CH-V./ LA GOUVERNANCE DES SI

1. DEFINITIONS

Dans son sens la plus large la gournance peut designer la strategie mise en œuvre pour atteindre les objectifs. La gourvenance consiste a fixer au si les objectifs lier a la strategie de l’entreprise.

Schema

* 1. Gouvernance des SI et gouvernance des TI

Très souvent on constacte une confusion en entre la gouvernance des TI et SI, ils n’ont pas le même objectif et ne suivent pas la meme demarche.

* La gourvenance des TI s’occupe de l’utilisation des technologie de l’information, des technologie informatique afin d’ameliorer la productiviter des entreprise ou des organisations
* La gouvernance des SI a pour but d’ameliorer le fonctionnement des systemes d’informations des entreprises et plus generalement des organisations. Elle conserne non seulement la direction de l’organisation mais aussi tous les metiers de l’entreprise qui concours a la creation de valeurs grace au SI.

La gouvernance des SI a pour but de definir quels sont les principaux objectifs. Les fonctions et les taches pour alimenter la nouvelle fonction du management.

* 1. Bonne pratique de la gouvernance

La mise en œuvre des SI reponse sur la gouvernance d’un certain nombre de pratique connu des tous les professionnelles. Elle concerne 4 domaines :

* Conception d’un système d’information
* Le fonctionnement et le pilotage des systemes d’information
* Le pilotage et l’evolution des SI
* L’evolution des SI

Exemple de bonne pratique :

* Un SI permettre d’augmenter les volumes traiter ;
* De reduire les couts unitaires des operations
* Un SI dois etre conçu par un professionnel qui peut etre un architecte fonctionnel
* Un SI dois disposer les tableaux de bord permettant de suivre les évolutions et le cas echeant de prendre des mesures collectifs.

1. Gestion des risques des SI

**Risque = Menace + Vulnerabilites**

**Incident = consequence d’un probleme.**

# Pour ne plus avoir d’incident faut regler les problemes

#Incident : coupure d’electriciter.

#Vulnerabiliter = trou, petit cloture

#Menace : qui ? quoi ?

1. Les risques humains

Les risques humains sont les plus importants meme s’ils sont le plus souvent ignorer ou minimiser. Il concerne les utilisateurs mais egalement les informaticiens eux-meme.

* + La maladresse : comme pour toute activites les humains peuvent commettre des erreurs. Ils leurs arrivent plus frequenment d’executer, d’effacer involontairement des programmes
  + L’inconscience et l’ignonrance : de nombreux utilisateur de l’outils informatique sont inconscient au risque qu’ils accours sur les systemes qu’ils utilisent et introduisent souvent des programmes malveillants sans le savoir.
  + L’ingénierie social : méthode pour obtenir d’une personne des informations confidentielles que l’on n’est pas senser obtenir en vue de les exploiter a d’autre fin. Elle se consiste a ce faire passer pour quelqu’un qu’on n’est pas et de demander des information personnels(login, mot passe, donnee confidentielles).

1. Les risques techniques

Les risques techniques sont lier au defaut et panne inevitable que connaissent touts les système materiels. Cependant les pannes on des causes indirectes, voir très indirect difficile a prévoir.

Si on peut le plus souvent negliger la probabiliter d’une erreur d’execution d’un processeur, la plupart des composants electroniques peuvent comporter des defauts et finissent un jours ou l’autre par tomber en panne.

* + Incident lier au logiciel : ils sont tres loin les plus frequents. ils empeche les processus metiers de fonctionner. Il s’agit des bugs applicatifs.
  + Incident lier a l’environnement : les machines électroniques et les reseaux de communications sont sensible au variations de température ou d’humidité ainsi qu’au lier au magnetiques. Il n’est pas rare que les ordinateurs connaissent des pannes definitifs a cause de conditions climatiques inhabituelles.

1. Risques juridiques

L’ouverture des applications sur le web et la mltllcatin des mssags lctn agmnt ls s jsd. Lr a l’sags ds tchnlgs.on peu citer notament :

* Le nn respect de la legislation relative a la signature numerique.
* Le nn respect de la legislation a la vie privee.

1. Les indicateurs de la perfomance

Une gouvernance efficace des si passe par suivi desindicareurs clees. A savoir :

* **La disponibiliter des systemes**.

Le suivi de la disponibilider des système represente un premier indicateur clee. Face a ces donnee, il n’est important pour le directeur des si de pouvoir anticiper l’evolution des besoins en ressource informtif en vue de prevoir et planifier la monter en puissance de l’infrastructure existant.

* **La qualiter des services, des processus metiers :** en terme de qualiter de service, la direction informatique ne peut passer a coter d’une supervision de la qualiter de service par rapport au applications ou processus metiers.
* **Le temps de retablissement en cas d’incident** : les indicateurs technique de disponibiliter ceter par la supervision du volume de charge encaisser par les serveurs et surtout les temps de reponse globaux des temps de système
* **Le niveaux de securiter du si** : parmi la grande mission du dsi figurent celle de garantir l’integriter et la garantie des donner stocker.
* **Le degree de satisfaction client(utilisateurs)** : il permet de prendre la température de vision que les salarier on vis-à-vis de la dsi.
* **Efficaciter des investissements informatiques** : toute une serie d’indicateur et leurs nevolution dans le temps permettent l’efficaciter des investissements informatiques
* **L’etat d’avancement des projets si** : le suivi de l’etat d’avancement d’un chantier informatique passe par celui du portefeuille de projet
* **L’efficaciter du support client et de la maintennace** : la performqnce du support s’evalue financierement en fonction de l’assistance du cout de l’utilisateur. La qualité de service se mesure qd a elle du nombre de ticket ouvert et de la duree moyenne des appel et de la duree moyenne de resolution d’incident
* **Le degree d’alignement strategique** : au niv strategique, le tableau de bord du resp infomatique a pour mission de suivre le respect du bussnes plan la dsi.

#Indicateur viendra devoir

1. Securiter des SI

* 1. – Risque

Probabilité pour que survienne un evenement nusible par rapport a une menage. et peu influencr sur la réalisation des objectif

4.2- Menaces

Cause potentiel d’un incident indesirable, qui peut nuire a un système ou a une organisation.

Les differents types de menace sont :

* Dommage physique par exemple feu
* Désastre naturel par exemple tremblement de terrer, inondation, foudre
* Perte de service essentiel par exemple panne de climatissation, panne electrique.
* Perturbation causer par radiation par exemple radiation electromagnetique
* Information compromise par exemple vol de document.
* Panne technique par exemple saturation du reseaux.
* Origine des menaces

|  |  |  |  |
| --- | --- | --- | --- |
|  | Naturelle | Deliberer | Accidentelle |
| Incendies | X | X | X |
| Vol equipement |  | X | X |
| Tremblement de terre | X |  |  |

4.3- Risque et mesure << Danger >>

Un element percu comme negatif est un risque pouvant freinner la creation de valeur ou detruire la valeur existante d’une organisation.

C’est pourquoi le risque negatif est souvente associer a la menace. On definie habituellement le terme <<danger>> comme une categorie de risque contre laquelle l’integrite physique des personnes est menacer.

Definition scientifique de risque :

Espérance mathématique d’une fonction de probabilité d’evenement.

Des qu’un evenement a moins de 100% de chance de se realiser il y’a risque.

Une gestion de risque efficace permet de réduire l’incertitude et de prevoir le futur.

Pour prevoir le futur ils vous faut des donnees fiable tels que evenement du passer, simulation de probleme probabiliste.

#Examen : cours 10 points & etude de cas 10 points

|  |  |  |
| --- | --- | --- |
|  | Menace | Risque |
| Incendies | Court-circuit | Degats |
| Vol | Voleur | Perte |
| Hackeur | Hacker | Perte |
| Virus informatique | Virus | Incident |
| Incident | Pluies | Perte |

4.4 – Le risque et probabilite statistique

En securte de l’information par exemple une enquete statistique nous apprend que 2% des employees fournissent au moins un faux document lors de l’embauche. Une entreprise de 10 000 employer peut deduire quel pourrais etre confronter a 200 cas internes. Comment l’entreprise pourrais devrais agr connaissant ce risque et quel sont les options possibles ?

4.5 – Le risque et les opportunites

Les scenarios a risques peuvent representer des opportuinites pour des organisations. Les principes repose sur la prise de risque soit un gain ou avantages supplementaires puis esperer en participant a une activiter plus risquer.

Par exemple, en implémentant un logiciel on a les risques superieurs(Bug, incompatibiliter avec les autres applicatons) et les gains de productiviter esperer doivent etre encore plus grand.

1. Stratégie de gestion du Risque

|  |  |  |
| --- | --- | --- |
|  | Stratégie de gestion du Risque | Exemple d’application en securite de l’information |
| Positive | Maximiser le retour sur l’investissement en tenant compte de la prime | Prendre le risque d’investissement dans lses projets a fort rendement le risque |
| Neutre (Incertitudes) | Calculer les probabiliter s des differents scenario de risque | Effecuter le veille technologique et surveiller les risques |
| Negatif (Menace) | Eviter, transferer, Reduire | Eviter les technologies pour securiser |

1. Definition du risque en Securite

La definition du du risque en securite de l’information est generalement lier au aspect negatif de la et a la menace

Ainsi, la premier objectif de la securiter de l’information n’est pas d’augmenter les opportunuiter des objectifs mais de limiter les possibiliter de perte. Le risque c’est l’effet de l’incertitude sur l’atteinte des objectifs.

Un risque en securiter de l’information est souvent :

* Exprimer en terme de combinaison les connaissances d’un evenements associer a la probabiliter de survenu
* DEfinis comme la possibiliter qu’une menace des donnees exploite la vulnerabliter d’un actifs de l’information et nuire donc a l’organisme.

1. Objectif et mesure de securiter

L’objectif de la mesure est la declaration decrivant ce qui est a accomplir par suite de la mise en place des mesures. La mesure est le moyen du management du risque.

On a  les mesures techniques, les mesures administratives, les mesures managerialles et les mesures juridiques.

1. Les 10 principes du management du risque en SI

Le management du risque créer de la valeur et de la reserve, les principaux sont :

* Le management du risque est intergrer au processus organisationnel
* Le management du risque est integrer au processus de prise de decision
* Le management du risque traite explicitement de l’incertitude
* Le management du risque est systematique, structurer et utiliser en temps utile.
* Le management du risque s’appuis sur la meilleurs information disponible.
* Le management du risque est adapter.
* Le management du risque integre les facteurs humains et culturels
* Le management du risque est transparent et particicpatifs
* Le mangement du risque est dynamique, iteratif et reactif au changement
* Le management facilite l’amelioration continue de l’organisme

1. Les avantages de la mise en œuvre du Management du Risque

Ces avantages sont :

* Accroritre la vraisemblance d’atteindre les objectifs
* Ameliorer l’identification des oportunuite et des menaces
* Amelioere la redaction des rapport obligatoire et volontaire
* Ameliorer la gouvernance
* Etablir une base fiable pour la decision et la planification
* Ameliorer les moyens de maitrise

10- Les types de vulnerabilite

* Materiel informatique : manque ‘entretien, cadre non approprier
* Logiciel : absence d’entretien des logs, interface de saisie compliquer
* Reseaux : Absence de chiffrement des transfere, point unique des acces.
* Personnel : fromation insuffissante, manque d’encadrement

Exercice :

#Pour mettre en place un système d’information il faut rencenser les activiter

Cas SIGMA

1. Donner 5 information du texte en precisant type, source, forme, qualite
2. Ressence 3 faiblesse de l’activiter de sigma
3. Quel sont les qctiviter de la’activiter sigma
4. Donner 3 fonction de sigma
5. Presenter par un schema le si, son environement et les flux
6. Quels sont les composante actuel du si de sigma

#On ne peut pas laisse progiciel comme xa