REPUBLIQUE DU CAMEROUN

Paix – Travail – Patrie

****

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR

****

REPUBLIC OF CAMEROON

Peace – Work – Fatherland

****

MINISTER OF HIGHER EDUCATION

****

Université de Dschang

Institut Supérieur de Technologie et du Design Industriel

Mémoire de fin d'étude

AUDIT DU SYSTEME D'INFORMATION DES RESSOURCES HUMAINES DE L'INSTITUT UNIVERSITAIRE DE LA CÔTE

En vue de l'obtention du Master Professionnel en Système d'Information Audit et Conseil

Rédigé et soutenu par :

CHEBOU CHOUPE Gabriel

Matricule N° : ISTDI11E002496

Licence en Génie Logiciel

Devant le jury composé de :

Président : Pr TCHINDA René

Rapporteur : Dr BOWONG T. Samuel

Examinateur : M. NYAM Aquila

Sous la supervision de :

Dr NOUMEDEM KENFACK Jaurès

Sous l'encadrement académique de :

M. NYAM AQUILA

Enseignant à l'IUC

Sous l'encadrement Professionnel de :

Mme BAZIRUTWABO N. Sabine

Responsable Ressources Humaines - IUC

Année académique 2016-2017

Je dédie ce mémoire à

Mme SELENOU Née KENMOE Thérèse

REMERCIEMENTS

De nombreuses personnes nous ont apporté leur soutien dans la réalisation de ce mémoire et nous tenons à leur exprimer ici toute notre gratitude. Il s'agit :

- M. NYAM Aquila qui nous a fait l'honneur d'être notre encadreur. Nous le remercions profondément pour son encouragement continu et aussi d'être toujours là pour nous écouter, nous aider et nous guider par ses précieux conseils. Ce qui a contribué à la mise sur pied de ce document
- Dr NOUMEDEM Jaurès, notre Superviseur pour ce mémoire, qui nous a suivis et surtout recadré afin que nous puissions produire ce document.
- Dr FOTSING Christian, avec qui nous avons murit les recherches sur l'audit des systèmes d'information pendant deux longues années et qui a été notre principal support pour la mise en œuvre de notre travail.
- Mme BAZIRUTWABO N. Sabine, notre encadreur professionnel, qui de par son expertise, nous a permis de cerner le métier afin de pouvoir mener à bien notre mission.
- L'équipe de développement SEED qui nous a été d'une aide précieuse dans le déroulement de notre mission.
- Nos enseignants de l'Institut Universitaire de la Côte pour leur dévouement et leur assistance tout au long de nos études universitaires.
- Nos parents sans qui ont œuvrés pour que nous soyons l'étudiant que nous sommes aujourd'hui.
- Nos oncles et tantes qui ont été à la base de notre parcours académique de par leurs sacrifices.
- M. et Mme CIAMS, pour le soutien qui a été le leurs lorsque nous étions en difficulté.
- Le personnel de la DAAF (Direction des Affaires Administratives et Financières) de l'Institut Université de la côte ; ainsi que tous les collègues qui de par leurs encouragements nous ont permis d'atteindre notre objectif.
- Nos camarades de promotion avec qui nous avons passé de nombreux moments.

SOMMAIRE

LISTE DES ABREVIATIONS

CT : Comité Technique

EN : European Norm – Norme Européenne

IEC : International Electrotechnical commission - Commission Electrotechnique Internationale

ICS : International Classification for Standards -Classification Internationale pour les normes

IIA : Institue of Internal Auditors

ISO : International Standards Organisation – Organisation International de Normalisation

ISACA : Information System Audit and Control Association

NC : Norme Camerounaise

NF : Norme Française

GTA : Gestion de Temps d'Activité

SI : Système d'Information

SIRH : Système d'Information des Ressources Humanes

LISTE DES TABLEAUX

LISTE DES FIGURES

RÉSUMÉ

Le système d'information est le socle sur lequel repose l'activité de l'entreprise. De ce fait, il est en soumis à de nombreuses contraintes. Les évolutions dans la gestion des ressources humaines, ont donné lieu à un système d'information des ressources humaines aujourd'hui fortement informatisé de telle sorte que lorsqu'il ne l'est pas, il semble inefficace. Pour garantir un système d'information répondant aux besoins d'une activité, la démarche souhaitable est de mener un audit de celui-ci afin de mettre en miroir ce qui est fait et ce qui devrait être fait, et faire des recommandations pour l'amélioration de la productivité de celui-ci. Le thème qui a été l'objet de ce mémoire est intitulé « audit du système d'information des ressources humaines à l'Institut Universitaire de la Côte ». Les différentes tâches qui ont été les nôtres nous ont permis de prendre connaissance l'environnement des systèmes d'information des ressources humaines.

De plus, l'audit des actifs applicatifs et de la sécurité que nous avons menés grâce aux questionnaires et aux interviews réalisés au regard des normes internationales ISO 27001 (le système de management de la sécurité), ISO 27002 (Code de bonne pratique pour le management de la sécurité de l'information),des référentiels de bonnes pratiques tels que CObIT (Control Objectives for Information and related Technology, en français Objectifs de contrôle de l'Information et des Technologies Associées) fournit par l'ISACA (Information System Audit and Control Association), a permis de dresser le bilan sur l'état actuel du système d'information des ressources humaines. Et nous avons abouti par des recommandations qui pourraient permettre d'améliorer les points faibles de notre cible d'étude.

Nous pouvons dire de manière générale que, compte tenu du fait que l'application soit encore en cours de développement, il n'est pas judicieux de dire que l'IUC doit se mettre à la quête d'une nouvelle solution. Mais, l'absence d'une politique de sécurité du système d'information reste une faiblesse à laquelle il faudra y remédier.

ABSTRACT

The information system is the foundation on which the business activity is based. Because of this, it is subject to many constraints. Changes in the management of human resources have given rise to a computerized human resources information system today, in such a way that when it is not, the human resources information system seems ineffective. To ensure an information system that meets the needs of an activity, the desirable approach is to conduct an audit of the activity in order to have an idea of what is being done and what should be done, and make recommendations for improved productivity. This academic work is entitled "Audit of the Human Resources Information System at the University Institute of the Coast". The various tasks undertook allowed us to become acquainted with the environment of human resources information systems.

In addition, the audit of the application assets and the security that we carried out thanks to the questionnaires and the interviews carried out according to the international standards ISO 27001 (the system of safety management), ISO 27002 (Code of good practice for the information security management), benchmarks of good practices such as CObIT (Control Objectives for Information and Related Technology), provided by ISACA (Information System Audit and Control Association), made it possible to take stock of the current state of the human resources information system. This helped us come up with recommendations that could improve the weak points of our study target.

We can say in general that, given the fact that the application is still under development, it is prematured to say that the IUC should look for a new solution. We can say in general that, given the fact that the application is still under development, it is not wise to say that the IUC must be looking for a new solution. But, the absence of a security policy for the information system remains a weakness that must be addressed.

INTRODUCTION GENERALE

Dans le monde aujourd'hui, l'informatisation du système d'information est devenue un enjeu majeur pour la pérennité de l'entreprise.

L'Institut Universitaire de la Côte a entrepris depuis 2015 d'informatiser ses différents processus métiers. Et pour ce faire, il a développé un progiciel de gestion intégré (PGI) qui devrait permettre d'optimiser les processus de l'entreprise en vue de permettre à ses différents métiers de créer de la valeur. La fonction gestion des ressources humaines s'est vue doté des modules GRH et Paie. Cependant, la gestion des ressources humaines et paie nécessite un système d'information de qualité et sécurisé de manière à satisfaire aux exigences de qualité d'une bonne information ; ainsi que, permettre aux personnes en charge de la gestion des ressources humaines d'être plus productives. C'est dans ce contexte que nous avons entrepris une évaluation du sous-système d'information des ressources humaines; permettant de faire un état des lieux du niveau d'intégration du progiciel mis en place, pour les activités de la fonction de gestion des ressources humaines au sein de cette organisation. De ce fait, quelques point, doivent être passés en revue afin d'y apporter d'éventuels contributions. Ainsi, nous avons évalué la qualité de l'information, l'alignement stratégique de l'application ; ainsi que la sécurité du système d'information des ressources humaines.

Le choix du sujet « *audit du système d'information des ressources humaines* » s'inscrit dans une démarche académique et scientifique que nous nous sommes données. En effet, ce thème trouve sa justification dans le fait que la fonction gestion des ressources humaines de par ses multiples tâches, dont certaines sont spécifiques à la taille de l'entreprise, au secteur d'activité ; doit disposer d'un système d'information fiable, sécurisé et performant. C'est le cas notamment à l'Institut Universitaire de la côte qui exerce dans le domaine de l'enseignement, et où les informations utilisées par les processus du système d'information des ressources humaines font l'objet des variations continues en raison des mouvements du personnel dans le domaine éducatif. Et l'on doit donc disposer des outils garantissant au minimum l'intégrité, la fiabilité, la disponibilité des données malgré les nombreuses fluctuations qui interviennent dans l'entreprise en matière de gestion des ressources humaines.

Ce mémoire est structuré en quatre (04) chapitres dans lesquels, nous avons tour à tour présenté l'état de l'art sur l'audit des systèmes d'information des ressources humaines, l'état de lieu du système d'information des ressources humaines de l'Institut Universitaire de la Côte ; ensuite la mise en œuvre de l'audit du système d'information des ressources humaines de l'Institut Universitaire de la Côte et enfin les résultats de l'audit et les recommandations.

CHAPITRE I : ETAT DE L'ART SUR L'AUDIT DES SYSTEMES D'INFORMATION DES RESSOURCES HUMAINES

Ce chapitre a pour objectif de dresser l'état de l'art de l'audit des systèmes d'information des ressources humaines. C'est une démarche préliminaire qui nous permettra de capitaliser les savoirs et les savoirs faire existants pour mener à bien ce projet. Elle présente de manière succincte et condensée les bases et les approches théoriques de ce travail. Étant donné que l'objectif est de faire une appréciation objective du système d'information de gestion des ressources humaines.

SECTION I. Système D'Information Des Ressources Humaines

Pour mieux cerner la notion *« Système d'Information de gestion des ressources humaines* », nous allons l'aborder dans cette section à travers celle de SI. En effet, le SIRH est un sous ensemble d'un SI.

1. Notion de système d'information

Les auteurs définissant ce qu'est un système d'information le font habituellement selon une ou plusieurs de ces trois perspectives : en partant du contenu informationnel au cœur de tout système d'information, en insistant sur sa dimension technologique, ou en y incluant une composante humaine.

Un SI peut être aussi défini comme un ensemble de composants inter-reliés. Celles-ci recueillent, traitent, stockent et diffusent de l'information afin d'aider à la prise de décision, à la coordination, au contrôle, à l'analyse et aux capacités de représentation de situations au sein d'une entreprise (LAUDON, et al., 2013)

D'autres auteurs étendent le périmètre du SIRH aux êtres humains. Ainsi, pour (ANGOT, 2005) , un système d'information est :

- d'une part, un ensemble organisé d'éléments qui permet de regrouper, de classifier, de traiter et de diffuser de l'information sur un phénomène donné ;
- d'autre part, un réseau complexe de relations structurées où interviennent hommes, machines et procédures, qui a pour but d'engendrer des flux ordonnés

d'informations pertinentes provenant de différentes sources et destinées à servir de base aux décisions.

Selon (REIX, et al., 2011), le SI est « un ensemble organisé de ressources : matériel, logiciel, personnel, données, procédures… permettant d'acquérir, de traiter, de stocker des informations (sous forme de données, textes, images, sons, etc.) dans et entre des organisations»

Nous retrouvons dans cette définition les principales caractéristiques et les fonctions d'un système d'information. Elle souligne également une organisation conséquente des ressources humaines et informatiques pour la gestion des informations.

(GILLET, et al., 2010) Regrettent l'assimilation courante entre système d'information et technologie. Il s'agirait là d'un signe de notre époque de n'envisager les systèmes d'information qu'au travers du prisme de l'informatisation. Selon ces auteurs, des systèmes d'information reposant uniquement sur l'utilisation de techniques manuelles (p.ex. Papier et crayon) ou sur des échanges informels d'information pourraient tout autant être qualifiés de systèmes d'information.

Pour plus de confort de lecture, lorsque nous ferons référence au terme système d'information (SI), nous parlons bien entendu de systèmes d'information informatisés. Cette définition rappeler le rôle fondamental d'un SI qui est celui de fournir des informations susceptibles d'aider à prendre des décisions stratégiques, budgétaires et opérationnelles.

2. Définition du Système d'information des ressources humaines

On retrouve les mêmes tendances relevées ci-dessous lorsqu'il s'agit de définir un système d'information destiné aux ressources humaines (SIRH).

La perspective centrée sur le contenu informationnel du SIRH est défendue par (KOVACH, et al., 1999) pour qui le SIRH « est un process systématique/méthodique utilisé pour acquérir, stocker, mettre à jour, extraire et valider des informations nécessaires pour une entreprise au sujet de ses ressources humaines, des activités de son personnel et des caractéristiques de ses unités organisationnelles ».

D'autres auteurs décrivent le SIRH au travers du rôle de support technologique qu'il offre aux activités RH:

Ainsi, pour B. Merck « le SIRH est un ensemble de logiciels plus ou moins interconnectés qui permettent d'assurer de façon cohérente différents actes administratifs et des opérations de gestion appliquées aux ressources humaines »

- Ou encore F. Silva, pour qui « le SIRH est un progiciel qui informatise, d'une part, un certain nombre de tâches des différentes missions de la fonction RH et, d'autre part, leur circuit de l'information […] La logique de mise en place d'un SIRH induit que les tâches qui seront automatisées vont ainsi constituer une suite de flux d'informations à valeur ajoutée »

On retrouve ici aussi certains auteurs qui reconnaissent l'inclusion d'une composante humaine dans la définition du SIRH :

- Hendrickson : « Le SIRH n'est pas limité au matériel informatique et aux logiciels qui constituent la partie technique du système. Cela inclut aussi les personnes, les politiques, les pratiques et les informations nécessaires pour remplir la fonction RH. De ce fait, un SIRH fonctionnel doit créer un système d'information qui permette l'intégration des politiques et des pratiques utilisées pour gérer le capital humain de l'entreprise ainsi que les pratiques requises pour utiliser le système informatique »

Cette définition élargit le périmètre du SIRH en prenant en compte les utilisateurs, leurs objectifs et leur environnement. Cette précision a, à nos yeux, toute son importance puisqu'elle pose la priorité des finalités stratégiques de la GRH sur le SIRH chargé de les servir.

3. Système d'information des ressources humaines (SIRH) et Système d'information (SI) de l'organisation

On entend souvent des personnes, responsables de la gestion des ressources humaines, affirmer que certains points de vue et informations sur les personnes de leur organisation ne les intéressent pas, car ils n'appartiennent pas au SIRH, mais au SI industriel ou autre qui concerne d'autres chefs de services.

L'approche globale de la systémique permet de raisonner de manière plus pertinente. Dans l'optique d'un système d'information, système nerveux de l'organisation, on voit bien que les sous-systèmes ne peuvent fonctionner de manière totalement

indépendante les uns des autres et s'ignorer. On ne pourra donc parler du SIRH qu'en tant que sous-ensemble du SI global de l'organisation.

Cependant le SIRH aura un angle de vue correspondant au domaine de gestion et de prise de décision du service RH. Ce sera une qualité essentielle des outils, qui composeront le système d'information, que de permettre des angles de vue différents et des accès régulés aux informations d'un même objet, au sein d'un ensemble commun cohérent.

Les principes de base des outils utilisés dans le SIRH, doivent être les suivants :

- Une base de données unique où les informations ne sont pas redondantes
- Une ergonomie unique, facilitant l'apprentissage de l'utilisateur et de la productivité.

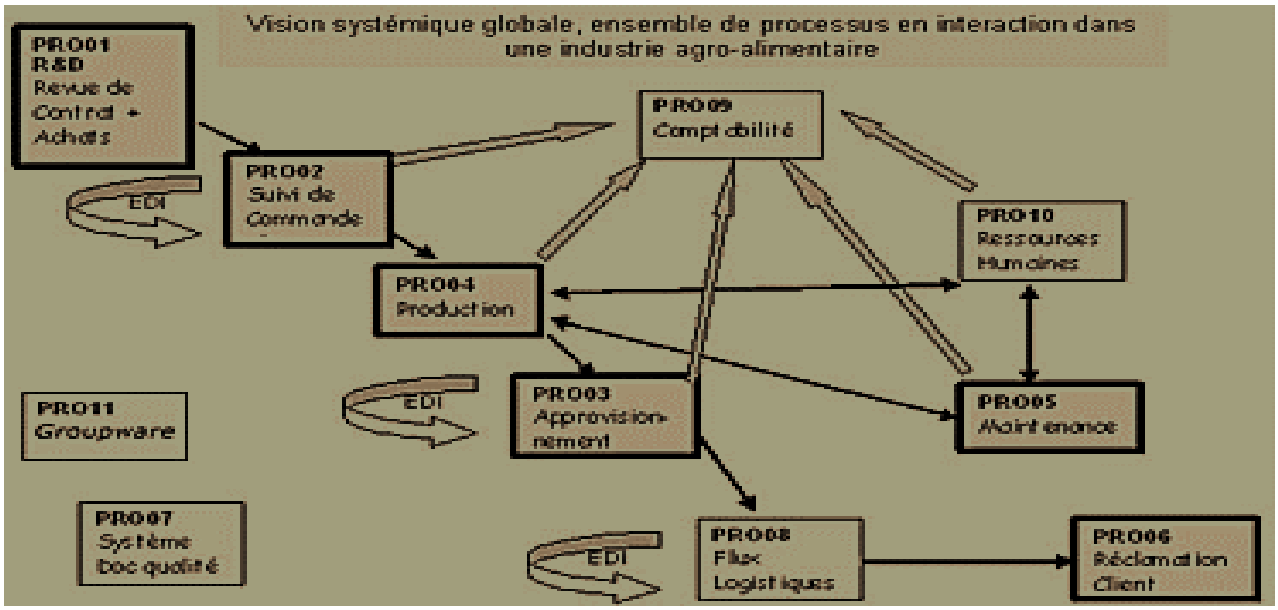


Figure 1: Positionnement du SIRH dans la vision globale de l'organisation

Deux remarques essentielles s'imposent :

- Le SIRH est une composante fonctionnelle du SI, c'est-à-dire qu'il constitue un processus support par opposition aux processus opérationnels.
  Les processus opérationnels sont ceux qui ont pour but de créer la valeur ajoutée dans l'organisation. Ils représentent l'exercice du « métier » de l'organisation. Les processus supports offrent aux processus opérationnels un cadre leur permettant de réaliser leur travail créateur de valeur ajoutée dans de bonnes conditions ;

- Le SIRH n'est pas isolé, mais au contraire, par sa position dans le système global, il doit être alimenté par des informations émanant d'autres processus, à caractère opérationnel. Il s'agira notamment des ordres de fabrication, bons de travail ou relevés d'heures, destinés en priorité au contrôle des coûts et de la gestion, mais pouvant alimenter également le suivi de l'annualisation du temps de travail et la paie.

  De son côté, le SIRH participe à l'alimentation du processus support comptabilité. En effet, la comptabilisation des salaires devra être automatisée, afin de déverser les charges salariales en comptabilité.

4. La composition d'un SIRH

Il existe une multitude de représentations de la composition d'un SIRH dans la littérature académique et professionnelle. La revue Entreprises & Carrières fait d'ailleurs le constat suivant : « Le SIRH ressemble de plus en plus à un gigantesque jeu de Lego®. Au programme : des solutions qui s'interfacent à tous les étages ! Un véritable patchwork d'outils cohabite désormais dans cet écosystème qu'est devenu le SIRH. D'où l'intérêt, nous semble-t-il, d'établir une cartographie fonctionnelle des offres développées par les éditeurs de logiciels»[1]

La revue s'est lancée dans un projet de cartographie fonctionnelle SIRH de grande ampleur, articulé autour de sept thématiques RH (recrutement, formation, compétences et connaissances, temps et activités, rémunération globale, paie et tableaux de bord), où la revue a interrogé pas moins de soixante éditeurs de logiciels présents sur le marché pour connaître la couverture fonctionnelle de leur outil.

De leur échantillon, il en ressortait que :

- 24 éditeurs ne couvrent qu'un seul thème RH, ce sont des spécialistes ;
- 18 éditeurs couvrent entre deux et trois thèmes fonctionnels, 12 d'entre eux gravitent autour du recrutement, de la formation, de la gestion des compétences et des connaissances alors qu'ils étaient auparavant spécialisés dans un seul de ces sujets ;
- enfin, 12 éditeurs sont de purs généralistes balayant l'ensemble des thématiques RH.

[1] « Solutions Informatiques RH », in Entreprises et Carrières, Hors-série n°2 (19 décembre 2006), n°837/838, p. 5.

B. Just modélise, pour sa part, le SIRH sous la forme d'un tableau listant un ensemble de processus, relevant de la gestion purement administrative et réglementaire, à une gestion individuelle ou collective des RH:

Tableau 1: Modélisation du SIRH selon B. Just

Gestion administrative et réglementaire	Gestion individuelle	Gestion collective
Gestion administrative (GA)	Recrutement	Contrôle de gestion social
Gestion des temps et activités (GTA)	Formation	Gestion prévisionnelle des emplois et compétences (GPEC)
Paie	Performance, entretiens d'évaluation	Rémunération globale
Reporting		

Source : Nous-mêmes

a) Gestion administrative (GA)

Selon B. Just, la GA est un domaine difficile à cerner du fait que « […] sa frontière avec d'autres domaines est floue et qu'on ne sait pas déterminer précisément où elle commence et où elle s'arrête. Pour certains, les diplômes sont dans la gestion administrative et pour d'autres ils sont dans la gestion de carrière »

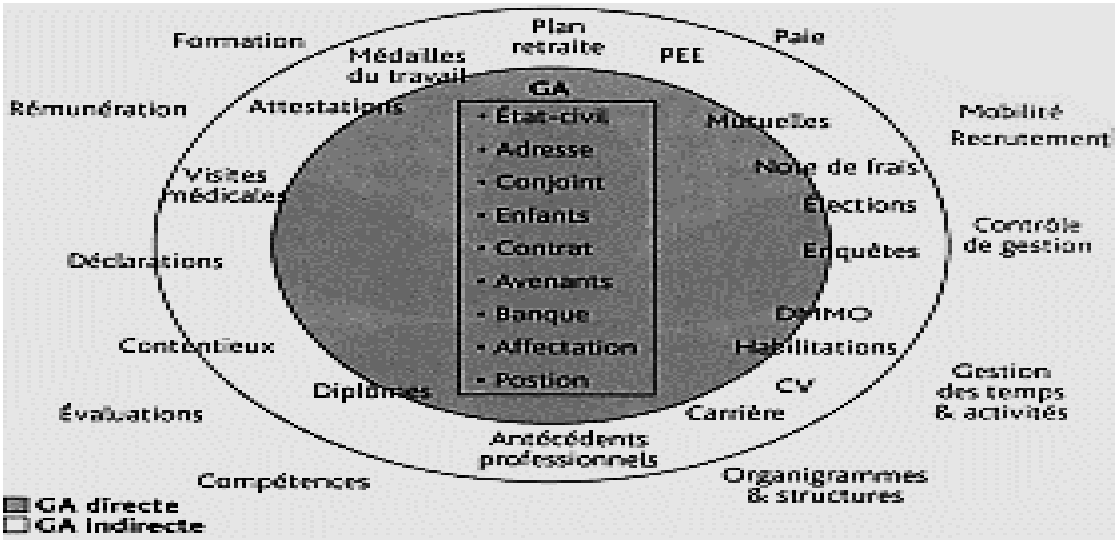


Figure 2: Périmètre de la gestion administrative

Ce processus est globalement essentiellement administratif et ne comporte ni complexité ni technicité particulière.

b) Gestion des temps et activités (GTA)

La GTA est l'un des modules les plus fréquemment présents dans le SIRH, avec la paie et la GA. Le périmètre et la sophistication de ce module dépendent pour beaucoup des besoins de l'entreprise qui l'intègre à son SIRH.

Certaines ont des besoins poussés en matière de planification, de gestion des horaires (cycles, annualisation, etc.) et s'équiperont plutôt d'un outil dédié à la GTA, un Best of Breed[2].

Pour d'autres organisations, la GTA se résume au suivi de la présence et des absences ainsi qu'en la mise à jour en temps réel des compteurs de congés et de réduction de temps de travail. La GTA est alors le prolongement direct de la gestion administrative et ne nécessite rien de plus que le module GTA de base proposé par la majorité des éditeurs de progiciels intégrés.

Quelques fonctionnalités permettent de distinguer l'offre des éditeurs :

- Badgeage
- Saisie déclarative des temps en ligne
- Gestion des congés, absences et RTT
- Gestion de la modulation du temps de travail
- Planification semi-automatique des temps de travail et des activités
- Gestion des intérimaires

c) Paie

La paie est la brique la plus ancienne et la plus mature du SIRH. Elle a longtemps formé le noyau central autour duquel venaient se greffer les autres modules dont la gestion administrative (GA) au premier rang. Ses calculs et ses données alimentent grandement les autres modules, sa justesse et son bon fonctionnement général ont un impact fort sur tout le SIRH.

[2] La possibilité d'intégrer des logiciels de différents éditeurs afin de choisir les solutions les plus adaptées (François Silva, Etre e-DRH)

Ce module doit être actualisé régulièrement pour garantir le respect des normes et procédures qui évoluent constamment en matière de rémunération et de législation sociale.

La paie est le processus RH le plus externalisé, particulièrement dans les pays comme la France, puisque le taux d'outsourcing de la paie y atteint 80%, contre 20% en moyenne à l'échelle européenne.

Quelques fonctionnalités permettent de distinguer l'offre des éditeurs :

- Pays couverts
- Gestion multi sociétés
- Aide légale en ligne ou téléphonique
- Mises à jour gratuites et automatiques selon les évolutions légales et conventionnelles

d) Recrutement / mobilité interne

Le recrutement n'est pas un acte anodin pour l'organisation. Il s'agit d'un investissement avec des conséquences sur le long terme.

La plupart des solutions SaaS[3] orientées « recrutement » sont des outils de niche peu interfacés avec le reste du SIRH. Ils permettent à chaque partie prenante de gérer, en ligne, tout ou partie du processus de recrutement :

- Les recruteurs disposent d'un espace extérieur à l'entreprise où publier leurs offres d'emploi ;
- Les candidats retrouvent les offres d'emploi sur le site de l'entreprise ;
- Chaque candidature passe par une série d'étapes avant d'être soit retenue, soit écartée.

Quelques critères sur lesquels les offres des éditeurs se distinguent :

- Formulaire de candidature en ligne
- Gestion du scoring[4] et du matching[5]
- Gestion de la relation candidat (réponses automatisées, agenda en ligne,…)

[3] Software as a Service ou logiciel en tant que service
[4] Pondération des qualifications recherchées dans les besoins et des compétences disponibles dans un profil
[5]Recherche de l'adéquation entre une qualification recherchée dans un besoin et les compétences d'un profil

- Gestion de la mobilité interne
- Gestion de l'onboarding[6]

e) Formation

Les modules de formation sont arrivés dans les SIRH historiquement à la suite des modules de paie et de GTA.

D'abord peu fournie, l'offre a été développée par les éditeurs sous la pression des utilisateurs. La formation joue un rôle crucial dans l'organisation, celui de garder les qualifications du personnel à jour et alignées sur les besoins pour mettre en œuvre la stratégie de l'entreprise.

Associée à la mobilité interne, elle permet de mettre en place une stratégie d'employabilité tout au long de la vie professionnelle des collaborateurs. Ceci a pour effet de renforcer la motivation des collaborateurs avec la prise en compte de leurs aspirations professionnelles, et de donner d'excellents résultats en matière de fidélisation du personnel.

Quelques critères sur lesquels les offres des éditeurs se distinguent :

- Gestion du plan de formation
- Gestion des entretiens de professionnalisation
- Gestion du catalogue formation
- Plate-forme de formation en ligne (LMS)
- Outil de conception de cours

f) Reporting

Les SIRH agglomèrent une quantité importante d'informations sur le personnel. Pour éviter qu'ils deviennent des « boîtes noires », il est crucial que de tels systèmes soient en mesure de restituer ces données sous la forme de rapports présentant les données dans un format qui ait un sens et une utilisé pour l'utilisateur.

Le reporting SIRH s'adresse à différentes catégories d'acteurs:

[6] Consiste à bien accueillir et intégrer les nouveaux collaborateurs à travers un processus systématique, complet et automatisé

- Fonction RH :
  - Restitutions ponctuelles ;
  - Synthèses ;
  - Rapports obligatoires ;
  - Analyses prévisionnelles ;
  - Tableaux de bord ;
  - Indicateurs de contrôle autour de divers processus.
- Managers :
  - Tableaux de bord de service (effectifs, absentéisme, entrées/sorties) ;
  - Indicateurs sur les collaborateurs (suivi de progression, taux d'entretiens réalisés).
- Collaborateurs :
  - Indicateurs personnels (suivi de carrière) ;
  - Fiches récapitulatives (carrière, formation).
- Contrôleur de gestion sociale :
  - Eléments budgétaires.

Quelques critères sur lesquels les offres des éditeurs se distinguent :

- Simulation de l'évolution de la masse salariale en intégrant l'évolution démographique
- Analyse statistique des indicateurs sociaux (absentéisme, licenciement, démission)
- Analyse statistique des temps et des activités
- Analyse statistique des actions de formation
- Analyse statistique des recrutements

La « Business Intelligence » (BI) va bien au-delà du reporting que l'on retrouve classiquement dans les SIRH. Il s'agit d'analyses prédictives dans une logique d'anticipation du futur permettant de minimiser les risques et d'effectuer, a priori à temps, les changements de cap

g) Gestion prévisionnelle des emplois et compétences (GPEC)

La GPEC est un processus RH dont l'apparition est récente dans le SIRH. Derrière cet acronyme se cachent des enjeux importants pour l'organisation:

- Développer l'employabilité mais aussi la mobilité ;
- Permettre aux seniors de se retirer sans perte de savoirs pour l'entreprise ;
- Assurer le plan de succession ;
- Recruter dans la diversité et fidéliser les meilleurs ;
- Répondre aux exigences opérationnelles en affectant les bonnes compétences, au bon moment et au bon poste ;
- Répondre à des évolutions de métier, des évolutions technologiques.

Une démarche GPEC donne souvent lieu à la mise sur pied de référentiels de compétences ainsi qu'à un dispositif d'évaluation permettant de mesurer les compétences disponibles dans l'organisation par rapport aux compétences requises pour son évolution.

Selon les cas, la durée d'un entretien peut aller de quelques minutes à plusieurs heures et donner lieu à un document se résumant à quelques lignes, mais pouvant aussi comporter plusieurs pages.

Pour B. Just, il est illusoire de penser qu'un SIRH pourra un jour parvenir à exploiter entièrement toute l'information qui émane d'un entretien individuel. Pour cause : « […] la part donnée au verbatim est trop importante »

Le palliatif consiste à mettre sur pied des formulaires standardisés, avec des systèmes de notation encadrés qui rendent en partie automatisable le traitement de ces données.

Quelques critères sur lesquels les offres des éditeurs se distinguent :

- Gestion des entretiens individuels
- Gestion des auto-évaluations
- Gestion du feedback à 360°
- Gestion des plans de successions
- Gestion d'un référentiel des métiers et des compétences
- Cartographie des connaissances et des compétences dans l'organisation

h) Rémunération globale

Une politique de rémunération efficace, c'est-à-dire tenant compte des réalités du marché, permet d'attirer, de motiver et de retenir les talents dans l'organisation. Outre la minimisation du turnover, elle vise par ailleurs à maîtriser la masse salariale et à optimiser les processus RH existants.

Quelques fonctionnalités permettant de distinguer l'offre des éditeurs :

- Gestion de la rémunération variable
- Gestion des augmentations individuelles
- Gestion des avantages sociaux et en nature
- Gestion de l'intéressement et de la participation

Cette section, nous a permis de positionner les SIRH dans le SI d'une organisation ; tout en ressortant les différents processus qui le constituent.

SECTION II. Les Concepts Liés À La Sécurité Des Systèmes D'information

Cette section nous permet de présenter certaines notions liées à la sécurité du système d'information de l'entreprise.

1. Gestion Des Risques De Sécurité Des Systèmes d'information.

Les systèmes d'information dont dépendent fortement l'activité opérationnelle et la fiabilité de l'information comptable et financière, rendent incontournable leur prise en compte dans une démarche sérieuse d'analyse des risques.

HASSID (2008 : 138) définit la gestion des risques comme un processus matriciel itératif de prise de décision et de mise en œuvre des instruments qui permettent de réduire à un niveau acceptable l'impact des vulnérabilités pesant sur toute entité.

Nous pouvons déduire de cette définition que la sécurité d'un SI revient à essayer de se protéger contre les menaces intentionnelles ou non, et d'une manière plus générale contre tous les risques pouvant avoir un impact sur le SI, ou sur des informations qu'il traite. Alors, qu'est-ce qu'un risque ? Comment peut-on garantir une sécurité raisonnable du SIRH ?

a) La notion de risque

La notion de risque est définie par IFACI (in RENARD, 2013 : 137) comme étant « un ensemble d'aléas susceptibles d'avoir des conséquences négatives sur une entité et dont le contrôle interne et l'audit ont notamment pour mission d'assurer autant que faire se peut la maîtrise. » Le risque résulte donc, de tout événement, comportement ou situation susceptible de provoquer un dommage à l'organisation et/ou de l'empêcher de réaliser ses objectifs ou de maximiser ses performances ou encore de saisir une opportunité. On distingue plusieurs types de risques. Ceux liés au SIRH sont qualifiés de risques opérationnels car découlant de l'activité comptable, auxquels l'on associe les risques liés aux moyens mis en œuvre pour produire l'information.

En effet, le risque opérationnel selon Bâle 2 (in JIMENEZ, 2008 : 19) est un risque de perte résultant d'une inadaptation ou d'une défaillance attribuables à des procédures, personnes et systèmes internes ou à des événements externes.

Cette définition recouvre les erreurs humaines, les fraudes et malveillances, les défaillances des systèmes d'information, les problèmes liés à la gestion du personnel, les litiges commerciaux, les accidents, incendies, inondations, etc.

Se référant à la sécurité des systèmes d'information, le risque serait la possibilité qu'une menace donnée exploite une ou plusieurs vulnérabilités d'un actif ou d'un groupe d'actif et cause ainsi un préjudice à l'organisation (ISACA, 2013 : 74). Cette dernière définition est celle qui retiendra notre attention dans la suite de cette étude. Alors qu'est-ce qu'une vulnérabilité ? Une menace ?

i. La vulnérabilité

La vulnérabilité est considérée par CARPENTIER (2009 : 31) comme une faiblesse des procédures de sécurité techniques et physiques ou encore d'une absence de protection qui peuvent être exploités par une menace.

Cette définition se limite aux mesures de sécurité alors qu'un actif informationnel peut présenter des faiblesses intrinsèques. En effet, ISO/CEI 27000 (in CLUSIF, 2010 : 5) donne une définition plus complète en ces termes : « la vulnérabilité est une faille dans un actif ou mesure de sécurité qui peut être exploitée par une ou plusieurs menaces ».

La réalisation du risque se manifeste donc par l'exploitation d'une ou des vulnérabilités par une ou plusieurs menaces.

ii. La menace

La notion de menace est, selon PILLOU & al. (2011 : 33), toute action susceptible de nuire dans l'absolu.

En d'autres termes, il s'agit de tout évènement dont la survenance est susceptible de compromettre l'atteinte des objectifs. On distingue les menaces à caractère non intentionnel qui peuvent globalement se scinder en deux catégories notamment les accidents (inondation, incendie etc.) et les erreurs et les menaces à caractère intentionnel (vol de données, modification ou altération des données, déni de service, émission de programme malveillant) qui sont essentiellement dues à de la malveillance qui peuvent être d'origine interne ou externe.

Les facteurs « probabilité » et « impact » caractérisent le risque et déterminent sa criticité. Le risque est susceptible de se produire et d'avoir un impact négatif sur la réalisation des objectifs. La gestion des risques est donc d'une très grande importance pour assurer la continuité des activités de l'entreprise.

b) Identification des risques de sécurité des systèmes d'information

Cette phase est la plus importante dans le processus de gestion des risques. Elle a pour but selon MENTHONNEX (1995 : 119), d'aider à connaître et à analyser les événements pouvant être à l'origine de la non-réalisation des objectifs poursuivis notamment par le SIRH.

Même s'il est difficile, voire impossible d'identifier de façon exhaustive tous les risques auxquels serait exposé le SIRH, il s'agira tout au moins, d'identifier ceux susceptibles de compromettre la continuité des activités.

Selon BERRADA (2012 : 70), identifier un risque ou un objet de risque revient à recenser l'ensemble des ressources dont l'entreprise a besoin pour fonctionner et à les rapprocher de tous les événements aléatoires, à localiser leur source.

En effet, un risque non identifié ne pourra jamais être traité. Plusieurs approches permettent d'identifier les risques. En se référant à JIMENEZ & al. (2008 : 63), nous pouvons noter à titre d'exemple les approches « brainstorming », « Top down », « Botton-up », etc.

c) Évaluation des risques de SSI

L'évaluation des risques est selon LINLAUD (2003 : 43), le préalable indispensable à l'élaboration du système de gestion de la sécurité de l'information.

L'objectif est d'obtenir, pour chaque risque identifié, une évaluation du niveau auquel l'organisation serait exposée. Ce niveau dépend de deux facteurs que sont l'impact et la potentialité (ou probabilité) du risque. CORDEL (2013 : 19) illustre le risque par la formule suivante : Risque = Probabilité d'occurrence × Impact.

BLOCH & al. (2011 : 252) expriment l'impact comme étant le produit d'une ou des menaces et d'une ou des vulnérabilités.

En d'autres termes, les menaces exploitent les vulnérabilités pour provoquer un dommage ou la perte d'un actif informationnel. Nous pouvons en déduire par transitivité que :

Risque = Probabilité d'occurrence × Menace × Vulnérabilité.

Dans un contexte où des mesures de sécurité ont déjà été prises, il faudra en outre tenir compte de la qualité de ces mesures ou de leur maturité. Alors le risque sera selon l'expression suivante :

$$Risque = \frac{Probabilité\ d'occurence * Menace * Vulnérabilité}{Contre-mesures}$$

Selon PINET (2012 : 47-48), l'impact (produit de la menace et de la vulnérabilité) et la probabilité d'apparition d'un risque s'évaluent à travers la définition d'une échelle faisant apparaître des différents niveaux d'appréciation. Le niveau des impacts doit être apprécié pour chacun des trois facteurs : disponibilité, intégrité et confidentialité des actifs sélectionnés.

La probabilité, selon CORDEL (2013 : 143) est déterminée soit par extrapolation (utilisation des données historiques disponibles et fiables), soit par prédilection (lorsque les données ne sont pas disponibles) ou en faisant le recours structuré aux experts.

Par ailleurs, les contre-mesures s'apprécient selon leur capacité à réduire l'impact et ou la probabilité d'un ou de plusieurs risques.

Une fois l'évaluation faite, une hiérarchisation consistant à attribuer une priorité aux différents risques identifiés et évalués est nécessaire. L'identification, l'évaluation et la hiérarchisation des risques, permettront d'établir la matrice des risques qui, pour reprendre HASSID (2008 : 139) est une forme de mesure et de priorisation des risques en une seule étape afin de déterminer le niveau de danger particulier, à l'aide des critères objectifs de probabilité et de gravité.

Nous notons qu'elle constitue, un outil d'aide à la prise de décision dans la gestion des risques en ce sens qu'un traitement approprié est réservé à chaque risque conformément à l'appétence aux risques de l'organisation. La figure 8 montre un exemple de matrice de risques.

Tableau 2: Matrice des risques (cotation des risques en termes de gravité et de probabilité)

Gravité	4- Très grave				
	3- Grave				
	2- Moyenne				
	1- Faible				
		1- Improbable	2-Peu probable	3- probable	4- Fréquent
	Probabilité				

Source : Nous-mêmes

Légende

Risques nécessitant un traitement obligatoire

Risques modérés

Risques à impact minimal

Toutefois, les différents niveaux d'appréciation des risques restent relatifs. Les finalités de cette matrice sont : de définir les risques les plus importants à maîtriser et de permettre de se baser sur un schéma commun pouvant aider à identifier et coter les risques.

d) Traitements des risques de sécurité du SI

Le traitement des risques de SSI consiste à trouver une réponse à chacun des risques identifiés, évalués et hiérarchisés. En d'autres termes il s'agit de prendre les mesures appropriées pour les ramener à un niveau acceptable ou de les rendre plus supportables pour l'organisation. Selon la norme ISO 27002 (2005 : 5), on distingue quatre manières de gérer le risque, par ordre croissant de coût : l'acceptation, l'évitement, le transfert ou le partage et la réduction.

i. L'acceptation du risque

Elle consiste, selon COSO II (in CORDEL, 2013 : 153), à « ne prendre aucune mesure susceptible de modifier la probabilité d'occurrence d'un risque et ou son impact ». Elle peut être justifiée si une réalisation du risque n'aura pas d'impact significatif sur l'entreprise c'est-à-dire si le risque est déjà en-dessous du seuil de tolérance de l'entreprise.

ii. L'évitement du risque

Selon KEREBEL (2009 : 65), éviter un risque consiste à renoncer par exemple à lancer une nouvelle activité ou à supprimer une activité existante, source de ce risque.

iii. La réduction du risque

Réduire le risque consiste à prendre des mesures afin de réduire la probabilité d'occurrence ou l'impact du risque, ou les deux à la fois ; ce qui implique tout un ensemble de décisions opérationnelles courantes (PwC[7] & al, 2014 : 127).

L'objectif est donc, de définir des mesures techniques et organisationnelles pour ramener le risque à un niveau acceptable. C'est le traitement le plus courant.

iv. Le transfert du risque

Selon WITHMAN (2011 : 147), le transfert d'un risque consiste à sous-traiter l'activité, source de risque ou en souscrivant à une assurance.

C'est une stratégie qui est donc nécessaire lorsque l'entreprise n'est pas en mesure de mettre en place des dispositifs de sécurité qui permettraient de réduire le risque. On parle aussi

[7] PricewaterhouseCoopers

du partage du risque si elle décide d'externaliser une partie ou l'ensemble de l'activité qui présente des risques.

Chacun de ces traitements a un coût ; et pour être rationnel l'entreprise doit veiller à ce que ce coût ne dépasse pas l'impact d'une survenance du risque. Il serait donc nécessaire de procéder à un arbitrage entre le coût du traitement du risque et l'impact de la survenance dudit risque.

La gestion des risques du SIRH, a donc pour finalité la sécurité de ce dernier afin de mettre en confiance les destinataires de l'information des ressources humaine.

2. Notion de sécurité du système d'information

La sécurité du SIRH constitue un domaine depuis et encore plus de nos jours déterminant pour la survie de l'entreprise. Pour que la gouvernance des SI atteigne ses objectifs, il est indispensable de tenir compte de la sécurité du système d'information des ressources humaines.

a) Définition de la notion de sécurité du système d'information

Nombreuses sont les définitions données à la notion de sécurité du système d'information. Nous portons notre attention sur quelques-unes susceptibles de nous aider à la comprendre.

Pour reprendre MENTHONNEX (1995 : 74), la sécurité d'un SI est un ensemble de moyens techniques ou non, de protection, permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des équipements et/ou des données traitées ou transmises et des services connexes offerts ou rendus accessibles par le système.

Selon la norme ISO 27002 (2005 : 14), la sécurité de l'information est l'état de protection face aux risques identifiés et résultant de l'ensemble des mesures de sécurité prises par une entreprise pour préserver : la confidentialité, l'intégrité et la disponibilité de l'information que détient l'entreprise, quel que soit le support (papier, électronique, etc.).

Ces deux définitions identifient clairement les principaux critères de sécurité à prendre en compte dans la gouvernance de la sécurité des SI tout en proposant les moyens à mettre en œuvre afin d'atteindre les objectifs de sécurité que nous aborderons plus loin.

b) La gouvernance de la sécurité du SIRH

Selon ITGI[8] (in WHITMAN & al, 2011 : 176), la gouvernance de la sécurité de l'information comprend toutes les responsabilités et les méthodes prises par la haute direction afin de fournir des orientations stratégiques pour la définition des objectifs de sécurité.

Elle est donc une activité continuelle qui doit tenir compte des besoins de l'organisation, tout en assurant son alignement par rapport aux objectifs généraux. En outre, il s'agit de mobiliser un ensemble de mesures de sécurité organisationnelles, procédurales et techniques, sans toutefois négliger l'importance de l'adhésion du personnel de l'organisation afin de s'assurer de la continuité des services et de la protection des actifs informationnels.

c) Les critères de sécurité

Selon FEVRIER (2013 : 29), le niveau de sécurité d'un SI peut s'interpréter comme sa capacité à demeurer inaccessible à l'ensemble des risques auxquels il est exposé, que ce soit en termes de contenant (structure) ou de contenu (données).

Pour connaître ce niveau de sécurité il faut pouvoir l'évaluer par des indicateurs. Ces derniers constituent les exigences fondamentales en matière de sécurité des SI. Ils caractérisent ceux à quoi s'attendent les utilisateurs vis-à-vis du SI.

Ainsi, selon LAFITTE (2003 : 31), LINLAUD (2011 : 11) et GHERNAOUTI (2013 : 1), la sécurité des systèmes d'information repose principalement sur trois critères que sont la Disponibilité (D), l'Intégrité (I), et la Confidentialité (C) décrits comme suit :

- La disponibilité

Elle garantit que les éléments considérés sont accessibles autant que besoin aux personnes autorisées. En d'autres termes, elle conditionne le fait que le système puisse fonctionner sans défaillance, durant les plages d'utilisation prévues, garantit l'accès aux services et ressources installées avec le temps de réponse attendu.

[8] Information Technology Governance Institute

- l'intégrité

La norme ISO/CEI 27002 définit l'intégrité comme la propriété de protection de l'exactitude et de l'exhaustivité des actifs informationnels.

Selon PINET (2012 : 44), l'intégrité d'un équipement, d'un système ou des données est obtenue lorsque ceux-ci ne subissent aucune altération ou destruction accidentelle ou volontaire.

- La confidentialité

Elle est la propriété qu'une information ne soit disponible, divulguée qu'aux personnes, entités ou processus autorisés. C'est également la garantie qu'une information n'est connue que de ceux qui sont habilités à en disposer (ANDRESS, 2014 : 6).

A ces trois critères primitifs et essentiels de la sécurité dits « critères DIC », nous pouvons également considérer selon ISO 27002 (2005 : 2) d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation, etc.

Il reviendra aux responsables de chaque entité de les hiérarchisés par rapport aux objectifs de sécurité. La figure 3 ci-après résume les critères et fonctions permettant de mesurer le niveau de sécurité du SI d'une organisation.

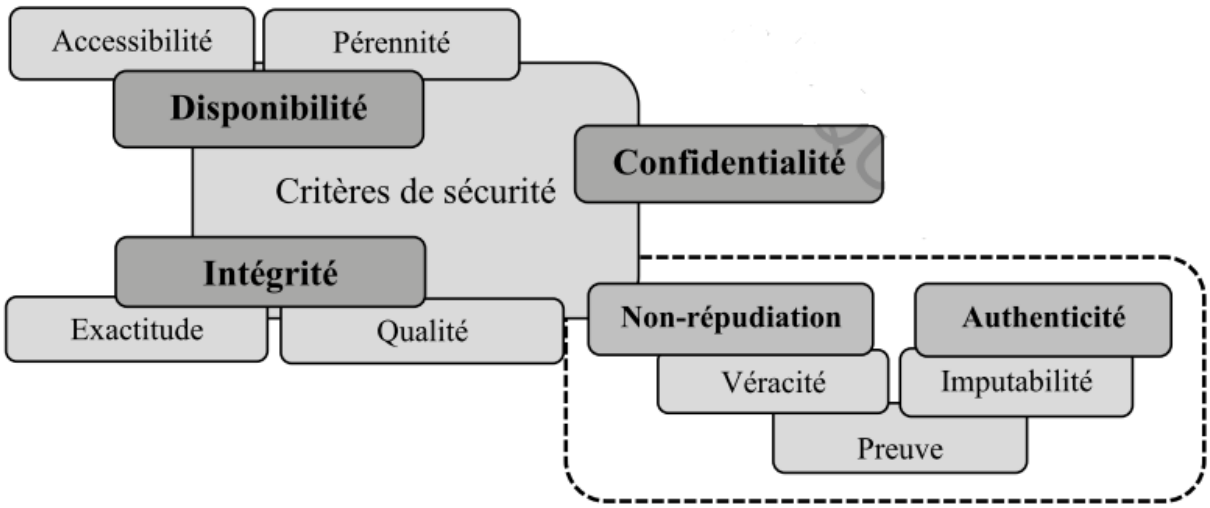


Figure 3: Critère de sécurité selon GHERNAOUTI

Nous pouvons retenir qu'un système d'information ou une application, pour être considéré comme « sécurisé », doit au minimum disposer les qualités suivantes :

- empêcher les accès et la consultation de données aux personnes non autorisées ;
- conserver et restituer les données dans l'état où elles ont été saisies ;
- fournir les données ou services requis lorsque les utilisateurs autorisés en ont besoin ;
- identifier et authentifier les utilisateurs sur le système d'information ;
- permettre de retracer chaque opération.

Cette section nous a permis de présenter quelques notions liées à la sécurité du système d'information des ressources humaines.

SECTION III. Les Concepts De L'audit Des SIRH

L'objectif de cette section est de présenter les concepts d'audit des systèmes d'information, afin de cerner le champ de notre étude.

1. Qu'est-ce qu'un audit ?

Un **audit** est un examen ou contrôle de la gestion et des conditions de fonctionnement d'une entreprise ou de l'un de ses services.

Un **audit** est une expertise professionnelle effectuée par un agent compétent et impartial aboutissant à un jugement par rapport à une norme sur les états financiers, le contrôle interne, l'organisation, la procédure, ou une opération quelconque d'une entité.

2. Pourquoi l'audit des systèmes d'information ?

Le site web Wikipédia définit l'**audit des systèmes d'information à travers l'audit informatique** (en anglais *Information Technology Audit* ou *IT Audit*). Il a pour objectif d'identifier et d'évaluer les risques (opérationnels, financiers, de réputation notamment) associés aux activités informatiques d'une entreprise ou d'une administration.

La loi n°2010/012 du 21 décembre 2010 relative à la Cybersécurité et à la Cybercriminalité au Cameroun définit l'audit spécifiquement l'audit de sécurité comme un examen méthodique des composantes et des acteurs de la sécurité, de la politique, des mesures,

des solutions, des procédures et des moyens mis en œuvre par une organisation, pour sécuriser son environnement et effectuer des contrôles de conformité de son système d'information.

On déduit donc de ces explications que, l'objectif principal de l'audit des systèmes d'information des ressources humaines est de garantir la conformité de celui-ci.

3. Les types d'audit

Pour mieux cerner la portée d'une mission d'audit, il est nécessaire de présenter les grands types d'audit :

a) L'audit interne ou "de première partie"

L'audit interne est demandé par l'entreprise elle-même : elle en est le commanditaire. Il s'agit de vérifier un certain nombre de points que l'entreprise elle-même fixe. Elle est absolument libre dans ses choix : points à vérifier, manière de les vérifier, qui va vérifier etc.

Le simple bon sens fait que l'entreprise ne va pas demander à celui qui a réalisé quelque chose d'aller auditer ce quelque chose... afin d'éviter les situations de juge et partie. L'entreprise peut très bien pour ces audits internes mandater un auditeur externe à l'entreprise.

Un audit interne se conclut sur un rapport avec description de constats et suivant des préconisations diverses. Ce rapport reste a priori interne à l'entreprise.

Dans nos métiers, ce type d'audit se focalisera sur la vérification de la bonne mise en place de plans de continuité ou de système de management de la continuité ou sécurité

b) L'audit externe de "seconde partie"

Nous sommes ici dans une autre situation, car l'audit est demandé par une partie prenante comme un client par exemple. Le "commanditaire" est donc externe et dispose de relations avec votre entreprise (en tant que client le plus souvent, voire prospect qui veut vérifier quelque chose avant de signer).

Ce client demande à un auditeur (de chez lui ou d'ailleurs, ce point est peu important) de faire un audit chez vous. Là encore l'audit va consister à faire des constats par rapport à un sujet que le commanditaire veut faire vérifier.

Dans nos métiers, on verra souvent un audit de ce type pour vérifier que l'entreprise respecte bien les règles qu'elle s'est fixées ou qu'elle assure respecter, dans le domaine de la sécurité ou continuité par exemple.

Ce type d'audit se termine par un rapport qui est la propriété du commanditaire (donc du client ou prospect dans cet exemple).

Il est assez courant que ce type d'audit soit prévu sur rythme annuel dans les contrats de service par exemple. Le client n'exercera pas forcément chaque année ce "droit à l'audit" de son fournisseur. Il le fera en revanche avant la fin du contrat de service pour décider s'il continue par exemple.

c) L'audit de "tierce partie"

Cette fois ci le commanditaire de l'audit n'est ni vous, ni un client mais une entité neutre externe. Cela peut être une autorité de tutelle, un organisme de contrôle, un certificateur...

L'audit va vérifier la conformité de quelque chose par rapport à une référence. Dans nos métiers cela peut être la conformité d'un système de management de la sécurité (ou continuité) par rapport à une norme ISO (27001 ou 22301) typiquement.

Le rapport, propriété de l'entité certificatrice, va pointer les écarts (ou "non-conformités") en les classant souvent par importance (remarque / mineur / majeur). Il ne comporte a priori pas de recommandations, sauf du type "je recommande à la certification".

En tenant compte de ce rapport et d'autres aspects réglementaires éventuels, le commanditaire décidera s'il accorde ou non un certificat de "conformité au référentiel XXX" à votre société. Il faut ici noter que si le référentiel demande qu'il y ait des audits internes, l'auditeur de certification ira vérifier qu'il y a bien eu des audits internes menés conformément aux exigences du référentiel. On voit bien là que les rôles sont très différents entre les différents audits.

4. Approche thématique de l'audit des systèmes d'information RH

L'audit des SI peut soit constituer un sous-domaine d'un audit généraliste (organisation, processus, régularité, etc.), soit être l'objet principal de la mission (application, projet, sécurité, respect de la législation, etc.)

Tableau 3: Approche thématique des audits SI

Thème audit SI	Description
Audit de la fonction informatique	Le but de l'audit de la fonction informatique est de répondre aux préoccupations de la direction générale ou de la direction informatique concernant l'organisation de la fonction informatique, son pilotage, son positionnement dans la structure, ses relations avec les utilisateurs, ses méthodes de travail…
Audit des études informatiques	L'audit des études informatiques est un sous-ensemble de l'audit de la fonction informatique. Le but de cet audit est de s'assurer que son organisation et sa structure sont efficaces, que son pilotage est adapté, que ses différentes activités sont maîtrisées, que ses relations avec les utilisateurs se déroulent normalement,…
Audit de l'exploitation	L'audit de l'exploitation a pour but de s'assurer que le ou les différents centres de production informatiques fonctionnent de manière efficace et qu'ils sont correctement gérés. Il est pour cela nécessaire de mettre en œuvre des outils de suivi de la production comme Openview d'HP, de Tivoli d'IBM,…
Audit des projets informatiques	L'audit des projets informatiques est un audit dont le but est de s'assurer qu'il se déroule normalement et que l'enchaînement des opérations se fait de manière logique et efficace de façon qu'on ait de fortes chances d'arriver à la fin de la phase de développement à une application qui sera performante et opérationnelle. Comme on le voit

	un audit d'un projet informatique ne se confond pas avec un audit des études informatiques.
Audit des applications opérationnelles	Les audits précédents sont des audits informatiques, alors que l'audit d'applications opérationnelles couvre un domaine plus large et s'intéresse au système d'information de l'entreprise. Ce sont des audits du système d'information. Ce peut être l'audit de l'application comptable, de la paie, de la facturation,…. Mais, de plus en plus souvent, on s'intéresse à l'audit d'un processus global de l'entreprise comme les ventes, la production, les achats, la logistique,…
Audit de la sécurité informatique	L'audit de la sécurité informatique a pour but de donner au management une assurance raisonnable du niveau de risque de l'entreprise lié à des défauts de sécurité informatique. En effet, l'observation montre que l'informatique représente souvent un niveau élevé de risque pour l'entreprise. On constate actuellement une augmentation de ces risques liée au développement d'Internet

Source : Nous-mêmes

5. Les acteurs de l'audit

L'audit met en œuvre différents acteurs aux rôles bien déterminés :

- **Le Commanditaire de l'audit** : c'est lui qui décide de l'audit, de son objectif, du contexte. C'est généralement la direction de l'entreprise, ou un client, ou un organisme officiel (état, organisme de certification...)
- **La Direction de l'audité** : c'est généralement le DSI ou la direction de l'organisme. C'est lui qui facilite l'organisation de l'audit et met en relation les auditeurs et les audités.
- **Les audités** : ce sont les personnes de la DSI (ou autres services internes à l'entreprise) qui vont apporter les éléments de réponse aux auditeurs
- **L'équipe d'audit** (un ou plusieurs auditeurs) : elle collecte les observations permettant de fournir les conclusions (rapports d'audit).
- **Les experts techniques** : mobilisés par l'équipe d'audit ponctuellement et sous son contrôle pour analyser un point spécifique

Si l'équipe d'audit est composée de plusieurs auditeurs, chaque auditeur a un rôle déterminé d'un commun accord dans un souci premier d'efficience (maîtrise des différents thèmes de l'audit, proximité géographique, disponibilité, niveau d'expérience requis...).

Cette section nous familiarise avec les concepts d'audit et particulièrement l'audit des systèmes d'information.

6. La Démarche d'Audit des Systèmes d'Information des RH

Le guide méthodologique pour l'audibilité des systèmes d'information pour Fiabilisation et certification des comptes des établissements publics de santé (Direction Générale de l'Offre Santé, 2013) définit la démarche classique d'audit en grandes étapes :

a) Planification de la mission

Cette étape comporte notamment l'approche générale des travaux, le niveau de supervision, les ressources nécessaires pour la réalisation de la mission, les besoins d'intervenants externes et d'autres professionnels

b) Prise de connaissance de la cible et de son environnement

Cette étape vise à recueillir les éléments relatifs au secteur d'activité, aux caractéristiques de la cible, aux indicateurs de performances financières, aux éléments de contrôle pertinents pour l'audit.

c) Evaluation du risque d'anomalies significatives

Cette étape consiste à apprécier l'efficacité du contrôle interne à détecter ou corriger des anomalies significatives dans le système.

d) Procédures d'audit mises en œuvre à l'issue de l'évaluation des risques

Les procédures d'audits comprennent les tests de procédures et les contrôles de subsistance. Dans cette étape, le certificateur détermine l'étendu et le calendrier de la mise en œuvre de ces procédures au regard des risques d'anomalies significatives identifiées.

SECTION IV. Normes, Référentiels, Méthodes Et Outils Pour L'audit Des Systèmes D'information Des Ressources Humaines.

Les outils pour l'audit des systèmes d'information sont nombreux et variés et de ce fait, il est important, d'avoir connaissance de ceux-ci afin de disposer des meilleurs pour pouvoir résoudre un problème. On distingue principalement les lois nationales, les normes internationales, les référentiels de bonnes pratiques ; ainsi que les standards.

1. La réglementation en matière d'audit des systèmes d'information au Cameroun

Depuis le 8 Avril 2002, le chef de l'Etat, par décret n°2002/092 du 08 avril 2002, a créé l'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC) et lui a assigné la mission globale de promotion et de suivi de l'action des pouvoirs publics dans le domaine des TIC. En pour la réalisation de sa mission, le cadre juridique en matière d'audit des systèmes d'information s'intéresse particulièrement à l'audit de sécurité d'un système d'information. Ainsi, l'activité d'audit de sécurité est régie par les textes ci-après :

- Loi N°2010/012 relative à la cybersécurité et à la cybercriminalité au Cameroun qui fixe le cadre légal de l'activité d'audit de sécurité en ses articles 7, 13, 14, 32 et 61 ;
- Décret N°2012/1643/PM du 14 juin 2012 fixant les conditions et les modalités d'audit obligatoire des réseaux de communications électroniques et des systèmes d'information ;
- Arrêté conjoint N°00000013/MINPOSTEL/MINFI du 10 mai 2013 fixant les montants et les modalités de paiement des frais perçus par l'ANTIC ;
- Décision N°00000094/MINPOSTEL du 30 mai 2013 fixant les frais d'audit de sécurité des réseaux de communications électroniques et des systèmes d'information ;
- Décision N°00000122/MINPOSTEL du 27 juin 2013 fixant les modalités d'organisation et de fonctionnement de la Commission chargée d'émettre des avis sur les demandes d'agrément pour l'exercice de l'activité d'expert auditeur dans le domaine de la sécurité des réseaux de communications électroniques et des systèmes d'information.

2. Les normes d'audit SI

Selon l'organisation internationale de normalisation (en anglais International Organization for Standardization) ISO, une norme est un document établi par consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des

règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats garantissant un niveau d'ordre optimal dans un contexte donné. Nous allons présenter en premier lieu les normes nationales qui régissent l'audit des systèmes d'information ; et en second lieu les normes internationales.

a) Les normes de l'audit des systèmes d'information au Cameroun

Au Cameroun, l'Agence des Normes et de la qualité (ANOR) est l'organisme chargé de définir les directives permettant aux uns et autres de garantir un niveau de qualité dans leurs activités. Le tableau ci-dessous est tiré du catalogue des normes Camerounaise de l'ANOR.

Tableau 4: Normes Camerounaises régissant l'audit

N°	Code Normatif Camerounais	Année et Comité Technique	Code ICS	Intitulé	Référence Norme Internationale
525	NC 524:2014 ISO/IEC 17021:2011	2014-CT 40	03.120.20	Evaluation de la conformité – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management	ISO/IEC 17021:2011
860	NC 859 :2014	2013-CT 40	03.120.230	Évaluation de la conformité -- Exigences et recommandations pour le contenu d'un rapport d'audit tierce partie de systèmes de management	ISO/IEC TS 17022:2012
861	NC 860 :2014	2013-CT 40	03.120.30	Évaluation de la conformité --Lignes directrices pour la détermination de la durée des audits de certification d'un système de management	ISO/IEC TS 17023:2013
920	NC 919 :2014	2013-CT 40	35.040	Technologies de l'information -- Techniques de sécurité --Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information	ISO/IEC 27006:2011
921	NC 920 :2014	2013-CT 40	35.040	Technologies de l'information -- Techniques de sécurité --Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information	ISO/IEC 27007:2011
922	NC 921 :2014	2013-CT 40	35.040	Technologies de l'information -- Techniques de sécurité --Lignes directrices pour les auditeurs des contrôles de sécurité de l'information	ISO/IEC TR 27008:2011
439	NC 438 : 2014 ISO/TS 22003:2013	2014-CT 49	67.020	Systèmes de management de la sécurité des denrées alimentaires – Exigences pour les organismes procédant à l'audit et à la certification de systèmes de management de la sécurité des denrées alimentaires	ISO/TS 22003:2013

Source : ANOR

Conseil pour l'interprétation du tableau

- Identifiant de la norme (Code Normatif)

L'identifiant est le code principal de la norme camerounaise. La structure du code est composée de chiffres séparés par deux points ; les deux, trois ou quatre premiers chiffres correspondent au numéro d'ordre de la norme. Les quatre chiffres suivants, correspondent à l'année d'adoption de la norme.

- Comité Technique d'élaboration de la norme

Les normes sont élaborées au sein des Comités Techniques. Cette colonne indique l'année d'élaboration de la norme, suivie du code d'identification du Comité Technique.

- Le code ICS

Il désigne la classe attribuée aux différents domaines de normalisation. Le code ICS est constitué par le code du domaine suivi d'un point, d'un nombre à trois chiffres pour l'identification du groupe, suivi éventuellement d'un point et d'un numéro d'identification du sous-groupe de normes.

- Intitulé de la norme

Il représente la dénomination de la norme telle qu'attribuée par le comité technique.

b) Les normes internationales

Au niveau internationale, le principal organisme chargé de réguler les normes est l'ISO. En matière d'audit des systèmes d'information, nous avons:

- ISO 19011:2011

Lignes directrices pour l'audit des systèmes de management

L'ISO 19011:2011 fournit des lignes directrices sur l'audit de systèmes de management, comprenant les principes de l'audit, le management d'un programme d'audit et la réalisation d'audits de systèmes de management. Elle donne également des lignes directrices sur l'évaluation de la compétence des personnes impliquées dans le processus d'audit, y compris le ou la responsable du management du programme d'audit, les auditeurs et les équipes d'audit.

L'ISO 19011:2011 est applicable à tous les organismes qui doivent réaliser des audits internes ou externes de systèmes de management ou manager un programme d'audit.

L'ISO 19011:2011 peut, en principe, s'appliquer à d'autres types d'audits, à condition toutefois d'accorder une attention toute particulière aux compétences spécifiques requises.

- ISO/IEC 27002:2013

Technologies de l'information -- Techniques de sécurité -- Code de bonne pratique pour le management de la sécurité de l'information

L'ISO 27002:2013 donne des lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information, incluant la sélection, la mise en œuvre et la gestion de mesures de sécurité prenant en compte le ou les environnement(s) de risques de sécurité de l'information de l'organisation.

L'ISO 27002:2013 est élaborée à l'intention des organisations désireuses de sélectionner les mesures nécessaires dans le cadre du processus de mise en œuvre d'un système de management de la sécurité de l'information (SMSI) selon l'ISO/CEI 27001; de mettre en œuvre des mesures de sécurité de l'information largement reconnues; et d'élaborer leurs propres lignes directrices de management de la sécurité de l'information.

- ISO/IEC 27006:2015

Technologies de l'information -- Techniques de sécurité -- Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

- ISO/IEC 27007:2017

Technologies de l'information -- Techniques de sécurité -- Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information

- ISO/IEC TR 27008:2011

Technologies de l'information -- Techniques de sécurité -- Lignes directrices pour les auditeurs des contrôles de sécurité de l'information

3. Les Référentiels de bonnes pratiques.

Il existe de nombreux référentiels de bonnes pratiques, notamment ceux fournit par ISACA (Information System Audit and Control Association) et IIA (The Institute of Internal Auditors).

- **Control Objectives for Information and related Technology (CObIT)**

CObIT (Control Objectives for Information and related Technology, en français Objectifs de contrôle de l'Information et des Technologies Associées) développé en 1994 (et publié en 1996) par l'ISACA est un outil fédérateur qui permet d'instaurer un langage commun pour parler de la gouvernance des systèmes d'information tout en tentant d'intégrer d'autres référentiels tels que ISO 9000, ITIL, etc.

La version 5 de CObIT est disponible depuis avril 2012. CObIT 5 est, à ce jour, le seul référentiel qui est orienté business pour la Gouvernance et la Gestion des Systèmes d'Information de l'entreprise. Il représente une évolution majeure du référentiel. CObIT 5 peut être adapté pour tous les types de modèles business, d'environnements technologiques, toutes les industries, les lieux géographiques et les cultures d'entreprise. Il peut s'appliquer à :

- La sécurité de l'information
- La gestion des risques
- La gouvernance et la gestion du Système d'Information de l'entreprise
- Les activités d'audit
- La conformité avec la législation et la réglementation
- Les opérations financières ou les rapports sur la responsabilité sociale de l'entreprise

CObIT fournit aux gestionnaires, auditeurs et utilisateurs de TIC (Technologies de l'information et de la communication), des indicateurs, des processus et des bonnes pratiques pour les aider à maximiser les avantages issus du recours à des techniques informatiques et à l'élaboration de la gouvernance et du contrôle d'une entreprise

Le référentiel CObIT 5 simplifie les défis de la gouvernance avec seulement 5 principes et sept facilitateurs. Il permet l'intégration avec d'autres approches et normes, incluant TOGAF[9], PMBOK[10], Prince2[11], ISO 20000, ISO 27001, ITIL[12],…

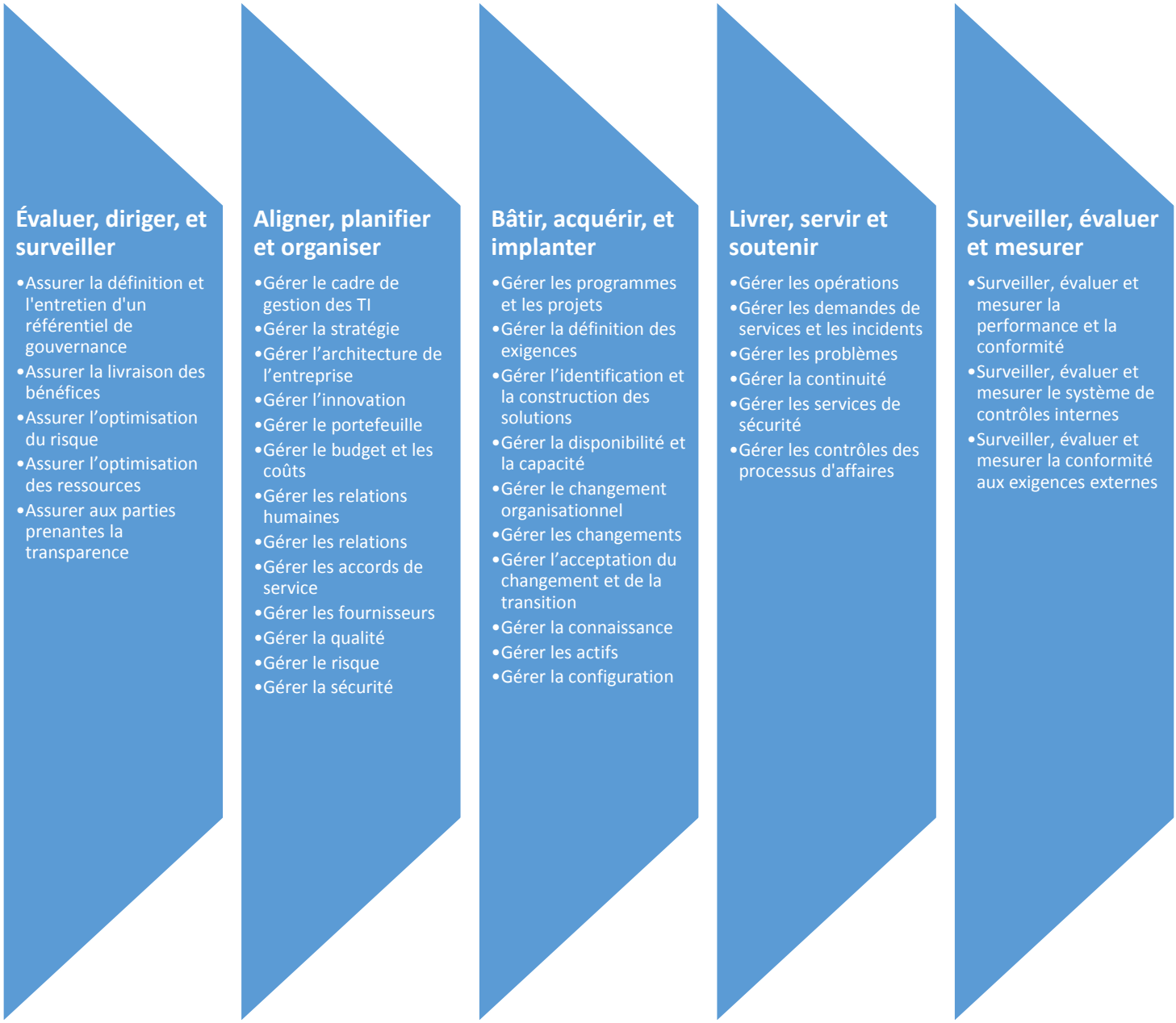


Figure 4: Fondamentaux de CObIT 5

[9] The Open Group Architecture Framework
[10] Project Management Body of Knowledge
[11] Projects In Controlled Environments
[12] Information Technology Infrastructure Library

- **Global Technology Audit Guides (GTAG)**

Les Global Technology Audit Guides (GTAG) sont des bonnes pratiques pour l'évaluation des risques liées aux technologies de l'information. En date du 06 décembre 2017 12 chapitres sont présenté comme traduite en français par l'Institut français des auditeurs et contrôleurs internes (IFACI : qui est le chapitre français de l'Institute of Internal Auditors (IIA)) :

- ☞ GTAG 1 : Les contrôles des systèmes de l'information
- ☞ GTAG 2 : Contrôles de la gestion du changement et des patchs : un facteur clé de la réussite pour toute organisation
- ☞ GTAG 3 : Audit continu : répercussions sur l'assurance, le pilotage et l'évaluation des risques
- ☞ GTAG 4 : Management de l'audit des systèmes d'information
- ☞ GTAG 5 : Le management et l'audit des risques d'atteinte à la vie privée
- ☞ GTAG 6 : Gérer et auditer les vulnérabilités des technologies de
- ☞ GTAG 7 : L'infogérance
- ☞ GTAG 8 : Audit des contrôles applicatifs
- ☞ GTAG 9: Gestion des identités et des accès
- ☞ GTAG 10: Gestion de la continuité des opérations
- ☞ GTAG 11: Développer le plan d'audit informatique
- ☞ GTAG 12: Audit des projets informatiques

4. Les Méthodes d'audit du SIRH

Les principales méthodes d'audit s'orientent plus vers l'analyse de risques de sécurité informatique. Ainsi nous pouvons retenir :

- EBIOS (Expression des besoins et identification des objectifs de sécurité)

La méthode EBIOS est une méthode d'évaluation des risques en informatique, développée en 1995 par la Direction centrale de la sécurité des systèmes d'information (DCSSI) Française et maintenue par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui lui a succédé en 2009.

Elle permet d'apprécier les risques Sécurité des systèmes d'information (entités et vulnérabilités, méthodes d'attaques et éléments menaçants, éléments essentiels et besoins de sécurité...), de contribuer à leur traitement en spécifiant les exigences de sécurité à mettre en place, de préparer l'ensemble du dossier de sécurité nécessaire à l'acceptation des risques et de

fournir les éléments utiles à la communication relative aux risques. Elle est compatible avec les normes ISO 13335 (GMITS), ISO 15408 (critères communs) et ISO 17799 ; et dispose également d'un logiciel pour son implémentation[13].

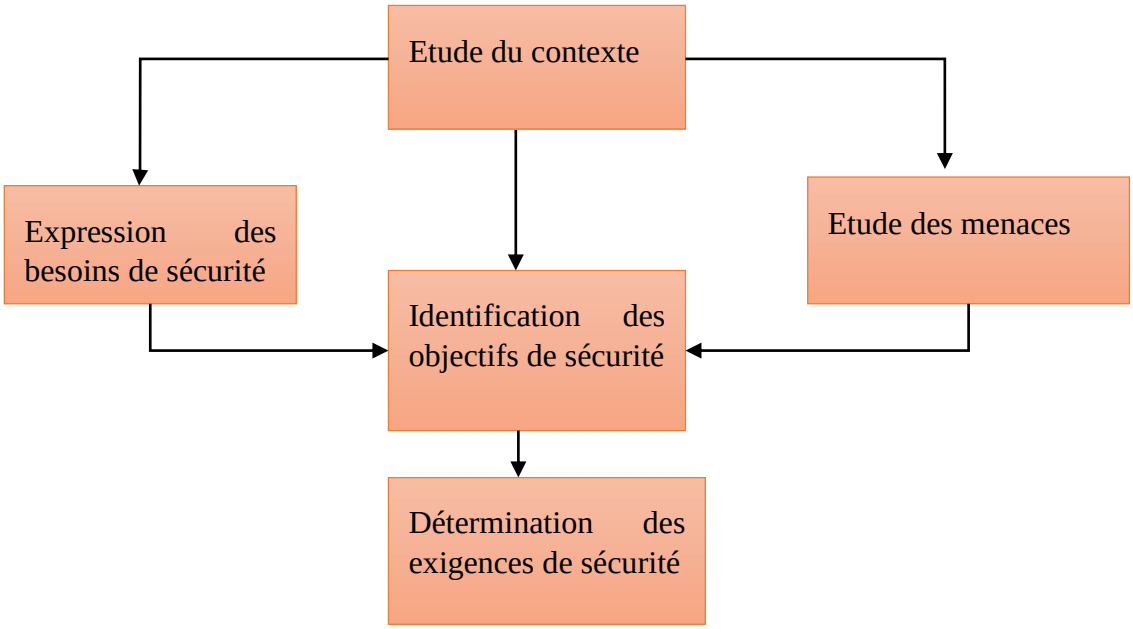


Figure 5: Démarche globale de la méthode Ebios

- Méthode d'analyse de risques informatiques optimisée par niveau (MARION)

La méthode d'analyse de risques informatiques orientée par niveau (Marion) est une méthode d'audit, proposée depuis 1983 par le CLUSIF[14], visant à évaluer le niveau de sécurité informatique d'une entreprise. L'objectif est double :

- situer l'entreprise auditée par rapport à un niveau jugé correct, et par rapport au niveau atteint par les entreprises similaires
- identifier les menaces et vulnérabilités à contrer.

- Méthode harmonisée d'analyse des risques (MEHARI)

La méthode harmonisée d'analyse des risques (MEHARI) est une méthode complète, outillée de gestion de risque associée à la sécurité de l'information d'une entreprise ou d'un

[13] https://adullact.net/projects/ebios2010/
[14] Club de la sécurité de l'information français

organisme. Elle a été développée initialement (depuis 1996) par le CLUSIF en France puis le CLUSIQ au Canada.

L'outil MEHARI le plus diffusé est MEHARI EXPERT, dont la dernière révision date de 2016. MEHARI répond pleinement aux lignes directrices édictées par la norme ISO 27005:2011, donc ISO 31000.

Ses objectifs sont les suivants :

- mieux connaître les activités et les processus mis en place par l'organisme afin d'en évaluer les risques en cas de dysfonctionnements, bien délimiter les actifs contribuant au traitement de l'information,
- connaître les menaces pouvant les atteindre,
- auditer les modes de mise en œuvre des services de sécurité (destinés à réduire les vulnérabilités) ;
- Déterminer les situations de risque à partir de scénarios intégrant les éléments précédents;
- Évaluer les niveaux de risque ainsi que les options de traitement et les moyens d'en diminuer le niveau;
- Préparer des plans de réduction des risques et s'assurer de leur mise en place dans le temps;
- limiter le volume de travail à fournir pour l'étude.

Ce chapitre nous a permis de prendre connaissance de de l'environnement des systèmes d'information des ressources humaines et de ses composantes d'une part et d'autre part nous avons essayé de ressortir les outils permettant de garantir un système de qualité tel que présenté par les experts du domaine des systèmes d'information. Dans le prochain chapitre nous allons nous intéresser au système d'information des ressources humaines de l'Institut Universitaire de la Côte.

CHAPITRE II : ETAT DE LIEU DU SYSTEME D'INFORMATION DES RESSOURCES HUMAINES DE L'INSTITUT UNIVERSITAIRE DE LA COTE

L'objectif de ce chapitre est de présenter le SIRH de l'institut Universitaire de la côte et leurs fonctionnement ; ainsi que la cartographie applicative et enfin ressortir les point faibles et les points faibles de ce système afin de proposer un cahier de charge de projet d'audit.

SECTION I. Présentation De L'institut Universitaire De La Côte

Aujourd'hui, l'enseignement supérieur se trouve à la croisée des chemins dans la plupart des pays développés ou en développement. Ainsi, l'**Institut Universitaire de la Côte** (**IUC**) grande institution privée d'enseignement supérieur a pour vocation la formation intellectuelle et humaine des étudiants de diverses nationalités aux cycles de Brevet de Technicien Supérieur et d'ingénieur, de licence et master professionnel. Cette formation contribue au développement des entreprises et de l'entreprenariat en rapport avec l'évolution du monde industriel, technologique et des affaires.

1. Création Et Evolution de l'Institut Universitaire de la Côte

L'Institut Universitaire de la Côte en abrégé IUC a été créé pour résoudre un problème majeur constaté dans le milieu professionnel. Dans un secteur d'activité comme dans un autre, le manque de techniciens bien formés se fait ressentir, de même que l'inadéquation grandissante de produits du système éducatif avec les besoins du marché d'emploi et même dans toute la zone CEMAC.

Ainsi, pour pallier à cette situation et répondre au besoin du marché, l'IUC a vu le jour sous le nom ISTDI (Institut Supérieur des Technologies et du Design Industriel) par arrêté N°02/0094/MINESUP/DDES/ESUP du 13Septembre 2002 et autorisation d'ouverture le 18 Septembre 2002 avec le soutien d'une coopération française.

Implanté dans la région du littoral, département du Wouri, arrondissement de Douala 5ème, quartier Logbessou, elle avait pour cible principale les aspirants à une formation industrielle (MSI, MAVA, ET, II, GC…) et d'ingénieur (prépa, 3IL).A ce titre, elle était dotée en 2003 d'un bâtiment d'environ 08salles de classe accueillant un effectif d'environ 30 étudiants répartis dans pratiquement 06 filières. Afin de manager cet ensemble, le personnel administratif était composé de 06 employés coiffé par un directeur.

Ce pan de l'enseignement étant parfaitement maitrisé, le besoin d'élargir ses horizons entraine l'ouverture des filières commerciales en 2007. Cet accroissement de l'institut a porté le nombre d'employé a environ 20, face à un effectif à la hausse d'environ 3000 étudiants dispatchés en 13 filières à 2 niveau d'études (07 commerciales et 06 industrielles).

En 2011, l'institut est officiellement érigé en Institut Universitaire de la Côte et englobe en son sein trois établissements :

- ISTDI : Institut Supérieur des Technologies et du Design Industriel
- ICIA : Institut de Commerce et d'Ingénierie d'Affaires
- 3IAC : Institut d'Ingénierie Informatique d'Afrique Centrale

A côté de ces instituts, l'IUC prépare les candidats à la certification CISCO. L'organisation interne est revue, le personnel administratif est passé à presque 160 employés. Les effectifs ont considérablement augmentés et sont d'environ 5000 étudiants. Le site quant à lui s'est agrandit. Il est constitué d'un plateau technique conséquent et des infrastructures de pointe : 80 salles de cours de plus de 3000 places assises, 14 laboratoires modernes et bien équipés conçu afin de former les étudiants non seulement opérationnels sur le marché de l'emploi, mais également les doter d'un savoir-faire ; de deux amphithéâtres de 150 et 500 places sonorisés avec vidéosurveillance, une bibliothèque.

2. MISSIONS / OBJECTIFS

L'IUC a pour mission globale d'aider les jeunes étudiants à construire et à réaliser leur projet de formation. Son souci majeur étant de former les étudiants non seulement opérationnels sur le marché de l'emploi mais aussi inégalable dans leurs domaines. C'est pour cette raison que afin de doter les étudiants d'un savoir-faire très satisfaisant, l'institut s'attelle à recruter un corps enseignant digne dans le but de disperser les meilleurs cours.

Comme toute entreprise ayant une vision à long terme, l'IUC tend à devenir un vrai établissement universitaire technologique en adéquation avec les besoins des entreprises.

En ces mots, ce dernier fait part de son engouement à faire des étudiants des personnes aux profils professionnels comme les entreprises l'entendent.

Pour atteindre ses objectifs, l'IUC dans son organisation dispose d'un organigramme plus ou moins complexe dans lequel le service des ressources humaines se trouve sous la Direction des Affaires Administratives et Financières. (***Annexe 1***).

SECTION II. Le Système d'Information des Ressources Humaines de l'IUC.

Le service des ressources humaines de l'Institut Universitaire de la Côte est celui auquel nous nous intéressons. Nous allons identifier ici ses différentes composantes afin de déceler d'éventuels manquements.

1. Les objectifs du SIRH

L'IUC aujourd'hui regroupe environ 150 personnels permanents (enseignant administratif) et 300 enseignants vacataires qui interviennent par mois. Le système d'information des ressources humaines est un instrument susceptible d'aider les gestionnaires à planifier, contrôler et évaluer l'exécution et les résultats des opérations liées à la gestion de ces ressources humaines.

Il permet de répondre aux missions principales du service des ressources humaines que sont :

- La gestion administrative du personnel
- La gestion sociale (CNPS, Assurance)
- La gestion prévisionnelle du personnel
- La gestion de la paie.

Pour cela, il doit pouvoir enregistrer les flux d'information (données du personnel, paie, congés, etc.), les classer et, périodiquement en faire une synthèse qui sera présentée aux responsables. Comme corollaire, les informations fournies par ce système doivent :

- Permettre aux décideurs de prendre des décisions stratégiques et opérationnelles qui conviennent.
- Permettre aux différents collaborateurs d'avoir une image de marque de l'Institut.
- Permettre la création de la valeur par le service RH

Ainsi, Le SIRH de l'IUC a également des objectifs opérationnels en ce sens qu'il doit aider à traiter des informations nécessaires à l'exécution des tâches quotidiennes. Pour récapituler, les utilisateurs souhaitent pouvoir expliquer, contrôler, prévoir et informer à partir

des informations produites par le SIRH.

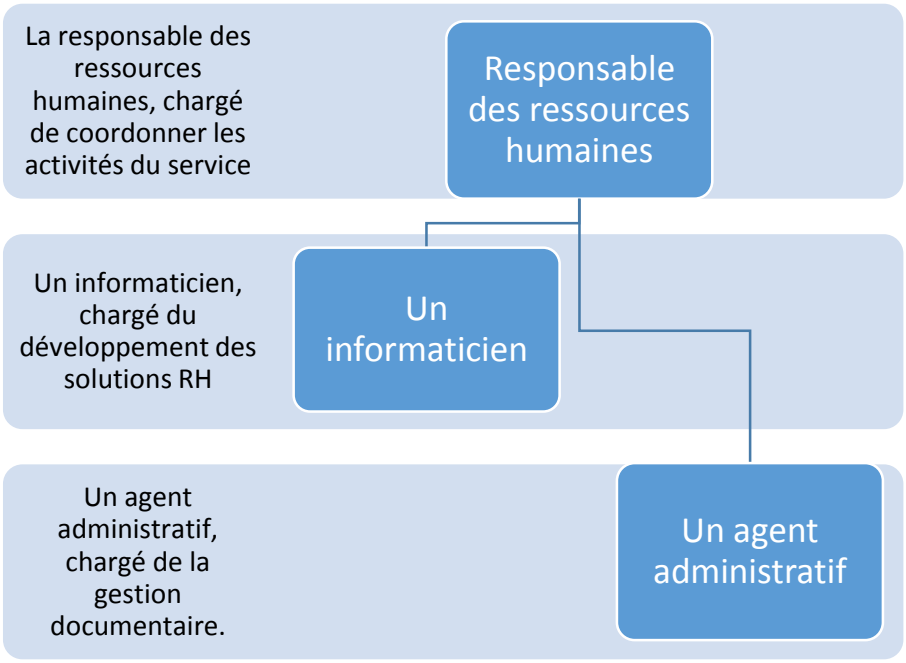
2. Les Composantes Du SIRH de l'IUC

Le SIRH de l'IUC, pour assurer les fonctions de collecte, de traitement, de stockage et de diffusion des informations, utilise divers moyens notamment les moyens humains, matériels, pour n'en citer que ceux-là.

a) Les Acteurs du SIRH de l'IUC

Le service des ressources des ressources humaines de l'IUC se trouve sous la direction des affaires administratives et financières ; et est constitué actuellement de 3 membres.

Figure 6: organigramme service RH-IUC



Source : Nous même

Le SIRH interagit également avec des acteurs externes au service RH. Nous avons ainsi ;

- Le service de la comptabilité

Ce service, en étroite collaboration avec le service des ressources humaines suit les activités comptables et fiscales. Il doit informer principalement le SIRH des changements apportés aux lois de finance annuelle du Cameroun.

- La Division des systèmes d'information

La mission de ce service est de gérer le réseau interne et externe à l'IUC. Il est également l'acteur principal de la sécurité des différents systèmes d'information. Il veille également au bon fonctionnement des matériels informatiques

- Le SEED (Software Enterprise Engineering Division)

Sa mission principale est de produire et/ou assurer la maintenance des logiciels en interne permettant d'automatiser les processus métier de l'entreprise.

- Le personnel enseignant

Celui-ci est le principal acteur exploitant les ressources informationnelles du SIRH à travers l'application mobile. Il a par exemple la possibilité de télécharger sa fiche de paie à travers l'application.

b) L'architecture technique et applicative

L'IUC, pour le bon fonctionnement des activités RH, utilise des matériels (ordinateurs, réseaux, etc.) et des logiciels.

En 2017, le progiciel Morpheus est la principale application autour de laquelle s'arpente les processus RH. Il s'agit d'un ERP (Enterprise Resource Planning) dont 2 modules principaux sont consacrés à la gestion des ressources humaines et de la paie. A cet ERP déployé, une application mobile androïde permet d'avoir accès à certaines informations liées à la gestion de la paie tel que la fiche de paie depuis le réseau internet.

Pour permettre aux éléments logiciels d'assurer leurs fonctions, un ensemble de matériel existent également dans le SIRH. Une cartographie de l'infrastructure est présentée en ***annexe 2***

Le tableau suivant présente les caractéristiques des composants ainsi que des logiciels.

Tableau 5:Liste du parc informatique du service RH

Eléments	Caractéristiques
Système d'exploitation	Windows 7
Microsoft office	Version 2013
Kaspersky internet Security	Version 2017
Postes de travail	Ils sont au nombre de 3 au service des ressources humaines, ils sont sur une électrique ondulée
Imprimante	HP LaserJet P1100,

Source : Nous-mêmes

3. Les processus du SIRH de l'IUC

La fonction gestion des ressources humaines d'une entreprise se caractérise par la singularité de ses taches. A travers le tableau ci-dessous nous allons positionner les processus RH de l'IUC dans les processus générique de la fonction RH d'une entreprise.

Tableau 6: Positionnement des processus RH de l'IUC dans le processus génériques RH

CATEGORIES	ACTIVITES	Existant	Inexistant	Commentaires
Gestion Administrative et réglementaire	Gestion administrative (GA)	**X**		
	Gestion des temps et activités (GTA)	**X**		Elle se limite principalement à la gestion des congés
	Paie	**X**		
Gestion individuelle	Recrutement	**X**		La formalisation de ce processus reste une nécessité
	Formation		**X**	

	Performance, entretiens d'évaluation		**X**	
Gestion Collective	Contrôle de gestion social			
	Gestion prévisionnelle des emplois et compétences (GPEC)		**X**	
	Rémunération globale	**X**		
Reporting	Reporting	**X**		Ce processus se limite pour le moment à la restitution ponctuelle de donnée

Source : Nous-mêmes

SECTION III. La gestion de la sécurité du SIRH de l'IUC

Cette section est consacrée à la description de la manière dont l'IUC s'organise pour la gestion menaces qui pèsent sur son SIRH et ceci à travers des dispositions prises pour prévenir, détecter et corriger d'éventuelles vulnérabilités

1. Organisation de la sécurité du système d'information

L'IUC ne dispose pas d'organe spécifique chargé de la gestion de la sécurité de son système d'information des ressources humaines. Cette gestion est plutôt laissée aux soins de la division des systèmes d'information (DSI) qui s'assure de la disponibilité, de l'intégrité et de la confidentialité des informations.

2. Les dispositifs et les procédures de sécurité

Le premier dispositif de sécurité mis en place est l'obligation faite aux utilisateurs du respect des bonnes pratiques pour la sauvegarde de l'intégrité de l'information et des outils de travail.

Bien qu'ils ne soient pas documentés, d'autres dispositifs de sécurité sont déployés pour assurer la sécurité des personnes et des biens.

a) Les dispositifs de sécurité physique et leur gestion

Les locaux du service des ressources se ferment à clé. Cependant, le matériel informatique n'as de dispositif antivol.

Des imprimés expliquant les comportements à tenir en cas d'incendie sont affichés à l'entrée de ce bloc administratif. De même, trois extincteurs d'incendie sont disponibles. La salle des serveurs est fermée et c'est la division des systèmes d'information qui garde les clefs. Les serveurs sont gardés à une température maximale de 18° Celsius à l'aide d'un climatiseur, en vue d'éviter qu'ils surchauffent.

b) La sécurité logique (la gestion des accès)

L'utilisation de l'application Morpheus est régit par les droits d'accès ; qui sont attribuer aux utilisateurs par le SEED et donnent droit aux fonctionnalités à la demande de la Directrice des Affaires Administratives et Financières. La demande doit être faite par téléphone ou par courriel. Bien que les droits d'accès soient créés en tenant compte des tâches de l'agent avec le programme, il n'existe pas une liste qui renseigne sur les droits d'accès octroyés.

L'accès à un poste de travail se fait sans authentification préalable. D'autres personnes peuvent travailler sur un même poste de travail sans contraintes.

En ce qui concerne l'accès au réseau tous les sites Internet sont accessibles aux agents.

En ce qui concerne le prêt de mot de passe aucune règlementation n'y est faite.

3. Formation et sensibilisation

Au service des RH, chaque utilisateur de l'application Morpheus doit être formé sur place. Les formations sont organisées après le recrutement et lorsque le besoin se fait sentir. En cas d'ajout ou de mise à jour d'une fonctionnalité les utilisateurs qui sont susceptibles de travailler avec cette application reçoivent des formations.

En matière de sensibilisation du personnel à la sécurité de l'information, la direction générale passe par les différents responsables pour sensibiliser le personnel affilié en ce qui concerne une nouvelle procédure ou une quelconque décision. L'objectif étant de faire comprendre à tous le personnel (utilisateurs, managers et informaticiens) les enjeux de la

sécurité ainsi que la conduite à tenir vis-à-vis de l'information ou des ressources spécifiques qu'ils gèrent ou utilisent.

4. Documentation

Cette articulation, fait référence principalement au manuel des procédures RH et aux manuels « utilisateurs » de l'application Morpheus utilisée par le service.

Il existe un manuel de procédure RH formalisant certaines activités RH. Néanmoins, dans la gestion du personnel, le code du travail est le guide principal des RH.

En ce qui concerne l'application Morpheus, il n'existe pas encore de manuel utilisateur

5. Gestion de la continuité des activités

L'IUC étant l'un des leaders dans l'enseignement supérieur privé au Cameroun, garantir la continuité de l'exploitation en cas de sinistre est pour les dirigeants un enjeu de taille.

Pour cela, en dehors du site du siège qui gère les principales activités, elle dispose d'un site de secours, prêt à accueillir les différentes directions « métier » en cas de sinistre. De même, pour assurer la sécurité de ses matériels informatiques et favoriser la continuité des activités en cas de délestage, l'IUC dispose d'un groupe électrogène à démarrage automatique à son siège et dans le campus d'Akwa. Aussi, chaque poste de travail du service RH se trouve sur une ligne ondulée avec un onduleur central de trente (30) minutes d'autonomie.

Ce chapitre nous a permis de matérialiser le système d'information des ressources humaines actuel. La revue du cadre organisationnel et des dispositifs de sécurité physiques et logiques constitue le grand point développé. Ce chapitre nous a également permis d'appréhender les pratiques actuelles ; lesquelles seront le socle de nos analyses et de nos éventuelles recommandations à travers la mise en œuvre de notre mission d'audit. Cette mise en œuvre de l'audit fera l'objet du prochain chapitre

CHAPITRE III : REALISATION DE LA MISSION D'AUDIT DU SIRH DE L'IUC

L'audit du système d'information d'une organisation, comme nous l'avons souligné précédemment, a pour objectif de rapprocher les pratiques de celle-ci aux bonnes pratiques, d'analyser les écarts éventuels afin de proposer des actions pour renforcer les procédures et dispositifs de sécurité. Notre étude ne va pas déroger à cette démarche.

Les différentes étapes de nos travaux avec les diligences menées seront présentées premièrement, ensuite nous présenterons sous forme de projet de rapport d'audit les résultats de la mission tout en faisant ressortir les forces et les faiblesses des procédures et des dispositifs mis en place par l'IUC afin de garantir la sécurité de son SIRH

SECTION I. Préparation de la mission

Toute mission d'audit pour atteindre les objectifs, exige une bonne préparation. Cette préparation constitue en d'autres termes la phase d'étude de la mission où il importe de prendre des dispositions nécessaires au bon déroulement des travaux sur le terrain. Elle a consisté à initialiser la mission, à faire la prise de connaissance du domaine audité et à préparer les documents indispensables à la mission.

1. Initialisation de la mission et prise de connaissance de l'entité

Notre mission a été débutée avec une analyse documentaire sur l'audit des systèmes d'information.

Par la suite, nous avons porté à la connaissance des différents responsables en relation avec le SIRH, le thème de notre étude et les objectifs poursuivis. Des amendements ont été apportés par ces responsables.

Nous avons également élaboré des questionnaires de prise de connaissance (***annexe 3 et 4***) et des questionnaires de contrôle interne (***annexe 5***) qui permettent d'interroger l'environnement du SIRH. Ainsi, nous avons pu prendre connaissance des activités, de l'histoire, de l'organisation de l'IUC en générale et de son SIRH en particulier. Ces informations nous ont permis de présenter le SIRH (chapitre 2).

Une fois la prise de connaissance faite, nous avons procédé à un découpage de la mission en objets auditables ; à l'élaboration du tableau des risques, du plan de la mission, du rapport d'orientation et du programme de vérification

2. Découpage du SIRH en objets auditables et choix du référentiel de la mission

Le découpage des différents éléments composant le SIRH permettra de couvrir un ensemble de point. Nous allons découper les éléments composant le SIRH en objets auditables afin de pouvoir cerner les risques majeurs qui peuvent entraver son bon fonctionnement.

☞ Les actifs applicatifs permettant gestion de l'information

L'audit d'une application peut avoir deux visées distinctes : l'audit de fiabilité et de sécurité ou l'audit d'efficacité et de performance. Un audit complet couvrira ces deux périmètres.

- ***L'audit de fiabilité et de sécurité*** a pour objectif d'émettre une appréciation motivée sur la fiabilité de l'outil informatique, c'est-à-dire sur la qualité du contrôle interne de l'application et la validité des données traitées et restituées. Ce type d'audit permettra de mettre en évidence d'éventuelles failles dans la chaîne de contrôle composée de contrôles programmés effectués par la machine et de contrôles manuels restant à la charge des utilisateurs.
- ***L'audit d'efficacité et de performance*** a pour objectif d'apprécier l'adéquation de l'application aux besoins et aux enjeux de l'organisation, d'évaluer sa contribution à la création de valeur, d'évaluer sa performance et sa rentabilité et enfin d'évaluer sa pérennité et sa capacité d'évolution.

☞ La sécurité logique, physique et environnementale

Ces différents domaines ou fonctions du SIRH ont été évalué au regard des bonnes pratiques de sécurité que proposent les normes ISO 27001 et 27002 que nous dérouleront au travers de la méthode EBIOS; du guide pratique d'audit des technologies de l'information « GTAG 8 - audit des contrôles applicatifs » ; de référentiel de bonnes COBIT version 5 concernant la sécurité de l'information.

3. Plan de mission

L'auditeur du système d'information doit établir un plan de mission. Selon la norme 2200 de l'IIA, ce plan doit comporter les objectifs, le champ d'intervention, la date et la durée de la mission, ainsi que les ressources allouées

Tableau 7: Plan de mission

PLAN DE MISSION		
AUDIT DU SYSTEME D'INFORMATION DES RESSOURCES HUMAINES		**Entité** : IUC **Référence** : PM
OBJECTIF GENERAL DE LA MISSION : Documenter le niveau de vulnérabilité du système d'information des ressources humaines		
Champ d'intervention		La mission portera sur l'audit des applications relatives aux activités RH ; ainsi que les aspects organisationnels, physiques et procéduraux de la sécurité des SIRH de l'IUC
Date et durée de la mission		La mission débutera le 09 octobre 2017 et s'étendra jusqu'au 30 Décembre 2017 (83 jours)
Ressource :		La mission se fera par nous même sous la supervision de la responsable RH
Approche retenue		Approche par les risques
CALENDRIER DE LA MISSION		
09/10/2017–22/102017	2 semaines	Préparation de la mission et prise de connaissance du SIRH
23/10/2017-11/11/2017	2 semaines	Préparation des documents de travail (QCP, QCI, Feuilles de test...)
13/11/2017-17/11/2017	05 jours	Achèvement du programme de vérification
18/11/2017-09/12/12017	18 jours	Mise en œuvre du programme de vérification
11/12/2017-16/12/2017	06 jours	Préparation des conclusions
18/12/2017-20/12/2017	03 jours	Rédaction du projet de rapport
21/12/2017-23/12//2017	03 jours	Soumission du projet de rapport
26/12/2017-30/12/2017	05 jours	Soumission du projet de rapport pour validation et intégration des commentaires

Source : Nous-mêmes

Dans le cadre de l'exécution de notre mission, nous avons tenu compte de l'objectif général de la mission, du champ de la mission, de sa date du début et de sa durée. Nous avons présenté également l'approche retenue pour la mission et le calendrier y afférent

SECTION II. Audit des applications du SIRH à l'IUC

Le but de l'audit d'une application opérationnelle est de donner au management une assurance raisonnable sur son fonctionnement. Il faut noter que toutes les applications d'un système d'information ne sont pas auditables. C'est ainsi que l'audit des applications s'intéressera particulièrement aux applications standards ou progicielles et aux applications spécifiques développées en interne.

Par applications standard , nous entendons des progiciels dont le but principal est de mettre à disposition des fonctionnalités de base et des outils de création de processus et de workflows, et dont la paramétrisation permet la mise en place de solutions spécifiques qui répondent aux besoins de l'entreprise.

Dans le cas de développements internes, l'auditeur n'est pas en mesure de s'appuyer sur les informations et les expériences généralement connues et doit adapter sa procédure d'audit à l'application concernée.

Dans le cas d'espèce, l'application à laquelle nous nous intéressons est développée en interne ; cependant il s'agit d'un progiciel regroupant un ensemble de métiers de l'institut. Nous allons scruter uniquement les modules de gestion de ressources humaines et la paie.

Pour mener à bien notre travail, nous allons nous intéresser aux aspects efficacité, performance, fiabilité et sécurité de l'application.

1. Audit d'efficacité et de performance de l'application

Dans cette phase nous avons choisi une population. Nous nous sommes intéressés à deux (02) profils les développeurs de l'application (ceux chargés de programmation et de l'intégration de l'application) et les utilisateurs de l'application (ici, il s'agit principalement du personnel du service des ressources humaines et de la directrice des affaires administratives et financières). L'effectif au total était de 10 personnes (4 utilisateurs du service RH et 6 acteurs du développement logiciel).

Pour permettre à notre population de bien cerner les questions (annexe 6) et d'y répondre de manière objective, nous avons pris rendez-vous avec les différents intervenants, dans le but de les soumettre à une interview au cours duquel, nous avons échangés sur le questionnaire, ensuite nous avons complétés par des questions qui ne figuraient pas dans la fiche à l'exemple de :

- Pensez-vous que l'application Morpheus améliore vraiment vos tâches quotidiennes ?
- Connaissez-vous des applications de gestion des ressources humaines que vous semble plus adapté à votre tâche que Morpheus ?
- Pensez-vous que les fonctionnalités des modules RH et paie pourront permettre d'automatiser les permissions et absences qui sont entièrement manuels aujourd'hui ?
- Comment se fait la mise à jour des fonctionnalités ?

L'audit d'efficacité a permis d'apprécier l'alignement stratégique de l'application, l'adéquation aux besoins des utilisateurs. Tandis que l'analyse de la performance et de la pérennité a permis d'apprécier les capacités fonctionnelles actuelles et d'avoir un aperçu de la vision donné à l'application.

2. Audit de la sécurité et de la fiabilité

Afin d'évaluer la sécurité et la fiabilité de l'application, nous nous sommes intéressés à trois (03) axes, à savoir analyse des risques associés à l'organisation, analyse des risques associés à l'application et enfin analyse des risques associés à la fonction informatique.

Afin de pouvoir couvrir tous champs nous avons soumis le questionnaire de contrôle interne (***annexe 7***) à la DIPD (Direction des Infrastructures, de la Planification et du Développement) qui regroupe les ressources expertes pouvant nous permettre d'avoir des réponses fiables. Ce questionnaire était bien évidemment accompagné des interviews qui ont permis la bonne compréhension de l'orientation des questions. Nous avons pu observer la mise en place de bonnes pratiques dans la gestion de la sécurité également quelques manquement qui seront sujets dans le chapitre suivant.

SECTION III. Audit de la sécurité du SIRH

1. Définition du cadre de gestion des risques du SIRH

Selon la méthode EBIOS, la première étape consiste entre autre à identifier les sources de menaces, de préparer les métriques et identifier les biens essentiels du système.

a) Les sources de menaces

Tableau 8: Les Sources de menaces

Type de source de menace	Sources de menace	Retenu	Justification
Source humaine interne, malveillante, avec de faibles capacités	Stagiaire	X	
Source humaine interne, malveillante, avec des capacités importantes	Attaque cybercriminelle	X	
Source humaine interne, malveillante, avec des capacités illimitées	Employé du service maitrisant	X	
Source humaine externe, malveillante, avec de faibles capacités	Personnel de nettoyage (soudoyé)	X	
Source humaine externe, malveillante, avec des capacités importantes	Concurrent (éventuellement en visite incognito) Maintenance informatique	X	
Source humaine externe, malveillante, avec des capacités illimitées			Non, le service n'estime pas y être exposé.
Source humaine interne, sans intention de nuire, avec de faibles capacités	Employé peu sérieux	X	
Source humaine interne, sans intention de nuire, avec des capacités importantes			Non, le service n'estime pas y être exposé.
Source humaine interne, sans intention de nuire, avec des capacités illimitées	Employé peu sérieux (ceux qui jouent un rôle d'administrateur)	X	
Source humaine externe, sans intention de nuire, avec de faibles capacités	Client, Cotraitant, Partenaire	X	
Source humaine externe, sans intention de nuire, avec des capacités importantes	Fournisseur d'accès Internet Hébergeur	X	
Source humaine externe, sans intention de nuire, avec des capacités illimitées			Non, le service n'estime pas y être exposé.
Code malveillant d'origine inconnue	Virus non ciblé	X	
Phénomène naturel	Phénomène naturel (foudre, usure,...)	X	
Catastrophe naturelle ou sanitaire	Maladie	X	
Activité animale		X	
Événement interne	Incendie des locaux Panne électrique	X	

Source : Ebios

b) Les métriques utilisées

- ✓ Les critères de sécurité retenus : disponibilité, intégrité et confidentialité

Afin d'exprimer les besoins de sécurité, les critères de sécurité retenus sont les suivants :

Tableau 9: Critères de sécurité du SIRH

critère de sécurité	Définitions	Niveaux	Description détaillée de l'échelle
Confidentialité	Propriété des biens essentiels de n'être accessibles qu'aux personnes autorisés.	Public	Le bien essentiel est public.
		Limité	Le bien essentiel ne doit être accessible qu'au personnel et aux partenaires.
		Réservé	Le bien essentiel ne doit être accessible qu'au personnel (interne) impliquées.
		Privé	Le bien essentiel ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître.
Disponibilité	Propriété d'accessibilité au moment voulu des biens essentiels par les personnes autorisées.	Plus de 72h	Le bien essentiel peut être indisponible plus de 72 heures.
		Entre 24h et 72h	Le bien essentiel doit être disponible dans les 72 heures.
		Entre 4h et 24h	Le bien essentiel doit être disponible dans les 24 heures.
		Moins de 4h	Le bien essentiel doit être disponible dans les 4 heures.
Intégrité	Propriété d'exactitude et de complétude des biens essentiels.	Détectable	Le bien essentiel peut ne pas être intègre si l'altération est identifiée.
		Maîtrisé	Le bien essentiel peut ne pas être intègre, si l'altération est identifiée et l'intégrité du bien essentiel retrouvée.
		Intègre	Le bien essentiel doit être rigoureusement intègre.

Source : EBIOS

✓ Echelle de gravité

L'échelle suivante sera utilisée pour estimer la gravité des événements redoutés et des risques :

Tableau 10: Echelle de gravité des menaces

Ordre	Niveau de l'échelle	Description détaillée
1	Négligeable	Le service RH surmontera les impacts sans aucune difficulté
2	Limitée	Le service RH surmontera les impacts malgré quelques difficultés
3	Importante	Le service RH surmontera les impacts avec de sérieuses difficultés
4	Critique	Le service RH ne surmontera les impacts (Sa survie est menacée)
5	Hyper critique	Le service RH n'ose pas envisager

Source : Ebios

✓ Echelle de vraisemblance

L'échelle suivante sera utilisée pour estimer la vraisemblance des scénarios de menaces et des risques :

Tableau 11: Echelle des vraisemblances des menaces

Ordre	Niveau de l'échelle	Description détaillée
1	Minime	Cela ne devrait pas se (re) produire
2	Significative	Cela pourrait se (re) produire
3	Forte	Cela devrait se (re) produire un jour ou l'autre
4	Maximale	Cela va certainement se (re) produire prochainement

Source : Ebios

c) Les biens identifiés

- Les biens essentiels

Les biens sensibles identifiés sont relatifs aux processus RH.

Tableau 12: Les biens essentiels

Processus essentiels	Informations essentielles concernées	Dépositaire
Gestion des vacations	Etat de vacation (validation des heures effectuées)	Le service suivi et évaluation
Gestion de la paie	▪ Les états d'allocations congés ▪ Les états d'heures supplémentaires ▪ Les états de paie ▪ Les bulletins de paie ▪ Les relevés de vacation	Service RH
Gestion des dossiers du personnel	Les dossiers physique du personnel (diplôme, contrat, CNI, CV, Sanction…)	Service RH

Source : Ebios

- Les biens supports

Nous avons les biens supports suivants :

- Local du service RH
- Les serveurs d'application Morpheus et de base de données
- Les administrateurs informatiques
- Le service RH
- Les ordinateurs du service RH
- Les outils de messagerie
- La suite bureautique office
- Le système d'exploitation Windows 7
- Internet
- Support papier

d) Les liens entre les biens essentiels et biens supports

Le tableau suivant présente les biens supports et leurs liens avec les biens essentiels :

Tableau 13: Liens entre biens essentiels et biens supports

Biens Supports \ Biens essentiels	Gestion des vacations	Gérer la paie	Gestion des dossiers du personnel	Gestion des procédures RH
Local du service RH	X	X	X	X
Le service RH	X	X	X	X
Les ordinateurs du service RH	X	X	X	
Les serveurs d'application et base de données	X	X		
Les administrateurs informatiques				
La suite bureautique office	X	X		
Système d'exploitation Windows 7				
Outils de messagerie				
Internet				
Support papier			X	X

Source : Ebios

2. Etude des évènements redoutés

a) Les évènements redoutés

Chaque ligne du tableau suivant représente un événement redouté par le service RH (bien essentiel, critère de sécurité, besoin de sécurité selon les échelles de besoin, sources de menaces et impacts). La gravité de chaque évènement redouté est estimée (cf. échelle de gravité) sans tenir compte des mesures de sécurité existantes.

Tableau 14: Les évènements redoutés

Evènement redoutés	Besoin de sécurité	Source de menaces	Impacts	Gravité
Gestion des vacations				
Indisponibilité des données de vacations	24-72h	-Employé peu sérieux -Incendie des locaux -Panne électrique	-Impossibilité de valider les vacations -Impossibilité de traiter la paie -Perte de crédibilité	2. Limitée
Compromission des données de vacations	Limité	-Employé peu sérieux -Employé soudoyé par les enseignants -Concurrent ayant hacker le système -Erreur système	-Perte financières -Perte de la crédibilité -Perte de notoriété	3. Importante
Indisponibilité des états de vacation en ligne	Plus de 72h	-Panne du système informatique -Indisponibilité du fournisseur d'accès internet	-Perte de crédibilité -Mécontentement du personnel enseignant	1. Négligeable
Gestion de la paie				
Indisponibilité du logiciel Morpheus	24-72h	-Employé peu sérieux -Panne électrique -Virus non ciblé -Personnel de maintenance	-Impossibilité de payer les salaires dans les délais -Perte de la notoriété -Mécontentement des personnels	3. Importante
Compromission des données de la paie	Intègre	-Personnel administrateur du système -Personnel ayant connaissance du système -Employé mécontent Employé soudoyé	-Trop perçu versé aux employés -Grève des employés -Perte financière pour l'entreprise -Perte de crédibilité -Redressement par l'Etat	4. Critique
Diffusion des salaires du personnel	Privé	-Employé peu sérieux -Attaque cybercriminelles	-Perte de crédibilité -Grève des employés -Bouche à oreille négatif	3. Critique
Gestion des dossiers du personnel				
Indisponibilité des dossiers du personnel	24-72h	-Personnel peu sérieux -Incendie des locaux -Attaque des rongeurs	-Impossibilité de fournir les dossiers au ministère -Perte de crédibilité vis-à-vis des usagers	2. Limitée

		-Dossier non fourni aux RH		
Altération des dossiers du personnel	Détectable	-Employé peu sérieux -Attaque des rongeurs -Incendie dans les locaux	-Perte de crédibilité -Perte de données	3. Importante
Falsification des documents	Détectable	-Personnel soudoyé -Concurrent peu sérieux	-Perte de crédibilité	2. Limitée
Gestion des procédures RH				
Indisponibilité des procédures	Plus de 72h	-Personnel peu sérieux	-Perte de crédibilité vis-à-vis des usagers	1. Négligeable

Source : Ebios

b) Evaluation de la gravité

L'importance relative des événements redoutés précédemment analysés (identifiés et estimés) est évaluée à l'aide du tableau suivant (cf. critères de gestion des risques) :

Tableau 15: Evaluation de la gravité des évènements redoutés

Gravité	Evènement redoutés
4. Critique	• Compromission des données de la paie • Diffusion des salaires du personnel
3. Importante	• Compromission des données de vacations • Indisponibilité du logiciel Morpheus • Altération des dossiers du personnel
2. Limitée	• Indisponibilité des données de vacations • Indisponibilité des dossiers du personnel • Falsification des documents
1. Négligeable	• Indisponibilité des états de vacation en ligne • Indisponibilité des procédures

Source : Ebios

3. Etude des scénarios de menaces

a) Les scénarios de menaces

Les pages suivantes présentent les scénarios de menaces potentiellement réalisables dans le cadre du sujet de l'étude. Les sources de menaces susceptibles d'en être à l'origine sont identifiées et la vraisemblance de chaque scénario de menace est estimée (cf. échelle de vraisemblance). Le détail des scénarios de menaces (menaces, vulnérabilités et prérequis) est décrit dans les bases de connaissances de la méthode EBIOS.

Tableau 16: Scénarios de menaces

Scénarios de menaces	Sources de menaces	vraisemblance
Le service RH		
Menace sur le service RH causant une indisponibilité	• Employé peu sérieux • Maladie	2. Significative
Menace sur le service RH causant une compromission	• Employé soudoyé • Personnel de nettoyage	3. Forte
Menace sur le service RH causant une Altération	• Employé mécontent • Employé soudoyé	1. Minime
Menace sur le service RH causant une Falsification	• Employé mécontent • Employé soudoyé	1. Minime
Menace sur le service RH causant une Diffusion	• Employé mécontent	1. Minime
Les administrateurs informatiques		
Menace sur les administrateurs informatiques causant une indisponibilité	• Maladie • Personnel peu sérieux	1. Minime
Menace sur les administrateurs informatiques causant une compromission	• Personnel peu sérieux • Personnel soudoyé	3. Forte
Menace sur les administrateurs informatiques causant une Altération	• Personnel mécontent • Personnel peu attentif	1. Minime
Menace sur les administrateurs informatiques causant une Diffusion	• Personnel mécontent • Personnel peu attentif	2. Significatif
Les serveurs d'application et de base de données		
Menace sur les serveurs causant une indisponibilité	• Cyber-attaque • Virus informatique • Maintenance • Personnel peu sérieux • Panne électrique	4. Maximale
Menace sur les serveurs causant une compromission	• Concurrent • Virus informatique • Personnel peu sérieux	3. Forte
Menace sur les serveurs causant une Altération	• Personnel peu sérieux • Virus informatique • Panne électrique	3. Forte
Menace sur les serveurs causant une Diffusion	• Personnel peu sérieux • Cyber-attaque • Personnel inattentif	2. Significative
Les outils de messagerie		
Menace sur les outils de messagerie causant une Diffusion	• Personnel peu sérieux • Cyber-attaque	1. Minime

Source : Ebios

b) Evaluation des scénarios de menaces à la vraisemblance

L'importance relative des scénarios de menaces précédemment analysés (identifiés et estimés) est évaluée de la façon suivante (cf. critères de gestion des risques) :

Tableau 17: Evaluation des scénarios de menaces à la vraisemblance

Vraisemblance	Scénarios de menaces
4. Maximale	▪ Menace sur le service RH causant une indisponibilité ▪ Menace sur les serveurs causant une indisponibilité
3. Forte	▪ Menace sur le service RH causant une compromission ▪ Menace sur les serveurs causant une compromission ▪ Menace sur les serveurs causant une Altération ▪ Menace sur les administrateurs informatiques causant une compromission
2. Significative	▪ Menace sur le service RH causant une indisponibilité ▪ Menace sur les serveurs causant une Diffusion ▪ Menace sur les administrateurs informatiques causant une Diffusion
1. Minime	▪ Menace sur le service RH causant une Altération ▪ Menace sur le service RH causant une Falsification ▪ Menace sur le service RH causant une Diffusion ▪ Menace sur les outils de messagerie causant une Diffusion ▪ Menace sur les administrateurs informatiques causant une indisponibilité

Source : Ebios

4. Etude des risques

a) Analyse des risques

Nous avons établi la liste des risques à partir des événements redoutés et des scénarios de menaces précédemment appréciés.

La gravité et la vraisemblance ont été estimées, sans, puis avec, les mesures de sécurité.

- R1 : Risques liés à l'indisponibilité des données de vacations
- R2 : Risques liés à la compromission des données des vacations qui doivent rester intègre
- R3 : Risques liés à l'indisponibilité du logiciel Morpheus
- R4 : Risques liés à la compromission des données de la paie qui doivent rester intègre
- R5 : Risques liés à la diffusion des salaires qui doivent rester privé
- R6 : Risques liés à l'indisponibilité des dossiers du personnel
- R7 : Risques liés à l'altération des dossiers du personnel

Tableau 18: Mesures existantes appliquées aux risques

Mesure de sécurité existante	Bien support sur lequel elle repose	Prévention	Protection	récupération	Risques
Assurance multirisque professionnelle	La direction de l'IUC			X	R1, R3
Installation d'un antivirus	Windows 7	X			R1, R2, R3, R4
Alimentation secourue	Serveur d'application et base de données		X		R1, R2, R3, R4
Dispositif DMZ (zone démilitarisé)	Réseau		X		R1, R2, R3, R4, R5
Sauvegarde journalier	Disque dur			X	R1, R4
Classement des dossiers dans une armoire fermant à clé	Local service RH		X		R1
Consigne de fermeture à clé des locaux	Local service RH	X			R2, R4, R5, R6, R7
Journalisation des actions des utilisateurs	Serveur d'application	X			R2, R4
Serveur de secours	Serveur d'application et de base de données			X	R3
Contrôle d'accès par mot de passe	Serveur d'application et base de données				R4
Extincteur	Local du service RH	X			R6
Dératisation	Local service RH		X		R6, R7

Source : Nous-même

b) Evaluation des risques

Les risques précédemment analysés (identifiés et estimés) peuvent être évalués à l'aide du tableau suivant (les risques rayés correspondent à ceux réduits par des mesures de sécurité existantes) :

Tableau 19: Evaluation des risques

Gravité	4- Critique	• Risques liés à la diffusion des salaires qui doivent rester privé	• Risques liés à la diffusion des salaires qui doivent rester privé	• Risques liés à la compromission des données de la paie qui doivent rester intègre	
	3- Important	• Risques liés à l'indisponibilité du logiciel Morpheus • Risques liés à l'altération des dossiers du personnel	• Risques liés à l'indisponibilité du logiciel Morpheus	• Risques liés à la compromission des données des vacations qui doivent rester intègre	• Risques liés à l'indisponibilité du logiciel Morpheus
	2- Limitée	• Risques liés à l'indisponibilité des données de vacations • Risques liés à l'indisponibilité des dossiers du personnel	• Risques liés à l'indisponibilité des données de vacations		• Risques liés à l'indisponibilité des données de vacations
	1- Négligeable				
		1- Minime	2-Significative	3-Forte	4-Maximale
	Vraisemblance				

Source : Ebios

Dans cette section, nous nous sommes attelés à évaluer la sécurité du système d'information des ressources humaines. Nous avons identifié de manière générale quelques menaces, ainsi que les risques liés à celui-ci.

Ce chapitre nous a permis d'évaluer l'application Morpheus, de prendre connaissances des menaces et des risques liés au système d'information des ressources. Et les recommandations pour réduire ces risques font l'objet du chapitre suivant.

CHAPITRE IV : RESULTATS DE L'AUDIT ET RECOMMANDATIONS

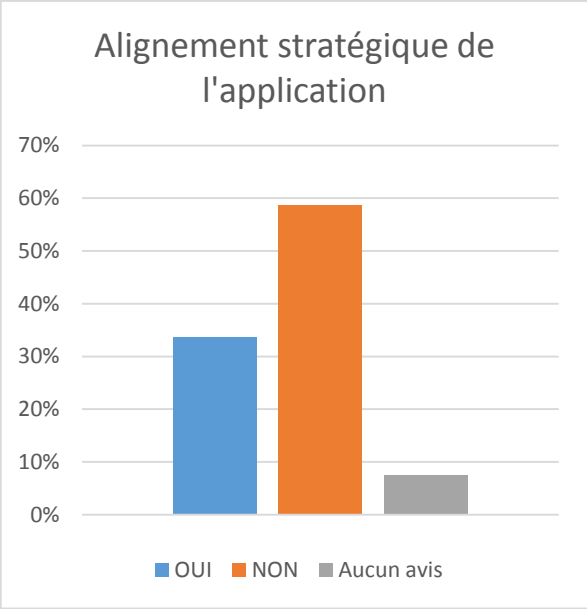
L'objectif de ce chapitre est de proposer des recommandations pour la mise en place d'un système d'information de gestion des ressources humaines de qualité, permettant à cette fonction de créer de la valeur ajoutée dans les entreprises.

SECTION I. Les résultats de l'audit de l'application et recommandations

1. Alignement stratégique de l'application

Tableau 20: Réponse au questionnaire sur l'alignement stratégique de l'application

	Réponses		
Questions	OUI	NON	Aucun avis
AL1	6	2	2
AL2	4	6	
AL3	1	8	1
AL4		9	1
AL5	1	7	2
AL6	5	5	
AL7		10	
AL8	10		
Total	27	47	6



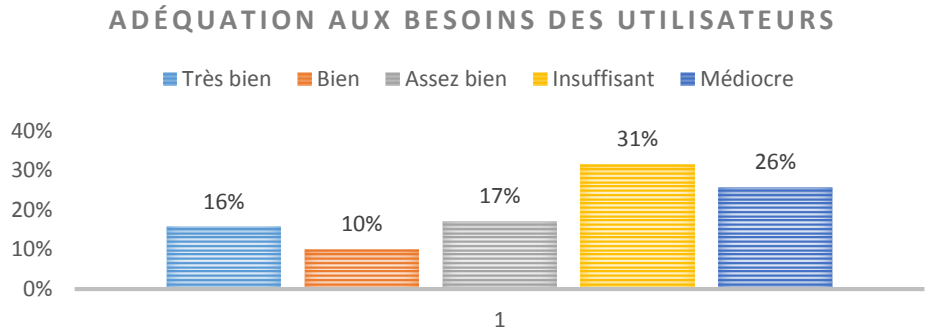
Source : Nous-mêmes

Au regard du graphique ci-dessus exprimant l'avis des parties prenantes de l'application, nous pouvons dire que l'application ne s'aligne pas sur la stratégie du service RH. Cela est surtout dû à l'absence de certaines fonctionnalités essentielles pouvant faciliter la gestion des ressources humaines.

2. Évaluation de l'adéquation aux besoins des utilisateurs :

Tableau 21: Réponse sur le questionnaire d'adéquation aux besoins

	Réponses				
Questions	Très bien	Bien	Assez bien	Insuffisant	Médiocre
AD1			3	5	2
AD2	2	2	3	2	1
AD3			1	7	2
AD4		3	3	3	1
AD5					10
AD6	4	2	2	1	1
AD7	5			4	1
Total	11	7	12	18	17

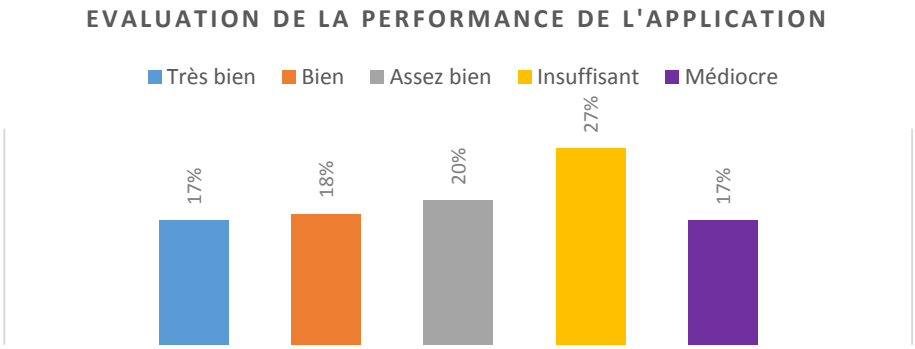


D'après le graphique, les utilisateurs de l'application estiment que les processus RH implémentés ne sont pas satisfaisants. Car certains processus sont encore externalisés ; ce qui engendre un double travail.

3. Audit de performance

Tableau 22: Résultat Questions sur les performations de l'application

	Réponses				
Questions	Très bien	Bien	Assez bien	Insuffisant	Médiocre
AP1			1	5	4
AP2	1	2	4	2	1
AP3			1	2	7
AP4		1	1	5	3
AP5	1	1	3	4	1
AP6	7	2	1		
AP7			1	8	1
AP8	6	2		1	1
AP9	1	3	5	1	
AP10		4	3	2	1
Total	19	20	22	30	19



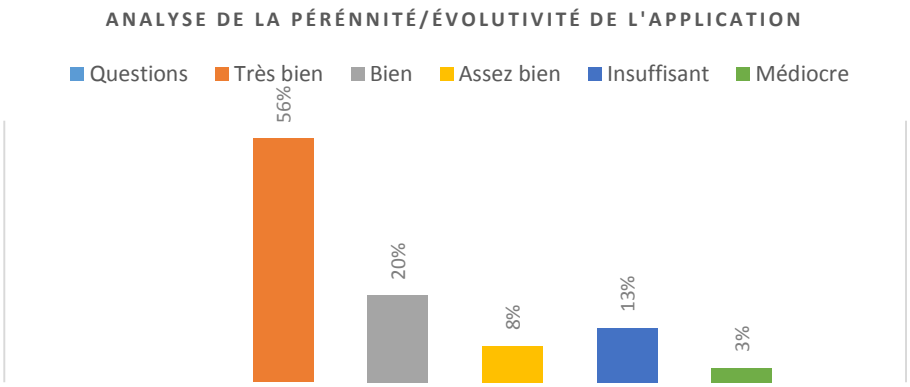
La performance de l'application reste insuffisante du fait que beaucoup de bug sont présent dans lors de l'utilisation de l'application.

Il n'existe pas de procédure formelle permettant de remonter les erreurs, ni guide utilisateur.

4. Analyse de la pérennité/évolutivité de l'application

Tableau 23: Résultat sur la pérennité et l'évolutivité de l'application

	Réponses				
Questions	Très bien	Bien	Assez bien	Insuffisant	Médiocre
E1	7	3			
E2	8	2			
E3	6	3	1		
E4	7	3			
E5	2	2	3	2	1
E6	7	3			
E7	6	2		2	
E8	4	3	2	1	
E9	10				
E10	10				
E11		2	2	5	1
E12		1	2	5	2
Total	67	24	10	15	4



La pérennité et l'évolutivité sont bien notées du fait que l'application est toujours en cours de développement.

5. Les recommandations

Selon le référentiel CObIT 5, la mise en œuvre de la vision stratégique doit être planifiée, communiquée et gérée selon différentes perspectives. Il recommande dans le processus « Planifier et Organiser » pour assurer l'alignement stratégique la mise en place d'une organisation adéquate ainsi qu'une infrastructure technologique ; afin de s'assurer :

- Le service utilise toutes les ressources de l'application
- Que tout le monde comprend l'objectif de l'application
- Les risques informatiques sont compris et gérés
- La qualité des systèmes informatiques est adaptée aux besoins métiers

Pour permettre à l'application de répondre aux besoins des utilisateurs, l'équipe de développement doit mettre en place le manuel utilisateur pour faciliter, la compréhension et la prise en main du logiciel.

Pour garantir la performance de l'application, l'on doit mettre en place des indicateurs de performance.

Le tableau RACI (Responsable, Acteur, Consulté, Informé), suivant est proposé au responsable de la cellule de développement logiciel afin que les utilisateurs soient informé des rôles dans son équipe, car lorsqu'une erreur survient l'utilisateur ne sait généralement pas vers qui se tourner.

Taches	Responsable	Acteur	Consulté	Informé
Développement fonctionnalité				
Gestion des bugs et incident				
Gestion de la maintenance				
Gestion des mises à jour				

Il a été également recommandé au responsable de la cellule de développement la mise en place d'un planning des mises à jours des fonctionnalités, afin qu'elles soient testées avant le début des taches relatives à la paie

Il est recommandé à l'équipe en charge de l'application Morpheus de mettre en place un système de reporting de bug ouvert à tous les utilisateurs pour qu'ils puissent remonter le plus rapidement possible les bugs et que les correctifs puissent suivre. Nous recommandons pour cela l'utilisation de MANTIS BUG TRACKER (https://www.mantisbt.org) qui est une solution open source.

Afin de garantir la sécurité et la fiabilité, un ensemble de bonnes pratiques doivent être appliquées à savoir :

- Définir clairement le rôle de chaque utilisateur,
- Produire un manuel pour l'administration de l'application
- Définir une politique d'identification forte permettant d'assurer une protection d'accès efficace (7 caractères minimum, gestion de l'historique des mots de passe sur 2 ans, contrôle de « trivialité », changement trimestriel des mots de passe,)
- Limiter les tentatives de connexion et les journaliser
- Définir clairement la procédure de gestion des incidents et des urgences

SECTION II. Mesures de sécurité du système d'information

Le tableau suivant présente les mesures de sécurité destinées à réduire ou transférer les risques.

Ces mesures de sécurité ont été déterminées dans l'objectif de couvrir différents éléments des risques à traiter (vulnérabilités, menaces, sources de menaces, besoins de sécurité ou impacts), d'aborder la plupart des thèmes de l'ISO 27002, de couvrir les différentes lignes de défense (prévention, protection et récupération), et ont été optimisées bien support par bien support.

Les risques identifiés sont les suivants :

- R1 : Risques liés à l'indisponibilité des données de vacations
- R2 : Risques liés à la compromission des données des vacations qui doivent rester intègre
- R3 : Risques liés à l'indisponibilité du logiciel Morpheus
- R4 : Risques liés à la compromission des données de la paie qui doivent rester intègre
- R5 : Risques liés à la diffusion des salaires qui doivent rester privé
- R6 : Risques liés à l'indisponibilité des dossiers du personnel
- R7 : Risques liés à l'altération des dossiers du personnel

Tableau 24: Mesures de sécurité recommandées

Mesure de sécurité existante	R1	R2	R3	R4	R5	R6	R7	Bien support sur lequel elle repose	Thème ISO 27002	Prévention	Protection	récupération
Interdiction d'accès aux locaux à toute personne (dont le personnel de nettoyage) sans la présence de membres du personnel					X	X	X	Local service RH	9.1. Zones sécurisées	X	X	
Pose de barreaux aux fenêtres		X		X	X		X	Local service RH	9.1. Zones sécurisées	X	X	
Dispositifs de lutte contre l'incendie	X	X	X	X	X	X	X	Local service RH	9.1. Zones sécurisées	X	X	
Activation d'une alarme anti-intrusion durant les heures de fermeture	X	X	X	X	X	X	X	Local service RH	9.1. Zones sécurisées	X	X	
Consignes de fermeture à clef des locaux		X		X	X		X	Local service RH	9.2. Sécurité du matériel	X	X	
Chiffrement des fichiers liés à la paie à l'aide de certificats électroniques	X	X		X				Local service RH	7.1. Responsabilités relatives aux biens		X	
Installation d'un antivirus sous Windows 7	X	X	X	X				Windows 7	10.4. Protection contre les codes malveillant et mobile	X		
Contrôle d'accès par mot de passe sous Windows 7	X	X	X	X				Windows 7	11.5. Contrôle d'accès au système d'exploitation	X		
Installation d'un antivirus sur les serveurs	X	X	X	X				Serveur d'application et de base de données	10.4. Protection contre les codes malveillant et mobile			X
Test trimestriel des fichiers sauvegardés				X				Serveur d'application et base de données	10.5. Sauvegarde			X
Journalisation des événements informatiques (accès, erreurs…)			X					Serveur d'application et base de données	10.10. Surveillance	X		
Restriction des accès nécessaires pour la maintenance					X			Serveur d'application et base de données	11.6. Contrôle d'accès aux applications et à l'information		X	
Mise en place d'un système RAID logiciel	X							Serveur d'application et base de données	12.2. Bon fonctionnement des applications		X	X
Gestion des vulnérabilités sur les serveurs			X					Serveur d'application et base de données	12.6. Gestion des vulnérabilités techniques	X		

Mise à jour régulière de l'antivirus des serveurs et de sa base de signatures			X					Windows 7	10.4. Protection contre les codes malveillant et mobile		X	
Sauvegarde hebdomadaire sur des disques USB stockés dans un meuble fermant à clef	X			X				Disque Dur	10.5. Sauvegarde			X
Alimentation secourue	X		X					Serveur d'application et base de données	9.2. Sécurité du matériel		X	
Élaboration d'une politique de sécurité de l'information	X	X	X	X	X	X	X	La direction de l'IUC	5.1. Politique de sécurité de l'information	X	X	X
Révision de la politique de sécurité de l'information au moins une fois par an	X	X	X	X	X	X		La direction de l'IUC	5.1. Politique de sécurité de l'information	X	X	X
Signature d'un engagement de confidentialité par les personnels	X	X	X	X	X	X		La direction de l'IUC	8.1. Avant le recrutement	X		X
Assurance multirisque professionnelle et sur les matériels informatiques				X				La direction de l'IUC	14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité			X

Ce chapitre, nous a permis de présenter les résultats et les recommandations permettant dans une première phase d'améliorer l'intégration du logiciel Morpheus dans le système d'information des ressources humaines. Dans une seconde phase, d'améliorer la sécurité du système d'information des ressources humaines.

CONCLUSION

Les objectifs de cette étude étaient d'apprécier le niveau d'intégration de l'application Morpheus dans le service des ressources humaines de l'Institut Universitaire de la Côte; de documenter le niveau de vulnérabilité du système d'information des ressources humaines de l'Institut Universitaire de la Côte par rapport aux différentes menaces afin de proposer des pistes d'amélioration. Cela à travers l'évaluation de l'effectivité et de l'efficacité des mesures mises en place par l'Institut Universitaire de la Côte pour répondre aux critères de disponibilité d'intégrité et de confidentialité du système d'information des ressources humaines.

En effet, pour répondre aux questionnaires attachés à cette étude, nous nous sommes intéressés aux notions théoriques liées au système d'information des ressources humaines, à l'audit des systèmes d'information. Par la suite, nous avons passé en revue l'application Morpheus qui est l'ERP utilisé au service des ressources humaines, les pratiques liées à la sécurité du système d'information des ressources humaines à l'Institut Universitaire de la Côte.

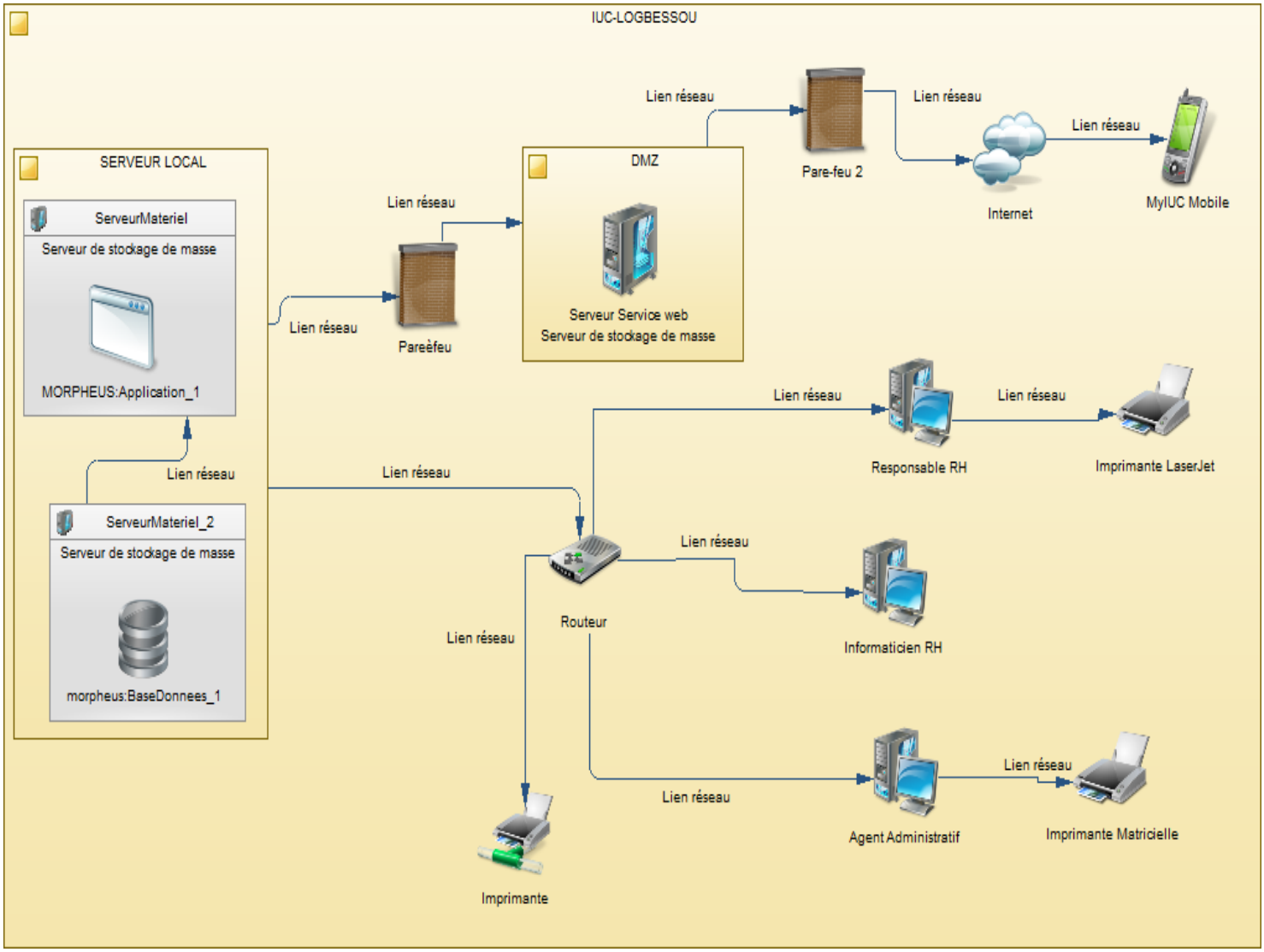
Ainsi, après évaluation des différents que nous avions définis, il ressort que l'Institut universitaire de la Côte pour permettre à l'application Morpheus de s'aligner sur la stratégie du service des ressources humaines doit automatiser toutes les fonctions essentielles des RH. En ce qui concerne la sécurité du système d'information, les risques liés à l'activité du service des ressources humaines, sont maîtrisés, mais comme on ne peut connaitre à l'avance toutes les menaces et toutes les vulnérabilités, il est recommandé de mettre en place une politique de sécurité, de mener un audit au moins tous les deux (02) ou trois (03) ans.

Notre travail, n'a pas été sans difficulté, car il était difficile de faire comprendre à certaines personnes que leur travail doit être passé en revue afin de déterminer les forces et faiblesses. De plus, nous avons eu de nombreux report de rendez-vous.

A l'issue de ce travail, nous avons pris conscience des responsabilités qui incombent aux auditeurs, et surtout que l'auditeur doit toujours se faire accompagner d'une expertise lorsqu'il n'as pas la compétence. Et enfin, notre étude s'étant limité au système d'information des ressources humaines, une évaluation de la sécurité des autres systèmes d'information serait également un atout considérable.

ANNEXES

<u>Annexe 2</u> : Cartographie du SIRH



Annexe 3 : Questionnaire de prise de connaissance des RH

Auditeur : CHEBOU CHOUPE Gabriel	**Objet du questionnaire et de l'entretien** : Prise de connaissance du service des ressources humaines		Entité : RH-IUC Référence : QPC_SIRH_1 Date :
Rédigé par : CHEBOU CHOUPE Gabriel	Complété par :		Validé par :
Personnes concernées	**fonction**	**Informé**	**Présent à l'entretien**
Personnes rencontrées			
Membre de l'équipe d'audit			
Superviseur			
Questions		Réponses des audités	
1. Présentation des interlocuteurs et du service			
Interlocuteur(s) : fonction ancienneté dans le service ; Expérience ou pratiques antérieures			
Avec qui travaillez-vous de manière habituelle sur les questions de RH ?			
Quels sont aujourd'hui les sujets les plus sensibles en matière de RH ?			
Quels sont les enjeux de la GRH à court et moyen terme dans votre structure?			
De quels outils disposez-vous pour piloter la RH : • à court terme ? • à moyen terme ?			
Disposez d'un tableau de bord ? Si oui, le communiquer à la mission. et le présenter rapidement.			
Disposez d'une cartographie des risques de service ? Si oui, la communiquer. Si oui, quel est le plan d'action associé ? Fournir le document correspondant.			
En l'absence de cartographie, quels sont à votre avis, les risques les plus importants liés à l'activité de votre service ? Parmi eux, quels sont ceux qui vous paraissent maîtrisés, pourquoi et comment ? Quels sont les risques les moins bien maîtrisés et pourquoi ?			
2. PRESENTATION DES COMPETENCES DU SERVICE			
Quels sont les domaines de compétences de votre service ?			
Certains domaines de compétences sont-ils partagés avec d'autres services ? Si oui, quels domaines et avec quels services?			

Certaines attributions RH sont-elles partagées avec d'autres directions ? Si oui, quelles attributions et avec quelles directions?	
Comment vos compétences se coordonnent-elles avec la direction budgétaire s'agissant notamment de la définition du volume des effectifs et de la masse salariale associée?	
3. PRESENTATION DES RESSOURCES DU SERVICE	
Comment votre service est-il organisé ? Fournir les organigrammes et les textes correspondants.	
Comment les personnels du service se répartissent-ils entre les différentes composantes du service ? Pourquoi cette organisation a été retenue (nombre d'opérations à traiter absence d'outils de gestion,..) ? Existe-t-il des fiches de poste pour tout ou partie des personnels ?	
Quels sont les profils de compétence que vous recherchez pour ces différents postes, notamment pour l'encadrement?	
Les agents de votre service bénéficient-ils de formations à la prise de poste et/ou d'actions de formation continue Si oui, sur quels sujets majeurs ? Qui organise la formation pour les agents de votre service?	
4. PERSONNELS GERES ET PERSPECTIVES D'EVOLUTION	
Disposez-vous d'un plan GPEEC et d'un plan d'action associé ? Les communiquer	
Etes-vous confronté(e) à une problématique de fort renouvellement des effectifs dans les prochaines années ? Si oui, sur quels types d'activités et/ou de compétences ?	
En fonction de l'évolution des missions, des activités ou de l'environnement de la direction, y-a-t-il une problématique liée à la nécessité de disposer de nouveaux profils de compétences dans les prochaines années ? Quelles mesures envisagez-vous de mettre en œuvre dans ce contexte ?	
Informations supplémentaires utiles à la mission :	

Annexe 4 : Questionnaire de prise de connaissance du SIRH

Auditeur : CHEBOU CHOUPE Gabriel	**Objet du questionnaire et de l'entretien** : Prise de connaissance du système d'information des ressources humaines		Entité : RH-IUC Référence : QPC_SIRH_2 Date :
Rédigé par : CHEBOU CHOUPE Gabriel	Complété par :		Validé par :
Personnes concernées	**fonction**	**Informé**	**Présent à l'entretien**
Personnes rencontrées			
Membre de l'équipe d'audit			
Superviseur			
Questions		Réponses des audités	
1. Présentation des interlocuteurs et du service			
Interlocuteur(s) : grade, fonction ancienneté dans le service ; Expérience ou pratiques antérieures			
Positionnement dans le service			
2. Le Système d'Information des RH : Fonctions informatisées			
Quelles sont les fonctions RH qui sont informatisées : • Recrutement : • Formation • Gestion administrative : mutations, avancement, promotions, positions administratives, mise à la retraite ? • Paye (ou préparation des fichiers paye) ? • Frais de missions/déplacements ? • Gestion des temps travaillés : congés, horaires variables, temps partiels … • Gestion des risques professionnels ? • Paye (ou préparation des fichiers paye) ? • Frais de missions/déplacements ? • Gestion des temps travaillés : congés, CET, horaires variables, temps partiels … • Gestion des risques professionnels ?			
Parmi ces fonctions informatisées, quelles sont celles qui sont accessibles : • aux agents en consultation ou en saisie ? • aux personnes extérieures à la direction en consultation ou en saisie ?			
3. L'architecture du Système d'Information des RH			
Quelles sont les interfaces entre ces applications ? (Quelles sont les applications qui communiquent entre elles ?) Commentaire du Schéma d'urbanisation s'il a été fourni.			
4. PROGICIEL INTEGRE			
La direction utilise-t-elle un progiciel intégré ? Si non, passer à la rubrique suivante. Si oui, lequel ? Depuis quand ?			

Pour quelles fonctions ? Qui en assure le paramétrage? Qui assure la maintenance et la mise à jour des évolutions ? Si le progiciel a remplacé une application plus ancienne, comment l'historique des données a-t-il été renseigné ou repris ? Quels contrôles ont-ils été effectués lors de la recette de l'application pour s'assurer de la qualité de la reprise de l'historique ?	
Certaines fonctions sont-elles gérées par d'autres applications ? Si oui, lesquelles ? Qui les a réalisées ? Qui en assure la maintenance ? Comment ces différents modules communiquent-ils entre eux ? Le cas échéant, des interfaces existent- elles avec d'autres applications ?	
Existe-t-il une assistance utilisateurs ? Assurée par qui ? Les demandes transmises par les utilisateurs ont-elles permis de détecter des bugs ? Comment ont-ils été corrigés ?	
Comment les agents ont-ils été formés au progiciel lors de sa mise en service ?	
Comment les agents nouvellement affectés sont-ils formés au progiciel ?	
5. LOGICIELS PRODUITS EN INTERNE	
Le service utilise-t-il des applications qui lui sont propres ? Qui les a réalisées ? Comment sont-elles maintenues ? Des interfaces existent-elles entre tout ou partie de ces applications ? Le cas échéant, des interfaces existent-elles avec d'autres applications ?	
Quelle est l'ancienneté de ces applications ? Y-a-t-il des risques liés : • à l'obsolescence des outils de programmation et/ou d'exploitation ? • à la perte de compétences fonctionnelles dans les équipes de la DSI ? • aux limites de l'application qui rendent son évolution difficile ? Si oui, pour quelles applications ?	
Si une ou plusieurs applications viennent d'être mises en service en remplacement d'applications antérieures, comment l'historique des données a-t-il été renseigné ou repris ?	
Quels contrôles ont-ils été effectués lors de la recette de l'application pour s'assurer de la qualité de la reprise de l'historique ?	
Si de nouvelles applications ont informatisé des fonctions gérées manuellement, comment l'historique (données des périodes antérieures) est-il géré ?	
La programmation prévisionnelle du SI prévoit-elle des évolutions relatives au SI-RH dans les prochaines années ? Si oui, lesquelles ?	
Quels risques sont-ils anticipés au titre de ces changements ? Des actions spécifiques sont-elles prévues ? déjà mises en œuvre? Fournir la documentation correspondante	
Pour préparer ces évolutions, les utilisateurs sont-ils associés à la définition des fonctionnalités du SIRH ? Dans ce cadre, ont-ils formulé des demandes en termes de : rôles et profils, gestion des droits et des habilitations associées, • contrôles applicatifs : bloquants, non bloquants	

• autres? Ces demandes ont-elles été prises en compte en totalité ou en partie ? Le cas échéant, expliquez pourquoi certaines demandes n'ont pas été prises en compte. Fournir les comptes rendus des réunions correspondantes, s'ils existent	
L'évolution prévue du SIRH s'accompagnera-t-elle d'une modification de l'organisation du travail des agents ? Si oui, quelles sont les actions prévues (et/ou déjà engagées°) en matière de conduite du changement ?	
Le SI produit-il de manière périodique : • des restitutions ? • des tableaux de bord ? Si oui, quels en sont destinataires ? Comment les utilisez-vous ? Fournir la documentation correspondante	
Le SI alimente-t-elle un Infocentre ? Si oui, quelle est la fréquence de mise à jour des données ? Existe-t-il des restitutions prédéfinies ? Si oui, lesquelles ? Est-il possible d'élaborer des requêtes spécifiques ? Si oui, de quelle manière ?	
Le SI permet-il de connaître à un instant « T », la répartition des effectifs suivant des critères définis ?	
Le SI permet-il de produire automatiquement l'ensemble des données rendues obligatoires pour la production du bilan social ? Si non, quelles sont les données qui font l'objet d'une collecte spécifique et/ou de retraitements manuels ou sur des outils bureautiques ?	
Autres éléments que vous souhaitez porter à la connaissance de la mission :	

Annexe 5 : Questionnaire de contrôle interne du service RH

NB : Ce questionnaire est un questionnaire général qui s'adresse plutôt au responsable de la fonction RH notamment dans sa première partie. En fonction du périmètre et du thème de l'audit, il peut être décliné auprès des responsables des différentes unités et services qui interviennent dans le processus RH (a priori, ce sont plutôt eux qui peuvent répondre au volet « identification des pratiques de maîtrise des risques »).

NA* : Non Appliqué

Auditeur : CHEBOU CHOUPE Gabriel	**Objet du questionnaire et de l'entretien** : Contrôle interne du système d'information des ressources humaines		Entité : RH-IUC Référence : QCI_SIRH_1 Date :
Rédigé par : CHEBOU CHOUPE Gabriel	Complété par :		Validé par :
Personnes concernées	**fonction**	**Informé**	**Présent à l'entretien**
Personnes rencontrées			
Membre de l'équipe d'audit			
Superviseur			

Présentation des interlocuteurs et du service	
Interlocuteur(s) : grade, fonction ancienneté dans le service ; Expérience ou pratiques antérieures	
Positionnement dans le service	

Présentation des interlocuteurs et du service	
Interlocuteur(s) : grade, fonction, ancienneté dans le service : Expérience ou pratiques antérieures	
Positionnement dans le service	

Questions	Réponses des audités			
	OUI	NON	NA *	Commentaires
1. CARTOGRAPHIE DES RISQUES ET PLAN DE MAITRISE DES RISQUES				
Disposez-vous d'une cartographie des processus RH ? Si oui, produire la documentation correspondante et en faire une rapide présentation.				
Quels sont les objectifs associés à ces processus ?				
DISPOSITIF DE CONTROLE INTERNE FORMALISE				
Existe-t-il une cartographie des risques RH ?				

Si oui, comment s'articule-t-elle avec la cartographie des processus ? Si non, passer directement à la rubrique : dispositif de contrôle interne non formalisé				
Quel est son périmètre : o cartographie des risques partielle ? o cartographie globale ? Couvre-t-elle les risques informatiques ou ceux-ci sont-ils traités de manière spécifique ?				
Comment a-t-elle été élaborée ?				
A qui a-t-elle été diffusée ?				
Qui est responsable de sa mise à jour ?				
Existe-t-il un plan d'action destiné à maîtriser les risques détectés ? Si oui, produire ce document.				
A quelle fréquence, évaluez-vous la mise en œuvre de ce plan et sur quelle base ?				
Disposez-vous d'indicateurs qui vous permettent d'évaluer l'efficacité des mesures prises ? Si oui, lesquels ?				
DISPOSITIF DE CONTROLE INTERNE NON FORMALISE				
En l'absence de cartographie des risques, quels sont à votre avis les points forts et les points faibles de la direction ?				
Quelles sont les missions/tâches les plus sensibles ?				
Quels sont les risques de dysfonctionnement les plus importants ?				
Avez-vous donné des orientations à vos collaborateurs pour prévenir ces dysfonctionnements/risques? Si oui, lesquelles ? En ce cas, comment suivez-vous la mise en œuvre de ces orientations ?				
IDENTIFICATION DES PRATIQUES DE MAITRISE DES RISQUES EXISTANTES				
Comment les agents accèdent-ils à la documentation règlementaire ?				
Comment la veille juridique est-elle organisée ?				
Quelle est la procédure suivie en cas de novation règlementaire importante ?				
Existe-t-il des guides ou outils similaires à la disposition des agents ?				
Disposez-vous de : • délégations de pouvoirs ? • délégations de signatures ?				

D'autres cadres ou agents disposent-ils de délégations de signatures ?				
Quel est la procédure suivie en cas de mutation d'un agent disposant d'une délégation de signature ?				
Quel est la procédure suivie en cas d'absence d'un agent disposant d'une délégation de signature ?				
Pour les processus informatisés, existe-t-il un système de signature électronique ? Si oui, pour quelles attributions ?				
A défaut, quelle est l'articulation entre signature manuelle et validation informatique ?				
Intervenez-vous dans le dispositif de gestion des habilitations informatiques pour : • l'ouverture des droits d'accès aux applications RH ? • l'attribution de profils en fonction des responsabilités, délégations dont disposent les agents ? Si oui, quel est votre rôle ? Si non, qui assure la gestion des habilitations ?				
Qui est responsable du contrôle des habilitations et notamment qui vérifie que les habilitations dont disposaient les agents quittant la DRH ou changeant d'attributions sont supprimées?				
Vos services rencontrent-ils des difficultés dans l'utilisation des applications RH : • du fait de l'indisponibilité des applications ? • du fait des limites de l'application (obligation de procéder à des traitements manuels complémentaires) ? • du fait de la persistance d'anomalies dans le traitement ?				
Quelles sont les procédures existantes pour assurer la qualité des données saisies dans les applications ?				
Disposez-vous d'indicateurs : • réclamations des agents, • contentieux, • autres ?				Si oui, les remettre à la mission.
Avez-vous constaté un manque de fiabilité de certaines données ?				
Autres éléments que vous souhaitez porter à la connaissance de la mission				

Annexe 6 : Questionnaire de contrôle interne (QCI)

NA* : Non Appliqué

Auditeur : CHEBOU CHOUPE Gabriel	**Objet du questionnaire et de l'entretien** : Contrôle d'efficacité et de performance de l'application	Entité : RH-IUC Référence : QCI_SIRH_2 Date :
Rédigé par : CHEBOU CHOUPE Gabriel	Complété par :	Validé par :

Présentation des interlocuteurs et du service				
Interlocuteur(s) : Grade : Fonction : ancienneté dans le service : Expérience ou pratiques antérieures				
Positionnement dans le service				
Questions	Réponses des audités			
	NON	OUI	NA*	Commentaire
Audit d'efficacité et de performance: **Évaluation de l'alignement stratégique de l'application :**				
AL1- Le projet s'inscrit-il dans le schéma-directeur du système d'information et ce dernier est-il aligné avec le schéma directeur du service?				
AL2-Existe-t-il une maîtrise d'ouvrage « forte » et impliquée ;				
AL3-Le service a-t-il participé à l'étude préalable et a validé le projet et notamment l'analyse coûts/bénéfices ;				
AL4-Le cahier des charges de l'application prend-t-il en compte tous les aspects du problème posé et du domaine fonctionnel considéré ?				
AL5-Le projet s'intègre-t-il de façon satisfaisante dans le système d'information existant (intégration technique et fonctionnelle) ?				
AL6-Les utilisateurs ont-ils été suffisamment associés à la définition des spécifications ou au choix de la solution puis aux évolutions successives ?				
AL7-Les utilisateurs réalisent-ils toutes leurs tâches dans l'application (évaluation du taux d'automatisation des opérations) ?				
AL8-Sinon, maintiennent-ils des systèmes parallèles (ancien système, tableurs) en dehors de l'application ? Existe-t-il des saisies multiples ?				
Adéquation aux besoins des utilisateurs :				

AD1-L'ergonomie de l'application est-elle satisfaisante ? AD2-Par exemple, la saisie d'une transaction récurrente est-elle suffisamment productive (nombre d'écrans optimisé, saisie assistée, temps de réponse acceptable, …) ?					
AD3-les rapports issus du système répondent-ils convenablement aux besoins des utilisateurs ? En particulier chaque niveau de management dispose-t-il de l'information qui lui est nécessaire (adéquation à l'organisation) ?					
AD4-Le support utilisateur (technique et fonctionnel) est-il satisfaisant et adapté aux utilisateurs et aux enjeux ?					
AD5-La documentation utilisateur est-elle adaptée, complète, accessible et permet-elle une utilisation optimale de l'application ?					
AD6-la formation des utilisateurs est-elle suffisante, adaptée et périodique, notamment pour une activité où le « turn-over » est important ?					
AD7-existe-t-il des enquêtes périodiques de satisfaction auprès des utilisateurs ? À l'aide ou non de ces enquêtes, évaluer le niveau de satisfaction des utilisateurs (performance de l'application, appropriation et maîtrise, qualité de la formation et du support, absence de phénomène de rejet, ...) ?					
	Tes biens	Bien	Assez-bien	Insuffisant	Médiocre
1. Audit d'efficacité et de performance : analyse de la performance					
AP1-La réduction des charges (notamment de personnel et d'exploitation) et/ou des délais (délais de traitements, délais de clôture, …) est-elle conforme à la réduction attendue lors de l'étude préalable ?					
AP2-A-t-on constaté des améliorations non quantifiables, définies ou pas lors de l'étude préalable (amélioration de la sécurité, du service client, ...) ?					
AP3-A-t-on réalisé une réingénierie des processus (Business Process Reengineering (BPR) ou une étude d'organisation préalablement à la rédaction du cahier des charges ?					
AP4-Les processus métiers sont-ils performants et optimisés (rechercher toute source d'amélioration possible) ?					
AP5-Les traitements sont-ils performants et les données cohérentes et fiables (voir guide d'audit « Fiabilité et Sécurité d'une application ») ?					
AP6-L'architecture technique est-elle adaptée et optimisée, notamment les bases de données (bon dimensionnement des configurations, gestion des évolutions techniques, personnalisation (tuning) des bases de données, …) ?					
A-t-on mis en place des indicateurs de performance et un contrat de service adaptés aux enjeux entre l'informatique et les utilisateurs : AP7-disponibilité de l'application, le cas échéant par plage horaire					

AP8-gestion des incidents et du support utilisateurs, fiabilité des traitements par lots (batch) ;					
AP9-gestion des demandes de maintenance et gestion des droits d'accès ;					
AP10-continuité d'exploitation et site de back-up.					
2. Audit d'efficacité et de performance : analyse de l'évolutivité/pérennité de l'application					
E1-Les technologies utilisées sont-elles conformes aux standards de l'organisation ?					
E2-Le logiciel est-il de conception récente et fondé sur des technologies portables, non obsolètes et évolutives (matériel, OS, SGBD, outils de développements, …) ?					
E3-Les technologies utilisées sont-elles matures et suffisamment répandues sur le marché (Linux, J2EE, .net,..) ?					
E4- Les compétences existent-elles sur le marché notamment dans le contexte d'un déploiement à l'international ?					
E4-Les technologies utilisées ont-elles suffisamment de marge pour faire face à un nombre croissant d'utilisateurs et de transactions?					
E5-L'application est-elle techniquement et fonctionnellement intégrée dans le SI ?					
L'application est-elle modulaire, paramétrable et conceptuellement adaptée aux éventuelles évolutions de l'activité, notamment : E6-capacité d'adaptation à une internationalisation (multilingue, multidevise et multi protocole, ...)?					
E7-capacité d'intégrer une nouvelle entité juridique, un nouveau produit, un nouveau métier, … ?					
E8-capacité de « filialiser » un métier de l'Organisation ou de décentraliser certaines activités ?					
E9-capacité d'un déploiement massif (client léger versus client lourd, ...) ?					
E10-L'application évolue-t-elle régulièrement par versions successives ?					
E11-Le volume des demandes de maintenance évolutive est-il « normal » (en fonction de l'âge de l'application) et de maintenance corrective « raisonnable » (20-25% max de la maintenance dans les 2 premières années) ?					
E12-Dispose-t-on d'un engagement ou d'une visibilité suffisante de la pérennité du progiciel (notamment en cas de gel des évolutions ou de l'état technique) ?					

Annexe 7 : Questionnaire de contrôle interne (QCI)

NA* : Non Appliqué

Auditeur : CHEBOU CHOUPE Gabriel	**Objet du questionnaire et de l'entretien** : Contrôle de la sécurité et de la fiabilité de l'application	Entité : RH-IUC Référence : QCI_SIRH_3 Date :
Rédigé par : CHEBOU CHOUPE Gabriel	Complété par :	Validé par :

Présentation des interlocuteurs et du service				
Interlocuteur(s) : Grade : Fonction : ancienneté dans le service : Expérience ou pratiques antérieures				
Positionnement dans le service				
Questions	Réponses des audités			
	NON	OUI	NA*	Commentaire
2. Audit de la sécurité et de la fiabilité : analyse des risques associés à l'organisation				
Existe-t-il un comité informatique, présidé par la direction générale et au sein duquel les directions utilisatrices sont représentées et influentes (stratégie, contrôle et pilotage,..) ?		x		
Existe-il, au sein de l'organisation, une « politique » relative aux applications, connue, partagée et mise en œuvre : ▪ couvrant l'ensemble du cycle de vie de l'application (conception, exploitation) ; ▪ favorisant la responsabilisation et l'appropriation par les utilisateurs de leur système d'information ? ▪ La notion de « propriété » d'application est-elle utilisée ?	x			
	x			
	x			
Le rôle et les responsabilités des utilisateurs vis-à-vis de l'application sont-ils clairement identifiés ?	x			
Couvrent-ils l'analyse des risques, la définition des besoins de sécurité, la gestion des changements et des évolutions, l'administration de l'application ?	x			
A-t-il été réalisé une analyse des risques, spécifique à l'application, qui a débouché sur la définition des besoins de sécurité (classification formelle des données et des traitements en termes de disponibilité, d'intégrité et de confidentialité) ?	x			
Dans le prolongement de l'analyse des risques et de l'expression des besoins de sécurité, a-t-il été mis en	x			

œuvre un contrat de service (SLA) entre l'informatique et la direction utilisatrice ?				
Existe-il un manuel d'administration de l'application, à jour et maîtrisé, comprenant notamment : mode d'emploi du manuel, présentation du module d'administration de l'application, droits d'accès « type » par poste, procédure de création / modification / suppression de droits d'accès, responsabilité d'autorisation, mode opératoire, documentation des pistes d'audit et nature des contrôles à réaliser,	x			
L'administration est bien assurée par les utilisateurs ?		x		
Le « propriétaire » dispose-t-il d'un compte-rendu (reporting) mensuel « intelligible » de la performance de l'application, dans le respect du contrat de service ?		x		
Existe-il un guide utilisateurs / manuel de procédures, diffusé, à jour et maîtrisé, comprenant notamment : ▪ mode d'emploi du manuel, présentation de l'application, mode opératoire, règles de gestion, écrans et zones de saisie, liste des messages d'erreurs, états de contrôle et d'exception, documentation des pistes d'audit ; ▪ description des contrôles programmés et des contrôles manuels compensatoires à chaque phase du traitement (mode opératoire, procédure d'escalade et/ou de recyclage des anomalies, délais de mise en œuvre, …).	x x			Pas pour tous les modules
3. Audit de la sécurité et de la fiabilité : Analyse des risques associés à l'application				
L'accès aux ressources de l'application (données et transactions) est-il restreint par un système de gestion d'accès ?		x		
Existe-t-il une procédure de gestion des profils utilisateurs de l'application placée sous la responsabilité du propriétaire de l'application (procédure de création / modification et suppression des droits d'accès) ?		x		
Chaque utilisateur possède-t-il un identifiant qui lui est propre ?	x			
Existe-t-il des comptes génériques pour accéder à l'application?	x			
Le mot de passe associé à l'identifiant permet-il d'assurer une protection d'accès efficace (7 caractères minimum, gestion de l'historique des mots de passe sur 2 ans, contrôle de « trivialité », changement trimestriel des mots de passe, etc.) ?	x			

Les tentatives de connexions infructueuses à l'application sont-elles enregistrées et contrôlées par le propriétaire de l'application?	x			
Les tentatives de connexions infructueuses à l'application sont-elles limitées ?		x		
L'accès aux données et aux transactions de l'application peut-il être correctement paramétré en fonction des tâches des utilisateurs ou le système de confidentialité est-il basé sur le contrôle d'accès aux données ?		x		
La séparation des tâches est-elle respectée dans le paramétrage des profils ? ▪ comparer les droits d'accès avec les fonctions des utilisateurs ; ▪ vérifier l'adéquation entre les droits et les profils ; ▪ vérifier que toutes les personnes ayant des droits d'accès sont toujours dans le service / l'organisation.	x			
La piste d'audit sur le système d'administration de l'application est-elle assurée et régulièrement contrôlée ?			x	
Tous les documents servant de base à la saisie sont-ils préparés, préformatés, complets et approuvés avant saisie ?		x		
Les facilités de saisie, l'ergonomie de la saisie, les messages écrans et les contrôles de format sur les données permettent-ils d'éviter puis de filtrer les erreurs de premier niveau ? Y-a-t-il unicité de la saisie de l'information ?		x		
Les contrôles de validation permettent-ils de détecter les doubles saisies, les saisies incomplètes, les incohérences (contrôle de vraisemblance et de rapprochement avec d'autres valeurs, contrôle de limite et d'étendue,…) et certaines erreurs de saisie (contrôle de sommation, totaux de contrôle pour les saisies de masse) ?		x		
Utilise-t-on des « brouillards » de saisie pour validation par réconciliation avec les documents sources ?		x		
Cette validation est-elle indépendante ?		x		
Les saisies des données « sensibles » et notamment les données permanentes et les paramètres de l'application sont-elles autorisées, complètes et exactes ?		x		
Les opérations effectuées sur des données sensibles sont-elles l'objet d'une piste d'audit suffisante et régulièrement analysée ? ▪ identité de l'auteur de l'opération ;		x		

▪ entité / fichier /donnée sur laquelle l'opération a été effectuée ; ▪ date et heure des événements ; ▪ valeur avant et après l'opération. Objectifs de contrôle de la piste d'audit : ▪ évaluation de la qualité des pistes (couverture, exploitabilité, …) ; ▪ évaluation de la sécurité des pistes (sécurité de ses constituants : OS, SGBD, ...) ; ▪ évaluation de la gestion des pistes (procédures de contrôle, archivage, …).				
Les procédures de transmission de fichiers en entrée assurent-elles l'exhaustivité et l'exactitude des informations transmises (contrôles systèmes) ?		x		
Les contrôles mis en œuvre lors de l'intégration des données par fichiers à l'application sont-ils suffisants et identiques à ceux mis en œuvre dans le cadre d'une saisie transactionnelle (contrôles applicatifs) ?	x			
Le système prévoit-il de conserver toutes les données rejetées dans un fichier d'anomalies protégé et de les éditer en vue d'un contrôle et d'un recyclage ?			x	
Les données rejetées sont-elles analysées et corrigées dans des délais raisonnables et compatibles avec les délais de validation des traitements ?		x		
Les corrections des données rejetées subissent-elles les mêmes contrôles que les données initiales, et jouissent-elles d'une piste d'audit suffisante ?		x		
Toutes les opérations de mise à jour des données sensibles sont-elles journalisées (transactions, traitements batch) ?	x			
Rapproche-t-on les totaux de contrôle de fin de journée et la différence est-elle analysée au travers des transactions journalisées ?				
Des contrôles automatiques périodiques, notamment de vraisemblance, sont-ils effectués afin de vérifier l'intégrité des montants gérés par l'application (niveau applicatif ou base de données) ?		x		
La couverture, le contenu et la distribution des états de sortie de l'application sont-ils adaptés aux enjeux et à l'organisation de l'organisation ?			x	
Effectuer une revue détaillée des états disponibles et de leur destinataire et vérifier que chaque nouvel état de sortie fait l'objet d'une procédure de recette.		x		
Chaque utilisateur dispose-t-il du bon niveau d'information et de moyen de contrôle adapté ?		x		

La distribution des états de sortie est-elle sous contrôle (existence d'une procédure permettant l'identification et la validation formelle des destinataires) et leur niveau de confidentialité assuré ?		x		
Les contrôles utilisateurs des états de sortie font-ils l'objet de procédures formalisées (guide de procédures), connues et appliquées ?	x			
Les procédures de validation des résultats (Qui, Quand, Comment), de classement et d'archivage des états produits sont-elles adaptées, formalisées, connues et appliquées ? existence d'une procédure, identification des responsables, délai de mise à disposition des états et délai de validation, procédures à suivre en cas d'incident.		x		
Lorsque l'application est la juxtaposition de plusieurs modules, l'homogénéisation des codifications et des règles de gestion a-t-elle été assurée ?		x		
L'intégrité et l'exhaustivité des données transmises entre les différents modules de l'application et/ou à des applications en aval sont-elles assurées ?				
4. Audit de la sécurité et de la fiabilité : analyse des risques associés à la fonction informatique				
Au sein du service informatique, les tâches relatives au développement et à l'exploitation de l'application sont-elles séparées ? ▪ Prendre connaissance de l'organigramme de la DSI, des descriptions de travaux (Job description) et de la procédure de mise en production.		x		
L'accès aux bibliothèques de production (données et programmes) est-il interdit aux analystes-programmeurs ? ▪ Sans réelle étanchéité des environnements de développement et de production, la séparation des tâches reste toute théorique. Analyser les droits d'accès. Un accès en lecture pour les chefs de projets est généralement admis		x		
La séparation des tâches est-elle maintenue et assurée en cas d'absence d'un salarié (maladie, vacances,..) ?		x		
L'équipe actuelle en charge de la maintenance (interne ou externe) a-t-elle une maîtrise suffisante de l'application et les moyens de la faire évoluer ?		x		Les moyens sont insuffisants
Existe-t-il une procédure formalisée et standard de maintenance de l'application validée par l'informatique et la maîtrise d'ouvrage concernée ?	x			

Les nouvelles versions (développement interne, progiciel) sont-elles systématiquement testées puis recettées dans un environnement dédié avant d'être livrées à l'exploitation ?		x		
Existe-t-il une procédure formalisée de transfert des programmes entre les environnements de recette et d'exploitation ?		x		
La documentation de l'application est-elle systématiquement mise à jour après chaque intervention de maintenance ?	x			
Les corrections effectuées en urgence sur les programmes sont-elles effectuées dans un cadre bien défini et formalisé ?		x		
Font-elles l'objet d'un rapport systématiquement revu par la direction informatique ?		x		
Un logiciel de contrôle de programmes sources et de programmes exécutables est-il utilisé pour identifier et tracer toute modification effectuée?		x		
Les travaux batch de l'application, qu'ils soient périodiques ou à la demande, sont-ils systématiquement planifiés et formellement validés par le responsable d'exploitation et par le responsable utilisateur ?			x	Pas de travaux batch
Existe-t-il une procédure de contrôle des traitements batch et d'archivage des comptes rendus d'exécution ?			x	
La gestion des incidents en général et les procédures d'urgence en particulier sont-elles définie et correctement documentées ?	x			En cours de documentation
La documentation d'exploitation est-elle à jour, dupliquée, protégée et inclut-elle les procédures de gestion des incidents et de reprise / redémarrage ?	x			En cours d'élaboration
Vérifier l'existence et l'application d'un Contrat de Service (SLA) pour l'application :	x			
Est-ce que le SLA couvre les besoins de disponibilité, d'intégrité et de confidentialité de l'application et de ses données ;	x			
Vérifier que les moyens organisationnels (ex : escalade, astreintes, procédures et reporting, ...), humains (effectif, compétences des personnels), matériels et logiciels (ex: architecture redondante, outil de mesure, ...) permettent le respect des engagements de service et la mesure rigoureuse du niveau de service.				
Évaluer le niveau de service par l'analyse des tableaux de bord.				
Les procédures de sauvegarde et de reprise de l'application sont-elles satisfaisantes et répondent-elles aux enjeux de l'application et aux engagements de service de l'informatique ?		x		

Une partie des sauvegardes est-elle stockée à l'extérieur de l'organisation (banque, société spécialisée) selon une périodicité adaptée aux enjeux ?		x		
En cas de sinistre grave, existe-t-il un plan de secours en adéquation avec les besoins et les enjeux (plan d'urgence, plan de repli, plan de reprise) ? ▪ vérifier le dimensionnement des moyens mis en place; ▪ déterminer les faiblesses du plan de secours existant (axes d'analyse : étude d'impact financier, sites de repli, plan de secours informatique, plan de secours télécom, sauvegardes des documents, procédures, organisation, logistique).		x		
Ce plan est-il périodiquement testé et mis à jour ?		x		
L'organisation dispose-t-elle d'un responsable sécurité et d'une politique formalisée en matière de sécurité informatique, conforme à la réglementation ?		x		
Cette politique couvre-t-elle la fonction informatique ?		x		
Les accès aux commandes système, aux bibliothèques et bases de données de production sont-ils protégés (logiciel de contrôle) et limités au personnel d'exploitation ?		x		
Les accès aux logiciels de base et utilitaires sensibles sont-ils contrôlés et systématiquement "tracés" ?		x		
Existe-t-il des procédures de contrôle périodique des accès aux ressources de l'application (analyse des « logs 6 » par le responsable de la sécurité) ?			x	Voir DSI

REFERENCES BIBLIOGRAPHIQUES

ANGOT, H. (2005). *Système d'information de l'entreprise: Des flux d'information au système d'information de gestion automatisé* (éd. 5e). Bruxelles: De Boeck.

DAYAN, & Armand. (2008). *Manuel de Gestion* (éd. 2e, Vol. I). Paris: Ellipses/AUF.

DORIATH , B., LOZATO, M., MENDES, P., & NICOLLE, P. (s.d.).

GILLET, M., & GILLET, P. (2010). *Système d'information des ressources humaines.* Paris: Dunod. Consulté le 2017

KOVACH, K., & CATHCART, C. (1999). "Human Ressource Information Systems (HRIS): Providing Business with Rapid Data Acces, Information Exchange and Stratégic Advantage". *In Public Personnel Management*, 275.

LAUDON, K., LAUDON, J., FIMBEL, E., & COSTA, S. (2013). *Management des systèmes d'information* (éd. 11e). Paris: Pearson.

MONACO, L. (2014). *Systèmes d'information de gestion* (éd. 3). Paris: Gualino.

Organisation internationale de normalisation. (s.d.). *Catalogue des normes.* Consulté le 12 04, 2017, sur ISO.org: https://www.iso.org/fr/standard/54533.html

REIX, R., FALLERY, B., KALILA, M., & ROWE, F. (2011). *Systèmes d'information et management des organisations* (éd. 6e). Paris: Vuibert Editions.

Silva, F. (2008). *Etre e-DRH: Postmodernité - Nouvelles technologies - Fonctions RH* (éd. 2e). (W. Kluwer, Éd.) France: LIAISONS.

TRAVAUX CITES

Direction Générale de l'Offre Santé. (2013, Janvier). Guide méthodologique pour l'auditabilité des SI. *Fiabilisation et certification des comptes des établissements publics de santé*. France. Consulté le Décembre 2017

REFERENCES WEB

adullact.net. (s.d.). *projects/ebios2010*. Consulté le 12 06, 2017, sur https://adullact.net/projects/ebios2010/

ANOR. (2015, Avril). Catalogue des normes Camerounaise. Consulté le 08 26, 2017, sur http://www.anorcameroun.info/documents/catalogue_des_normes.pdf

ANTIC. (s.d.). *Audit de Sécurité des Systèmes d'Informations*. (Agence Nationale des Technologies de l'Information et de la Communication) Consulté le 12 02, 2017, sur www.antic.cm: https://igf.cm/index.php/fr/component/k2/item/315-security-audit.html

Barbezat, M. (2011). *outils et référentiels d'audit informatique*. Consulté le 12 03, 2017, sur mindmeister.com: https://www.mindmeister.com/fr/66316990/outils-et-r-f-rentiels-d-audit-informatique

IFACI. (s.d.). *Audit des contrôles applicatifs.* Consulté le Novembre 04, 2017, sur www.ifaci.com: http://www.ifaci.com/bibliotheque/bibliotheque-en-ligne-telecharger-la-documentation-professionnelle/referentiel-international-de-l-audit-interne/acces-par-composante-du-cadre-de-reference/guides-pratiques-gtag-global-technologies-audit-guide/gtag-8-n-aud

IFACI. (s.d.). *Referentiel-international-de-l-audit-interne/guides-pratiques-ctag-211*. Consulté le 12 06, 2017, sur ifaci.org: https://membres.ifaci.com/Bibliotheque/Bibliotheque-en-ligne-telecharger-la-documentation-professionnelle/Referentiel-international-de-l-audit-interne/guides-pratiques-ctag-211.html

ISACA. (s.d.). *COBIT 4.1: Cadre de gouvernance et de contrôle informatique.* Consulté le Novembre 05, 2017, sur www.isaca.org: http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx

ISACA. (s.d.). *COBIT et les contrôles d'application: un guide de gestion.* Consulté le Novembre 04, 2017, sur www.isaca.org: https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-and-Application-Controls-A-Management-Guide.aspx

ISACA. (s.d.). *Normes de vérification et d'assurance des SI.* Consulté le Novembre 05, 2017, sur www.isaca.org: http://www.isaca.org/Knowledge-center/Standards/Documents/1201_std_French_1113.pdf

Organisation internationale de normalisation. (s.d.). *Catalogue des normes.* Consulté le 12 04, 2017, sur ISO.org: https://www.iso.org/fr/standard/54533.html

wikipedia l'encyclopédie . (2017, Août 25). *Audit_informatique.* Consulté le Septembre 24, 2017, sur librefr.wikipedia.org: https://fr.wikipedia.org/wiki/Audit_informatique

Table des matières