Audit SI

.David Autissier:

1) Le SI peut être décomposé en 5 grands métiers complémentaires:

1. Le pilotage du département SI: pour définir la Stie, la veille, les schémas directeurs et tableaux de bord de la fonction.

2. La gestion de la relation avec les utilisateurs: qui s'intéresse à toutes les prestations à réaliser pour assurer un niveau de service maximum à l'utilisateur.

3. Le développement applicatif: pour tout ce qui concerne les projets d'informatisation.

4. La maintenance applicative: pour traiter de toutes les actions de suivi et de contrôle du parc informatique existant.

5. La gestion de l'infrastructure technique: pour la mise à disposition de l'équipement machine et réseau.

→ Le référentiel de la fonction SI sera représenté par ce prisme en 5 rubriques métiers, pour chacune de ces 5 catégories, nous définissons les pratiques et les Ates qu'une fonction S'I peut effectuer, cette liste se veut exhaustive, dans la limite du possible. Ce qui doit être fait dépend des Ese, de leur secteur d'Até, du nombre de personnes composant la DSI et également du positionnement de cette fonction

2)

1. Structure de la grille d'évaluation.

Ates	Réalisation de l'Até		Importance de l'Até pour l'Ese	
	Oui	Non	Faible	Forte

Pour chacune des Atés, nous établirons si elle est réalisée ou non, et si elle est importante ou non pour l'Até de l'Ese. Celle permettra de faire une évaluation d'Até par un ta d'Até global et par un taux d'Até contingent qui tiendra compte de l'importance des Atés pour l'Ese.

2. Les questionnaires d'évaluation des Atés.

Les 24 Atés précédentes regroupées en 5 rubriques nous donnent un périmètre de la fonction que chaque Ese adaptera en fonction de sa stratégie en termes de SI, mais également en fonction de l'historique de construction de cette fonction.

Dans tous les cas, cette liste d'Atés constitue un référentiel mobilisable pour toute action d'évaluation, de réorganisation et d'évolution de la fonction SI

3. Le taux d'Até

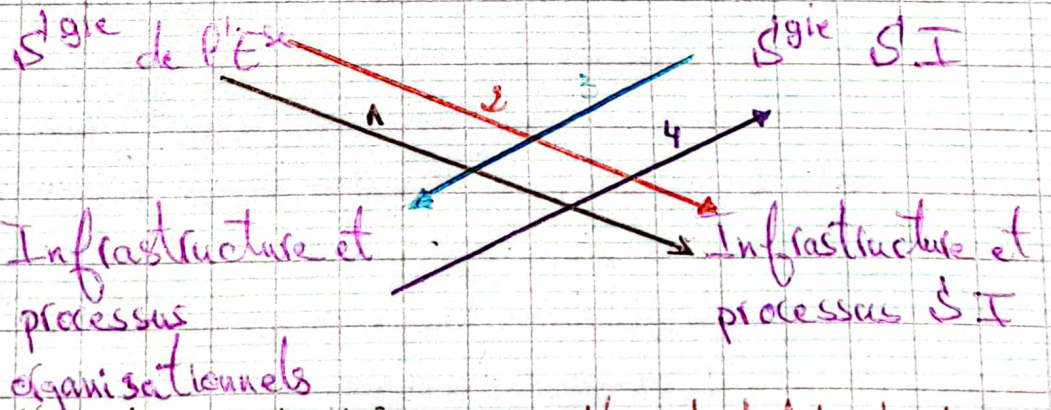
- Les différentes Atés définies dans le paragraphe précédent sont ensuite évaluées au regard des pratiques réelles dans les Eses pour déterminer, sur les 24 Atés types recensées, le % de celles réalisées dans l'Ese.
- Le ta d'Até des différentes rubriques sont ensuite synthétisés en un seul indicateur.
- Le ta d'Até permet de positionner la fonction SI sur une échelle de 0 à 100 avec 4 configurations types,

ta d'Até	
100	
75	SI exhaustif
50	SI développé
25	SI restreint
0	SI minimaliste

* La stratégie : est un ensemble d'actions coordonnées, d'opérations habiles, de manoeuvres en vue d'atteindre un but précis. Son but est d'atteindre les objectifs fixés par la politique en utilisant au mieux les moyens à disposition.
* La gouvernance : est un ensemble de décisions, de règles et de pratiques visant à assurer le fonctionnement optimal d'une organisation, ainsi que les organes structurels chargés de formuler ces décisions, règles et pratiques, de les mettre en oeuvre et d'en assurer le contrôle.
* Alignement stratégique : L'expression alignement Sgique se réfère au fait de mettre en place des processus au sein de l'Ese afin de faire concorder ses ambitions avec l'opérationnel. L'alignement Sgique peut concerner de fait toutes les strates et composantes de l'organisation, et assurer une parfaite coordination entre la Sgie globale et la structure organisationnelle et les différents services de l'Ese.

obf : . assurer la pérennité et la croissance.
. Rendre en compte la valeur des SI
. De faire du Sce informatique un service transversal
. Optimiser les dépenses liées au SI

Henderson & Venkatraman



1 : L'exécution de la Sgie 2. Dév d'un potentiel technologique
3 : Dev d'un avantage concurrentiel fondé sur la technologie
4 : Amélioration de la Qté de service

Ensuite, on dénombre 4 grandes composantes, c'est elles qui doivent s'aligner pour assurer une parfaite coordination:

- Stgie de l'Ese: son positionnement sur le Méché et son réseau d'affaires
- L'infrastructure et les processus organisationnels c-à-d Comment l'Ese s'organise au quotidien
  - Structure hiérarchique
  - Communication
  - Déroulé des opérations de chaque service
- Stgie SI: Il s'agit là encore de Stgie, mais se rapportant aux SI:
  - Technologies
  - Compétences
  - Gouvernance, etc...
- L'infrastructure et les processus SI à l'instar des processus généraux, ils codient les opérations... mais côté SI. Cette composante concerne alors:
  - Les applications utilisées
  - Les technologies employées
  - La manière dont les projets de développement.

Urbanisation du SI: Est une discipline d'ingénierie informatique consistant à faire évoluer le SI de celle-ci afin qu'elle soutienne et accompagne efficacement les missions de ladite organisation et anticipe ses transformations.

2. Démarché d'élaboration d'une mission de diagnostic

1. Établir un questionnaire de prise de connaissance
2. Établir un CR de mission comprenant 5 axes:
   - ✓ Prise de connaissance générale
   - ✓ Analyse de l'existant en matière de métiers et processus
   - ✓ Structure de SI de l'Ese
   - ✓ Prévisions et scénarios futurs

✓ Accompagnement de changement
3. Élaboration d'un nouveau SDSI

Processus d'implémentation et certification ISO 27001

- C'est un processeus long et complexe, donc il faut décortiquer et simplifier les mots clés.
- La période et le temps de la réalisation, ça varie entre un an (min), 3 ans et plus, ça depend de la taille de l'Ese et le volume de l'information.

La légende: La boucle PDCA, dans le processeus il y'a des Ates qui sont liés au domaine Plan, Do, Check, Act, avec des couleurs, et dans la culture amélioration continue.

↳ On peut dire que le processeus de certification s'inscrit parfaitement dans la boucle PDCA (des Ates liées à la planification, réalisation...) et chaque Até à des éléments d'entrée et de sortie.

En jaune (les livrables) En vert (les exigences de la norme)
En bleau (livrables exigés par la norme et qui vont faire l'objet de la certification)

1) La politique: Exigence de la norme qui demande l'appui de la direction (ne se sont pas des intentions, mais des faits (engagement de la direction à mettre en place les R^ces nécessai pour mettre en place la démarche qui va aboutir à la certification ou à mettre en place un SMSI). Concrétisé par des décisions (CR, PV, ...) + les documents.
2) Une fois on a la preuve que la politique est conforme aux exigences de la norme, on passe à la définition du périmètre du SMSI (domaine de définition), si vous ratez le Df, vous ratez les RT, le périmetre doit être définis clairement (dans certains cas on peut réduire la certification uniquemei domaine logiciel et matériels, c'est possible mais ce n'est pas bien) - le périmetre concerne l'ensemble des A. Informatio

3) 2ème étape la plus dure, l'identification des caractères de l'actif et l'évaluation des risques liés à ces actifs. L'inventaire est représenté sur un cylindre (support numérique) Excel, Access, logiciels spécialisés). On trouve des ESI spécialisées dans les logiciels d'inventaire des A. Informationnels (gestion des biens - CH7)

4).a/ Définir la méthode d'analyse des risques: Est ce que vous disposez des méthodes concernant les risques liés au Serveur Exp: Méthode EBIOS / MEHARI

4).b/ Justification des Rts par un rapport
Outils: Inventaire, (Rt = identifier et classifier les Rs et d'évaluer les risques en se basant sur des méthodes) SOA (statement of Applicability): revenir sur les chapitres de la norme et vérifier si ce chapitre est totalement/partiellement ou non appliqué et de donner par la suite les commentaires nécessaires), c'est grace au AMOA qu'on identifie les éléments clés qu'on doit travailler dessus afin d'améliorer le système. Soit les compétences en interne ou des cabinets spécialisées pour élaborer ces outils. Il faut que l'ensemble ou la majorité des exigences soit totalement appliquée (80% à 90%) pour pouvoir faire appel à la certification

6) Sur la base de l'inventaire, les rapports de risque et SOA on identifie un certain nombre de projet et chaque projet doit être documenté

7) Projet d'implémentation du SMSI: Après l'identification des risques, on passe à l'amélioration continue et par la suite on passe à l'évaluation de la pré-certification (voir si on est vraiement prêt ou pas encore). il faut avoir l'audit à blanc avant l'appel des auditeurs de certification (sont très exigeants).

- L'audit à blanc: Formulaire auto-diagnostic. chaque exigence (V/F), enfin on va avoir les Rts sous graphique par chapitre de la norme ainsi que le Rt global.
- Revue de conformité: Peut se faire par des réunions (projet par projet) et voir les actions correctives mais l'audit à blanc se fait d'une façon globale (SM global)

De 12 à 13, il faut avoir 80% à 90% pour arriver à l'audit de certification (revue de direction, DG, DSI, responsables des projets pour décider quels sont les actions à faire pour passer de 80 à 90, et quand est ce que on fera appel et quel organisme choisir) - Certificat pour 3 ans (la 1ère fois est compliquée)

Zakaria BOUHARROU