écrite faite auprès d'un titulaire d'une charge publique en vue d'influencer une décision déterminée par exp :

- L'élaboration ou la modification ou le rejet d'une proposition législative ou réglementaire ou d'un programme d'action.
- l'attribution d'un permis d'une licence ou d'un certificat.
- " " " contrat dans le cadre d'un appel offre publique ou d'une subvention d'un projet.
- la nomination d'un administrateur publique telque du secrétaire général de l'Etat ou les secrétaires de ministères.

b) Activités de lobbyisme : Elle récapitule tous les actes intervenant dans l'activité de L'Etat.

- Exp: les acteurs de lobbyisme : le président d'une association regroupant des entreprises d'Aluminium fait des représentations auprès du ministère de l'économie, de l'innovation et de l'énergie dans le but d'influencer le maintien d'une orientation sur la disposition du bloc d'énergie par les aluminerie Québécoise, leur permettant ainsi d'assurer leur développement et de participer à la création des emplois.

Quels sont les acteurs intervenant dans la situation ?

- le lobbyiste : le président d'une association regroupant des entreprises d'aluminium.
- le titulaire de charge : le ministère de l'économie . . . .
- Décisions visées : le maintien d'une orientation sur la disposition du bloc d'énergie.
- Activité de lobbysme : à expliquer.

4 les types de lobbying

* le lobbying général culturel : c'est la capacité de changer l'opinion, les habitudes. ce lobbying s'exécute souvent sur le long terme auprès de leader d'opinion et de média qui influence l'opinion publique.
* le lobbying stratégique : il représente un lobbying dirigé vers un environnement politique économique, juridique . . son objectif est de faire évoluer les différentes visions en une seule vision commune qui sert des intérêts d'un groupe particulier.
* le lobbying ciblé : il est orienté plutôt vers un environnement ciblé et vise d'obtenir un avantage compétitive face à un environnement concurrentiel.
* le lobbying général : il consiste à défendre un secteur d'activité ou une industrie précise.

a/ La veille Concurrentielle (voir page : 126) * objectif : collecter les différents informations qui concernent les concurrents (stratégie Rct D, les efforts fournis par les concurrents, politique de 4P, part de marché ....

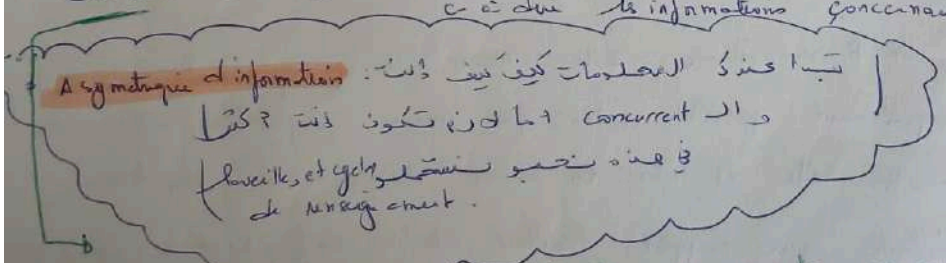
b/ la veille Technologique. (Page : 127).

* objectif : la veille doit cibler toutes les questions et les problématiques liés à l'innovation Technologique et qui permettra à l'Ets d'améliorer son efficience et d'assure un avantage Concurrentiel.

c/ la veille commerciale : (p: 127).

- fait référence à la recherche et de traitement de renseignement relative à l'évolution de marché et des clients. son objectif est de bien comprendre les besoins des clients à long Terme afin de proposer des nouvelle façons, innovations qui concernent le produit. et assurer un avantage concurrentiel face au marché.

De même la veille commerciale permet de suivre l'évolution en amont de marché c-à-dire les informations concernant les Frs., les clients ...



cette veille concerne l'analyse de marché en amont et en aval.

d/ la veille sociétale : (p. 128)

Déceler le changement qui s'opère dans la société et qui impact de transformer et perturber l'activité de l'Ets et son environnement.

e/ la veille environnementale : (PESTEL) (129)

- son objectif est de surveiller l'environnement "PESTEL".

f/ la veille juridique : (130)

objectif : surveiller les lois et les décrets, les débats parlementaires, les propositions

g/ la veille brevet (p 130) : fait référence à la recherche, relative aux brevet marque de déposer afin d'éviter toute copie ou piratage. de renseigner

- Benchmarking : p(134, 135, 136, 137)

a/ - Benchmarking interne : objectif : se pratique à l'interne d'une organisation - dans les grandes entreprises les process similaires se retrouvent dans différents départements ainsi aisé de faire des comparaisons afin de déterminer le meilleur processus

b/ Benchmarking concurrentiel : se réfère à une entreprise externe généralement leader dans ce domaine. La comparaison dans le cas s'effectue dans des activités similaires.

c/ Benchmarking - générique : consiste à comparer les Ex les plus excellents, ayant des processus similaires et quelque soit domaine d'activité.

→ la démarche de benchmarking peut se dérouler en 4 grandes phases :

✓ l'état diagnostic (Identification des cibles et des objectifs).

✓ la collecte des informations.

✓ l'adaptation et le dépouillement. (déploiement)

✓ l'observation des Rés et les ajustements possible.

D5 - la communication de crise :

- En tant que outil de l'IE, la communication de crise revet 3 stratégies principals : → S. de Reconnaissance : Elle consiste à accepter l'existence de crise de plus rapidement possible. donc par mener l'opération de communication l'entreprise doit aller vite et être en mesure de déterminer rapidement si elle est compétente par rapport hauteur de la crise (Elle a la capacité de gérer ce problème ou non). Pour être totalement efficace, cette communication nécessite une grande clarté. Il faut jouer sur la transparence et acquérir une crédibilité auprès de l'opinion public.

→ Cette stratégie vise à admettre sa responsabilité, toutefois s'il apparaît dévoilé la crise avant l'E" ce que la communication de celle ci est mauvaise et que la crise n'appartient déjà plus.

→ stratégie de diversion : Son objectif, est de changer l'angle de vue de la crise auprès des médias et de l'opinion publique. ainsi, il s'agit de reposter (renvoyer) la responsabilité à l'Extérieur, en disant tout ce qui profite de la situation

ou bien à appuyer sur le fait que le pire a été évité.
تقول ذلك خلال الاستجواب.

→ S. de refus de la crise : Elle consiste à nier l'évidence et à refuser toute l'état de crise dans l'organisation, à minimiser l'effet de la crise, à garder le silence de ne pas alimenter la crise ou bien à ne pas communiquer dès le début → Par contre, c'est avec le temps, de nouvelles informations contredisent ou appuit la culpabilité de la direction, cette stratégie pourra avoir des réelles impacts négatives sur son image et donc la firme risque de perdre sa crédibilité face à l'opinion public et les médias.