Chapitre 3
Auditer et évaluer un système d'information

1. Auditer, c'est décrire et qualifier

Auditer un système d'information consiste à l'appréhender dans sa globalité et dans sa complexité, tout en identifiant ce qui fait sa force, sa faiblesse, ainsi que les risques de le dégrader. Pour cela, nous devons disposer d'un outillage pour, d'une part, décrire la situation sans omission et sans rien laisser dans l'ombre, et d'autre part, qualifier cet existant afin d'en avoir une vision critique. La 2MSI nous apporte le soutien méthodologique nécessaire :

– La matrice en 21 briques nous permet d'organiser les investigations et de ne rien laisser de côté.

– Les trois critères de supervision, et leurs neuf sous-critères, nous donnent l'outillage pour qualifier le niveau de fonctionnement du SI.

Nous faisons ci-après l'hypothèse que l'audit porte sur la totalité du système d'information pris pour objet.

2. La matrice 2MSI structure la méthodologie de l'audit

La réalisation de l'audit suppose d'identifier et de collationner les données nécessaires à caractériser le système d'information de l'organisation. Pour chacune des briques de la matrice 2MSI, il s'agit de conduire une démarche d'évaluation.

Ainsi, si l'on considère la brique infrastructures réseau et télécom, la première en haut à gauche de la matrice, il faudra lui appliquer les trois critères et neuf sous-critères définis précédemment, afin d'établir l'état du SI en ce domaine.

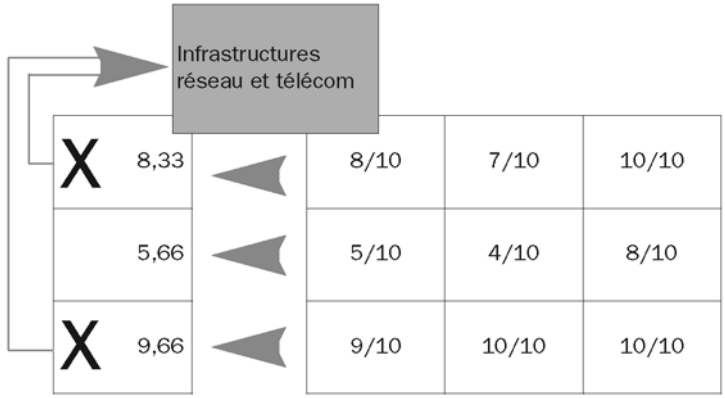
Analyse de la brique infrastructures réseau et télécom

Infrastructures réseau et télécom

Critères	Sous-critères		
Qualité de management du SI	Qualité de la maîtrise d'ouvrage	Qualité de la maîtrise d'œuvre	Documentation du SI
Pertinence des moyens mobilisés	Pertinence des RH Qualité des relations contractuelles	Qualité intrinsèque des outils technologiques	Coûts et analyse de la valeur
Performance des résultats obtenus	Satisfaction utilisateurs	Gestion proactive des incidents	Démarche qualité

Pour qualifier cet état, attribuons une note de 1 à 10 à chacun des trois sous-critères. Celle-ci dépendant de son niveau de satisfaction. La moyenne des sous-critères permet une cotation du critère, lequel est réputé servi s'il obtient une note au moins égale à 8.

Cotation de la brique infrastructures réseau et télécom



Chaque brique (ici, la brique Infrastructures réseau et télécom) est alors évaluée selon le nombre de critères servis et revêt une couleur :

– Brique gris clair : trois critères servis. Des améliorations sont peut-être nécessaires, mais la politique conduite dans ce domaine fonctionnel est suffisamment mature pour assurer sa part dans la cohérence du SI.
– Brique gris moyen : deux critères servis. Il existe une politique active, mais celle-ci est incomplète. Des actions sont indispensables.
– Brique gris foncé : un seul critère servi. La politique conduite est indigente et met en danger la cohérence du SI. Il convient d'engager immédiatement un plan d'action.
– Brique noire : aucun critère servi, ce qui exprime une quasi-absence de politique de gestion du SI dans le domaine concerné. Nous sommes en présence d'une zone de danger absolu.

Dans cet exemple, deux critères sont servis, la brique est donc gris moyen.

La méthode 2MSI permet ainsi un monitoring coloré de la situation du SI. Elle fournit, de façon très visuelle, un état des domaines prioritaires d'action.

Exemple de monitoring coloré, suite à l'audit du SI d'une PME de services

Infrastructures réseau et télécom	Supervision et exploitation réseau - Gestion opérateurs réseau & télécom	Intégrité, sécurité et PRA réseau & télécom
Serveurs (Hébergement et OS)	Supervision et exploitation serveurs	Intégrité, sécurité et PRA données et configurations
Devices (PC, tablette, smartphone)	Support et exploitation devices. Helpdesk	Sécurité devices
Editique	Support et exploitation parc éditiques. Helpdesk	Sécurité Confidentialité Coûts
Utilisateurs (annuaires, messagerie, bureautique)	Gestion droits, messagerie, bureautique	Sécurité et PRA annuaires, messagerie, accès
Applications métier	Supervision et exploitation applications métier. Relations éditeurs	Sécurité, intégrité et PRA applications métiers
Risques	Supervision des risques. Evaluation des impacts	Assurances, assistance juridique. Gestion de crise

Dans l'exemple ci-dessus, on observe que la politique de management du SI comporte deux zones noires (sécurité des environnements utilisateurs et sécurité des environnements métier) ; deux zones en alerte (sécurité des environnements serveurs et gestion des environnements utilisateurs) ; et six zones fragilisées (gestion des actifs réseau ; support utilisateurs ; sécurité des outils personnels ; gestion des relations éditeurs, supervision des risques, gestion des impacts en matière de risques). Ce monitoring coloré permet d'identifier immédiatement les domaines dans lesquels des actions prioritaires doivent être entreprises.

3. La matrice 2MSI organise les informations nécessaires à la réalisation de l'audit

Une fois la méthode définie, la principale question que se pose l'auditeur, est d'inventorier la matière dont il a besoin pour qualifier ce qu'il a à auditer. Dans cette perspective, nous nous adossons aux neuf sous-critères de cotation afin d'organiser cet inventaire, en répondant pour chacun d'eux à deux questions : que dois-je observer ou collecter ? Quelle méthode vais-je utiliser pour collecter et traiter cette information ?

Nous reprenons ci-après un exemple d'inventaire élaboré pour auditer le SI d'un de nos clients, la Spicojeu, en l'occurrence un important établissement public industriel et commercial :

Qualifier la qualité de la maîtrise d'ouvrage

Éléments à observer et/ou collecter	Méthodes de collecte et traitement
Organigramme et définition des responsabilités.	Observation. Entretiens. Étude des fiches de poste. Si besoin, reconstitution des fiches de poste.
Outil de gestion de projets : comptes rendus de comités de pilotage ; tableaux de bord ; outils de reporting ; position de la maîtrise d'ouvrage dans les procédures.	Observation. Entretiens. Étude des documents.
Compétence de l'intervenant délégataire de la maîtrise d'ouvrage. Posture dans l'organisation.	Observation. Entretiens. Étude des CV. Entretiens avec l'encadrement supérieur.

Qualifier la qualité de la maîtrise d'œuvre

Éléments à observer et/ou collecter	Méthodes de collecte et traitement
Organigramme et définition des responsabilités.	Observation. Entretiens. Étude des fiches de poste. Si besoin, reconstitution des fiches de poste. Et/ou étude des contrats de prestations ou d'infogérance.
Outils de gestion de projets : comptes rendus de comités de pilotage ; tableaux de bord ; outils de reporting ; position de la maîtrise d'œuvre dans les procédures. Outils de gestion de procédure.	Observation. Entretiens. Étude des documents. Étude des procédures et des méthodes d'intervention opérationnelle.
Compétence des maîtres d'œuvre. Posture dans l'organisation.	Observation. Entretiens. Étude des CV. Entretiens avec l'encadrement supérieur. Entretiens avec les maîtres d'ouvrage.

Qualifier la politique de documentation du SI

Éléments à observer et/ou collecter	Méthodes de collecte et traitement
Outils de gestion de la documentation primaire : notices, manuels, licences, programmes, codes. Base de connaissances. Méthode de préservation et de classement.	Vérification en posture d'audit sur site. Analyse des documents remis. Vérification par sondage aléatoire.
Outils de gestion de la documentation opérationnelle du SI : inventaires, descriptifs, plans, comptes rendus d'intervention. Base de connaissances. Méthode de préservation et de classement.	Vérification en posture d'audit sur site. Analyse des documents remis. Vérification par sondage aléatoire.
Outils de gestion de la documentation de structuration opérationnelle du SI : fiches de procédure, check-lists, plan de gestion des risques, plan de reprise d'activité.	Vérification en posture d'audit sur site. Analyse des documents remis. Vérification par sondage aléatoire.

Qualifier la pertinence des ressources humaines (internes) et la qualité des relations contractuelles

RH (internes)	
Éléments à observer et/ou collecter	**Méthodes de collecte et traitement**
Organigramme. Fiches de poste. CV.	Observation. Entretiens. Étude des fiches de poste. Si besoin, reconstitution des fiches de poste. Vérification des capacités d'expertise.
Complémentarité des compétences. Complétude des expertises.	Analyse des CV et domaines d'expertise. Analyse du taux de couverture des champs d'expertise adossée à la matrice 2MSI. Analyse de conformité entre politique d'internalisation et périmètre des expertises.
Politique de formation. Politique de transmission et partage des savoirs. Veille professionnelle.	Observation. Entretiens. Analyse plan et bilan de formation. Analyse des outils et méthodes de gestion des savoirs et de veille professionnelle.
Gestion des ressources humaines. Gestion prévisionnelle des emplois et des compétences. Ensemble des indicateurs de bilan social à l'échelle de la DSI.	Étude du bilan social de la direction des systèmes d'information. Analyse de la politique de GPEC de la DSI.