MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

ÉCOLE NATIONALE SUPÉRIEURE DE MANAGEMENT ENSM

Pôle Universitaire de KOLÉA

Mémoire présenté comme exigence partielle pour l'obtention du diplôme de Master en Management Stratégique et Systèmes d'Information

Thème :

Essai d'élaboration et d'application d'une procédure d'audit des systèmes d'information pour se conformer à la norme ISO/IEC 20000
Cas : Condor Electronis

Élaboré par : LEGHLAM Randa Lamis

BOUDISSA Hanane

Encadré par : Dr TOUMI Djamila

2022 /2023

Résumé

Ce travail vise à développer une procédure d'audit des systèmes d'information et à la mettre en œuvre pour se conformer à la norme ISO/CEI 20000 pour la direction des systèmes d'information de Condor Electronics à Bordj Bou Arreridj. Pour ce faire, une approche qualitative a été adoptée, incluant des entretiens semi-directifs et une analyse approfondie des documents pertinents. Les informations recueillies lors des entretiens, ainsi que les observations et les analyses des documents à l'aide de l'analyse SWOT, ont été cruciales pour déterminer les domaines essentiels à auditer. Les résultats de l'audit permettent d'identifier les non-conformités du système d'information et de proposer des pistes d'amélioration afin d'accroître la fiabilité et l'efficacité du système.
Mots clés : Audit des systèmes d'information, Audit interne, ISO/CEI 20000.

Abstract

This work aims to develop an information systems auditing procedure and implement it to comply with the ISO/IEC 20000 standard for the Information Systems Department of Condor Electronics in Bordj Bou Arreridj. To achieve this, a qualitative approach was adopted, which included semi-structured interviews and an in-depth analysis of relevant documents. The information gathered during the interviews, along with observations and analyses using the SWOT analysis, were crucial in determining the essential areas to be audited.

The audit results enable the identification of information system non-conformities and propose improvement measures to enhance the reliability and efficiency of the system.
Keywords: Information system audit, Internal audit, ISO/CEI 20000.

ملخص

يهدف هذا العمل إلى تطوير إجراء تدقيق نظم المعلومات وتنفيذ للامتثال للمعايير ISO / IEC 20000 لقسم نظم المعلومات بشركة كوندور للإلكترونيات ببرج بوعريريج. لتحقيق ذلك ، تم اعتماد نهج نوعي ، والذي تضمن مقابلات شبه منظمة و تحليل متعمق للوثائق ذات الصلة. كانت المعلومات التي تم جمعها أثناء المقابلات ، إلى جانب الملاحظات والتحليلات باستخدام تحليل SWOT ، حاسمة في تحديد المجالات الأساسية التي يجب تدقيقها.

تمكن نتائج التدقيق من تحديد عدم مطابقة نظام المعلومات واقتراح إجراءات التحسين لتعزيز موثوقية وكفاءة النظام.
الكلمات المفتاحية: تدقيق نظم المعلومات ، المراجعة الداخلية ، ايزو/اي اي سي 20000.

REMERCIEMENT

Je tiens tout d'abord à exprimer mes sincères remerciements à Allah, qui m'a accordé la grâce et la persévérance pour mener à bien ce projet de thèse. Sa guidance et sa bénédiction ont été essentielles tout au long de ce parcours.

Je tiens à adresser mes plus sincères remerciements à ma directrice de thèse, Madame Djamila Toumi, pour son encadrement précieux et ses conseils éclairés. Son expertise et son soutien indéfectible ont été récupérés à la réussite de cette thèse.

Je suis infiniment reconnaissant envers mon responsable de stage Mohammed Fouad pour son soutien inestimable et son assistance précieuse. Sa connaissance approfondie et ses conseils avisés ont été d'une importance cruciale.

Je souhaite exprimer ma profonde gratitude à ma chère famille, en particulier à ma mère et à mon père, pour leur amour inconditionnel et les sacrifices qu'ils ont consentis pour moi. Leur présence constante et leurs encouragements ont été une source inépuisable d'inspiration et mes frères, Imad, Anis, et Adam

Je tiens également à rendre hommage à mon frère jumeau, Wassim (Rahmatou allahi alayh), dont la mémoire demeure une source d'inspiration pour moi. Sa force et son courage continuent de m'inspirer chaque jour. J'aurais tant souhaité qu'il soit ici avec moi pour partager cette réalisation.

Enfin, j'aimerais exprimer ma profonde gratitude envers ma binôme consentie et talentueuse, Hanane Boudissa. Notre collaboration et notre travail d'équipe ont été d'une importance capitale dans la réussite de cette thèse.

À toutes les personnes qui ont reçu de près ou de loin à la réalisation de ce travail, j'adresse mes sincères remerciements. Votre soutien a été d'une valeur inestimable et a joué un rôle majeur dans cette réalisation académique.

REMERCIEMENT

En préambule à ce mémoire je remercie ALLAH le tout puissant, qui nous a aidé et nous a donné la force, la patience et le courage durant ces longues années d'études.

Je tiens également à exprimer ma gratitude à mon encadreur M. Djamila TOUMI pour son aide, sa disponibilité et son intérêt pour mon travail de recherche.

Je remercie très respectueusement mon tuteurs Mr. Mouhamed Fouad qui ont aussi contribué à la réalisation de ce travail en me donnant toutes les informations nécessaires et m'avoir accordé leur temps précieux au sein de l'entreprise Condor ELECTRONICS.

J'exprime mes sincères gratitudes à Messieurs les jurys qui nous font l'honneur de juger ce travail.

Je remercie aussi tous les enseignants que nous avons eu le plaisir d'avoir durant notre formation à L'École Nationale Supérieure de Management.

Pour finir, soyons reconnaissant aux personnes proches qui nous entourent.

Un remerciement spécial et sincère à nos chers parents et grands-parents pour leur amour inconditionnel et leur soutien durant tout mon parcours universitaire.

Je leur serai toujours reconnaissant pour la personne que je suis aujourd'hui. Sans oublier mon frère ARAFA et mes sœurs IMANE ,ZAINEB et bien sûr mes cousines surtout HAKIMA.

Je remercie ma collègue RANDA LAMIS LEGHLAM et tiens à vous exprimer ma sincère gratitude pour votre collaboration et votre aide précieuse tout au long de notre travail ensemble.

Je remercie tous mes amis pour leur aide et soutien.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

SI: Système d'information.

CAAT : Techniques d'audit assistées par ordinateur.

ERP: Enterprise ressource planning

EPP : Entreprises publiques et parapubliques.

CRIPP : Cadre de référence internationale des pratiques professionnelles ;

IFACI : l'institut Français de l'Audit et du Contrôle Internes ;

IT : Information Technology ;

ITSM : Information Technology Service Management ;

SMI : Système de Management Intégré ;

RSGSI : Responsable Standards & Gouvernance SI ;

RSSI : Responsable de sécurité des systèmes d'information ;

S&MD : Support et Master Data SI ;

E&D :Etude et Développement ;

INFRA: Infrastructure ;

GLPI : Gestionnaire Libre de Parc Informatique ;

COBIT: Control Objectives for Information and related Technology ;

ITIL : Information Technology Infrastructure Library ;

ISO : Organisation internationale de normalisation ;

CMMI: Capability Maturity Model Integration;

ISSAI : The International Standards of Supreme Audit Institutions;

CRM : Client Relationship Management ;

IFACI : Institut Français de l'Audit et du Contrôle Interne ;

SAP : SAP Software Solutions .

LISTE DES ANNEXES

INTRODUCTION

Introduction

Les technologies de l'information (TI) sont devenues un aspect vital des opérations des entreprises dans tous les secteurs d'activité dans le paysage technologique en pleine expansion d'aujourd'hui. Étant donné que les organisations s'appuient largement sur les systèmes et services informatiques pour générer de la valeur et atteindre leurs objectifs stratégiques, une gouvernance et une gestion efficaces de ces systèmes sont devenues essentielles. Dans ce contexte, les entreprises s'efforcent d'aligner leurs services informatiques sur les meilleures pratiques et normes internationales, telles que ISO/IEC 20000, qui donne des orientations pour la gestion des services informatiques (ITSM).

Condor Electronics, une entreprise technologique de premier plan, comprend l'importance d'adopter des normes internationales afin d'améliorer ses compétences en matière de prestation de services informatiques. La société espère améliorer sa fourniture de services informatiques, la satisfaction de ses clients et ses performances commerciales globales en se conformant à la norme ISO/IEC 20000.

Le DSI de Condor Electronics est chargé de fournir et de gérer les services informatiques à l'échelle de l'entreprise. Avec la complexité et la pertinence croissantes de l'infrastructure informatique, il est devenu essentiel de développer un système de gestion des services informatiques solide qui offre une fourniture de services de haute qualité. La norme ISO 20000 spécifie les meilleures pratiques et les normes de gestion des services informatiques, en mettant l'accent sur la conception, la transition, la livraison et l'amélioration des services.

Notre étude approfondie vise à élaborer une procédure d'audit des systèmes d'information (SI) et à la mettre en œuvre en conformité avec la norme ISO 20000 au sein de la Direction des Systèmes d'Information (DSI) de Condor Electronics. Dans cette optique, la présente recherche s'attache à répondre à la question principale suivante: Comment **développer une procédure d'audit du système d'information (SI) pour se conformer à la norme ISO 20000 et comment l'appliquer de manière adéquate ?**

Et les questions secondaires suivants :

-Quelles sont les principales étapes de la mise en place d'une procédure d'audit des systèmes d'information pour se conformer à la norme ISO 20000 ?

-Quels sont les outils et les techniques les plus appropriés pour mener à bien l'audit des systèmes d'information pour se conformer à la norme ISO 20000 ?

Introduction

-Comment élaborer cette mission d'audit du système d'information (SI) pour se conformer à la norme ISO 20000 en suivant cette procédure ?

-Quelles sont les recommandations pour documenter et rapporter les résultats de l'audit des systèmes d'information pour se conformer aux exigences de la norme ISO 20000 ?

Pour répondre à cette problématique, nous avons utilisé une méthode qualitative comprenant des entretiens semi-directifs et une recherche documentaire incluant la consultation de documents pertinents.

L'objectif de ce projet est de créer une procédure pour effectuer un audit SI dans le service informatique de Condor Electronics pour se conformer à la norme ISO 20000. Le protocole englobe tous les aspects du processus d'audit, tels que la planification, le travail sur le terrain et les rapports. L'approche sera conçue pour garantir que l'audit est effectué de manière systématique et complète, en évaluant tous les composants essentiels de l'infrastructure informatique et des processus de gestion des services.Et pour s'exercer davantage et s'assurer de la réussite de cette mission d'audit IT, il est possible de réaliser une mise en œuvre concrète.

Le choix de notre thème s'est inspiré du constat que la DSI de Condor Electronics n'avait jusqu'alors jamais réalisé de méthode d'audit du système d'information ISO 20000. Cela dénote un manque de structure et de critères précis pour évaluer le système d'information de l'entreprise pour se conformer aux exigences de la norme ISO 20000. Dans ce contexte, le développement d'une procédure d'audit adaptée à cette norme aiderait le service informatique de Condor Electronics à se conformer aux normes et à assurer une meilleure qualité de service IT pour l'ensemble de l'entreprise.

Pour le choix de l'entreprise Condor plusieurs facteurs ont influencé le choix du la direction de système d'information de Condor Electronics. Pour commencer, Condor Electronics est une entreprise bien connue dans l'industrie électronique, ce qui en fait une option intéressante pour une mission d'audit. De plus, le fait que leur DSI n'ait pas mis en place la procédure d'audit ISO 20000 est une opportunité de contribuer à améliorer leurs pratiques et à les aligner sur les standards mondiaux. En sélectionnant la DSI Condor Electronics, on obtient un exemple concret de la création de la procédure d'audit SI.

Notre mémoire est structuré en trois (03) chapitres Le premier chapitre sera dédié au cadre théorique et conceptuel. Nous commencerons par une revue de littérature qui exposera les

travaux antérieurs sur les audits des systèmes d'information en se référant à différents référentiels et normes. Dans un second temps, nous entreprendrons la définition de chaque concept étudié, en mettant en avant les éléments essentiels qui y sont liés. Le deuxième chapitre sera consacré au cadre méthodologique, où nous justifierons les choix méthodologiques qui ont été faits pour notre étude, Ensuite, dans le dernier chapitre, nous aborderons la partie pratique de notre étude. Nous détaillerons l'élaboration d'une procédure pour l'audit du système d'information, ainsi que la réalisation de cette mission d'audit. Ensuite, nous présenterons les résultats de l'audit obtenus et les recommandations qui en découlent.

CHAPITRE I :
REVUE DE LITTÉRATURE
ET
CADRE CONCEPTUEL

Ce premier chapitre est organisé en deux sections. Dans la première section, nous avons la présentation de la revue de littérature et on a une deuxième section sera consacrée à la présentation du cadre conceptuel de notre recherche et les principaux concepts, le modèle de recherche c'est les documents et l'observation pour nous aider dans le chapitre pratique.

SECTION 01: REVUE DE LA LITTÉRATURE

Le but de cette section est de rechercher différentes littératures portant sur l'audit des systèmes d'information.

1. Revue littérature de l'audit des systèmes d'information :

Selon l'article de (Oktania Purwaningrum, Baitun Nadhiroh, Siti Moukaromah, 2021) a pour objectif d'identifier les nouvelles connaissances sur le fait que l'audit des systèmes d'information est différent selon le niveau de maturité avec le cadre COBIT, Cette étude utilise une méthode de recherche en bibliothèque et est réalisée sur des articles scientifiques publiés dans des revues nationales ou des procédures en Indonésie. Ces articles doivent contenir le titre "Audit du système d'information" et avoir été publiés au cours des 10 dernières années.

Les résultats obtenus sont basés sur des objectifs de contrôle de chaque méthode. Actuellement, de nombreuses études utilisent l'audit de Système d'information mais aborde le niveau de maturité ou le modèle de maturité. Si D'après les liens de chaque composante de COBIT, on peut dire que l'audit des systèmes d'information diffère selon le niveau de maturité. Le niveau de maturité ou le modèle de maturité fait partie des étapes réalisées dans le processus d'audit vise à : Sensibiliser la direction informatique aux responsabilités internes maîtrise de l'informatique courante, s'assurer que les exigences de contrôle informatique existantes sont respectées devrait, optimiser et hiérarchiser les ressources informatiques, combler la gouvernance informatique.

Dans le processus d'audit du système d'information, plusieurs constats seront obtenus peut être utilisé par l'organisation concernant les raisons pour lesquelles les objectifs informatiques ne sont pas atteints.

Alors que le niveau de maturité ne produit qu'une valeur qui décrit la position de l'informatique pour soutenir les processus d'affaires de l'organisation.

Plusieurs études sous forme de revues ont été recherchées avec le titre "Audit du système d'information ". Sur les 10 revues obtenues, seulement 3 d'entre elles ont abordé le

processus d'audit complet du système d'information. Les 7 autres revues, bien qu'intitulées "Audit du système d'information", semblent discuter plutôt du niveau de maturité du système d'information.

A partir de cela, on peut conclure qu'il existe encore des différences dans les études portant sur le même titre "Audit du système d'information". Cette recherche devrait apporter de nouvelles connaissances afin d'orienter les recherches futures, notamment dans le domaine de l'audit des systèmes d'information. Les 10 revues ont été examinées pour pouvoir vérifier le contenu des revues. Sur 10 revues obtenues au hasard, 3 revues primées intitulées Information Systems Auditing et fait référence au processus d'audit du SI, tandis que les 7 autres connu sous le nom d'audit des systèmes d'information, mais n'aborde pas les niveaux de maturité discutez du processus de vérification. Cette étude devrait apporter de nouvelles connaissances sur le fait que les audits SI varient selon le niveau maturité, qui est également vérifiée dans le cadre COBIT 5.

2. Techniques de collecte de données sur l'audit des systèmes d'information à l'aide du cadre COBIT :

Selon l'article de (Putu Dhanu Driya,IGusti Lanang Agung Raditra Putra, IMade Ardwi Pradnyana,2021) a pour objectifs organisationnels, le processus d'atteinte des objectifs sera encore plus rapide. Cette étude vise à fournir une compréhension des techniques de collecte de données dans les audits de systèmes d'information avec le cadre COBIT et les aspects à prendre en compte dans le choix des techniques de collecte de données dans les audits de systèmes d'information avec le cadre COBIT.

Dans cette étude, les chercheurs ont utilisé des méthodes de recherche en bibliothèque, en se basant principalement sur des données secondaires. La méthode spécifique utilisée pour évaluer le sujet était une étude de la littérature, qui impliquait la recherche et l'analyse de 15 articles pertinents. Les données qui ont été obtenues sont ensuite compilées, analysées et conclues afin de tirer des conclusions concernant l'étude de la littérature. La recherche en bibliothèque peut être considérée comme une activité de recherche dans laquelle la collecte de données et d'informations est obtenue à l'aide de documents de bibliothèque tels que sous forme d' ouvrages de référence, de revues, d'articles, de comptes rendus liés au sujet de recherche La méthode d'étude de la littérature est une série d'activités concernant la collecte de données de bibliothèque, la lecture, l'enregistrement et le traitement des documents de recherche.

Les résultats obtenus sont le domaine Planifier et organiser contient des critères d'évaluation et de mesure qui comprend des indicateurs clés d'objectifs, des facteurs critiques de succès, des indicateurs clés de performance et des modèles de maturité. COBIT a pour objectif de permettre aux auditeurs de fournir plus facilement des recommandations d'amélioration aux organisations en termes d'amélioration de la gestion du système d'information dans le futur après notre recherche nous avons découvert le processus de réalisation d'un audit du système d' information se décompose en quatre étapes, à savoir : planification, préparation, mise en œuvre et rapport. Dans la phase de mise en œuvre, l'évaluation est effectuée à partir de données obtenues par diverses méthodes de collecte de données, telles que des entretiens, des observations et des enquêtes.

Et aussi nous avons découvert Sur la base des meilleures pratiques d'audit de système d'information (IT Governance Institute, 2004) et de la norme ISO 27002, les étapes d'un audit de système d'information sont généralement divisées en 3 étapes : planification et préparation, mise en œuvre de l'audit et rapport des résultats d'audit.

L'étape de planification et de préparation est l'étape initiale du processus d'audit.

Les résultats de cette étape permettront à l'auditeur de connaître les processus métier et informatiques de l'organisation, la portée et les objectifs qui ont été déterminés, ainsi que l'approche d'audit à suivre.

Au stade de la mise en œuvre, un audit du système d'information est réalisé pour tester l'adéquation et l'adéquation du système d'information d'une organisation. L'une des phases les plus importantes de cette étape est la phase de collecte de données ou de preuve.

Selon (Andry & Setiawan, 2019) et (Arisanti, 2011), si le niveau d'utilisation de l'informatique est élevé, il est conseillé d'utiliser un audit avec approche informatique à l'aide des techniques d'audit assistées par ordinateur (CAAT). La technique de collecte de données à COBIT 5 . en général nous pouvons conclure avant de commencer l'audit dans la section de collecte de données, il est préférable que l'auditeur détermine l'approche d'audit à mener, l'approche d'audit est divisée en trois, à savoir: Ordinateur, audit autour de l'ordinateur, audit avec l'ordinateur Les techniques de collecte de données dans les audits de systèmes d'information avec le cadre COBIT comprennent : des entretiens, des observations, des études de documents, des enquêtes. Les étapes d'un audit de système d'information sont généralement divisées en 3 étapes : Planification et préparation, Mise en

œuvre de l'audit et Rapport des résultats de l'audit. La détermination des techniques de collecte de données peut faire référence à la première étape de l'audit, à savoir la détermination de la portée de l'audit, ceci est très important étant donné que la collecte de données affecte toutes les étapes ultérieures de l'audit du système d'information, y compris en influençant les résultats de l'audit.

3.AUDIT INTERNE ET PERFORMANCE DES ENTREPRISES :

Selon l'article de (BEN BOUBAKARY, 2020) le but de cette étude était de saisir et d'examiner l'impact de l'audit interne. Avant de procéder au test des hypothèses, des analyses préliminaires ont été réalisées dans le cadre d'une méthode quantitative basée sur une enquête par questionnaire. Pour tester les hypothèses suivantes : selon la première hypothèse, les qualifications du principal dirigeant de la vérification auraient un effet bénéfique sur cette performance. La deuxième hypothèse suppose que la taille du service d'audit interne serait également associée à une performance financière améliorée. La troisième hypothèse suggère que les qualifications des auditeurs internes en particulier pourraient également influencer positivement la performance financière des EPP. La quatrième hypothèse, le niveau d'expérience des auditeurs internes aurait un effet positif sur cette performance. La cinquième hypothèse suppose que l'indépendance de l'audit interne serait également associée à une performance financière améliorée des EPP.

Une étude quantitative a été effectuée auprès d'un échantillon de 80 entreprises, ces analyses comprenaient notamment l'examen des corrélations entre les variables indépendantes, ainsi que le test d'égalité des paramètres des échantillons à l'aide du test du Khi-deux pour les variables nominales ou binaires.

Ces résultats soulignent encore une fois l'importance d'une qualification élevée pour ceux qui exercent ce métier, afin de pouvoir gérer efficacement tous les problèmes au sein de l'organisation. En effet, les auditeurs internes qualifiés contribuent à améliorer les performances de l'entreprise en leur permettant d'avoir une compréhension claire de la manière de gérer toutes les opérations et d'accomplir leur travail de manière optimale.

Nous pouvons conclure c'est que les autorités publiques du Cameroun sont conscientes de l'importance de l'audit interne pour aider les entreprises publiques à atteindre leur objectif de générer des profits, les résultats de l'étude ont confirmé les hypothèses H2, H3, H4 et H5, indiquant que la taille de l'audit interne, les qualifications et l'expérience des auditeurs ainsi que leur indépendance ont une influence positive sur la performance financière des

entreprises publiques du Cameroun EPP. En prenant en compte l'ensemble de ces facteurs, le risque d'un audit interne de mauvaise qualité serait réduit. Cela démontre l'engagement des autorités publiques camerounaises à améliorer la performance des entreprises qui sont touchées par les malversations financières et les contre-performances.

4. Le rôle de l'audit interne dans l'amélioration de la gouvernance d'entreprise :

Selon l'article de (Ziani Abdelhak, 2019) L'objectif de cette étude consiste à déterminer si l'audit interne peut jouer un rôle dans l'amélioration de la gouvernance d'entreprise. Pour ce faire, l'étude évaluera la capacité du système de contrôle interne à gérer les risques, à réduire l'asymétrie d'information et à protéger les droits des parties prenantes.

Une étude avec une enquête par questionnaire est analysée à l'aide d'une méthode quantitative une étude quantitative a été effectuée auprès d'un échantillon de 49 entreprises, et le modèle d'analyse est évalué à l'aide de différentes techniques telles que les pourcentages, le coefficient Alpha de Cronbach, le coefficient de corrélation, le test K-S à un échantillon et le T. Test de Student. les résultats indiquent que les personnes interrogées sont bien informées du nouveau rôle que doit jouer l'audit interne, qui est de garantir l'existence d'un système de contrôle interne efficace en surveillant les domaines critique : il est important de communiquer à l'administration toute forme de non-conformité dans le système de contrôle interne.

Cependant, lorsque ces non-conformités sont particulièrement graves, il est recommandé que l'auditeur prenne des mesures spécifiques et aussi que l'audit interne a pour responsabilité de surveiller et de signaler toute lacune dans le système de contrôle interne de l'entreprise. Si des problèmes ont été identifiés précédemment et ne sont pas encore résolus, l'audit interne doit prendre des mesures de suivi et en informer le conseil d'administration. Une fois que le conseil d'administration est conscient de ses responsabilités dans la mise en place du système de contrôle interne, l'audit interne doit également informer le conseil d'administration et la direction générale de toute lacune persistante qui nécessite une attention particulière. Selon les résultats du questionnaire portant sur le rôle de l'audit interne dans l'amélioration de la gouvernance d'entreprise en réduisant l'asymétrie d'information, les répondants ont indiqué que l'audit interne est considéré comme un outil efficace pour protéger les intérêts des actionnaires. Cela est accompli en garantissant la fiabilité des informations financières.

Les résultats liés à l'importance de la fonction d'audit interne dans la protection des droits des différentes parties prenantes. Les résultats indiquent que les garanties fournies par l'audit interne en matière d'intégrité, de qualité et de fiabilité des informations financières permettent aux parties prenantes de mieux comprendre la situation de leur entreprise, ce qui leur assure une satisfaction quant à sa performance. En d'autres termes, l'audit interne joue un rôle clé dans la transparence financière et contribue à renforcer la confiance des parties prenantes dans l'entreprise.

En conclusion, La revue souligne l'importance vitale de l'audit interne pour renforcer la gouvernance d'entreprise en Algérie. Les conclusions de l'étude indiquent que les personnes interrogées sont parfaitement conscientes de l'influence bénéfique de l'audit interne sur l'évaluation du système de contrôle interne, la gestion des risques, la réduction de l'asymétrie d'information et la défense des intérêts des parties prenantes.

5. Audit interne et gestion des risques opérationnels :

Selon l'article de (Younes EL KHATTAB, Younes ZOUHAIR, 2021) a pour objectif de consiste à faire un bilan de la performance de la fonction d'audit interne dans les organismes publics situés à Rabat (Maroc), en examinant sa capacité à gérer efficacement les risques opérationnels. Le procédé de recherche adopté dans cette étude est de nature hypothético-déductive et quantitative, s'appuyant sur un questionnaire avec échantillon de 40 établissements. Les informations recueillies ont été traitées à l'aide du logiciel SPSS, et le test du khi-deux a été utilisé afin de déterminer s'il y avait une dépendance entre les variables. En outre, pour approfondir l'analyse de la deuxième hypothèse, une régression logistique a été employée.

Après avoir étudié la relation entre l'audit interne et la contrainte de l'environnement, nous pouvons conclure que notre première hypothèse est invalidée. Il en ressort que la mise en place de la fonction audit interne ne dépend pas principalement de la turbulence et de l'incertitude de l'environnement.

Au contraire, la bonne gouvernance requiert la présence d'une fonction d'audit interne pour garantir un fonctionnement efficace et une gestion opérationnelle optimale. Suite à l'analyse des résultats, il est évident que la compétence et l'expérience professionnelle suffisante d'une équipe d'audit interne ont une influence positive sur la détection des zones à risques dans la plupart des établissements enquêtés. Par conséquent, cela confirme notre deuxième hypothèse formulée précédemment, à savoir que la compétence de l'équipe

d'audit interne joue un rôle crucial dans la maîtrise des risques liés aux différents processus, en validant cette hypothèse, nous concluons que pour assurer une maîtrise efficace du risque opérationnel, il est indispensable de disposer d'une équipe d'audit interne compétente et hautement qualifiée. Par conséquent, il est primordial d'investir dans la formation du personnel de la fonction audit interne, ce qui requiert une attention particulière. Étant donné que les établissements publics sont actuellement en train de se restructurer, certains d'entre eux n'ont pas encore mis en place un comité d'audit. Cependant, cela n'empêche pas l'audit interne de gérer efficacement les problématiques et les risques de l'organisme en matière de gestion des risques opérationnels. Le texte met l'accent sur l'influence du comité d'audit sur la fonction audit interne dans ce domaine.

Nous pouvons conclure que ces dernières années, l'audit interne au sein des institutions publiques de Rabat a considérablement progressé, en réponse à l'obligation légale et à l'exigence de bonne gouvernance et de bonne gestion.la vérification interne est aujourd'hui considérée comme l'outil le plus adapté pour atteindre les objectifs organisationnels tout en améliorant les processus de gestion des risques et de contrôle interne, Il est recommandé que les institutions publiques mettent en place un système de planification des ressources d'entreprise (ERP), investissent dans la formation régulière des auditeurs pour améliorer leurs compétences, et sensibilisent leurs employés à la culture de l'audit interne. Il est important de promouvoir une culture de vérification interne parmi les employés, afin que les auditeurs soient perçus comme des collaborateurs plutôt que des figures autoritaires, mais plutôt comme des aides qui aident l'établissement à atteindre les objectifs et à gérer les risques.

SECTION 2 : CADRE CONCEPTUEL

1- La notion de système d'information

1.1 Définition de système d'information :

Un SI comprend un ensemble complet et bien organisé d'éléments qui permettent de communiquer, acquérir, de traiter et de stocker la totalité des informations de l'organisation, sous forme de données, images, textes, sons, etc. Ce système inclut les logiciels, le matériel, les données, les procédures et le personnel, à l'intérieur ou à l'extérieur de celle-ci.

1.2 Les fonctions de système d'information :

Un SI comprend l'ensemble des composants qui permettent de gérer les informations qui se déroulent au sein de l'organisation. Ses rôles principaux sont les suivants :

Tableau 01: Les Fonctions De Système D'information

Collecte des données	• Les systèmes d'information doivent être alimentés par des données pour être utiles • Les données peuvent provenir de sources externes telles que les clients et les fournisseurs, internes à l'entreprise comme la création de factures, ou encore d'organismes institutionnels tels que l'État, le droit du travail, les banques et l'administration fiscale.
Stockage des données	•À chaque étape de traitement des données collectées et produites, c'est essentiel de les stocker .Toutes les données sont sauvegardées dans des bases de données clients ou fournisseurs, et l'archivage est exigé par les contrats de travail des employés.

Traitement des données	Pour atteindre les objectifs établis, il est nécessaire de transformer et de traiter certaines données. Par exemple, dans un logiciel comptable, un bon de commande d'un client doit être transformé en bon de livraison, facture et pièce comptable. En suivant une méthode, chaque élément de données peut fournir des informations supplémentaires.
Diffusion des données	La vraie valeur de toute information, qu'elle soit stockée ou créée, n'est atteinte que lorsqu'elle est communiquée de manière sécurisée au destinataire approprié, au moment approprié et avec le contenu approprié. Pour cela, le système d'information doit permettre une communication sécurisée des données.

Source : DCG 8 Systèmes d'information de gestion edition 2 2022

1.3 Les composants d'un système d'information :

Composante organisationnelle :

• Algorithmes et processus de stockage des données, identification du personnel de sécurité SI, protection des données à un caractère personnel (RGPD) et transmission sécurisée des données aux consommateurs ;
• Planification et évolution organisationnelle.

Composante humaine :

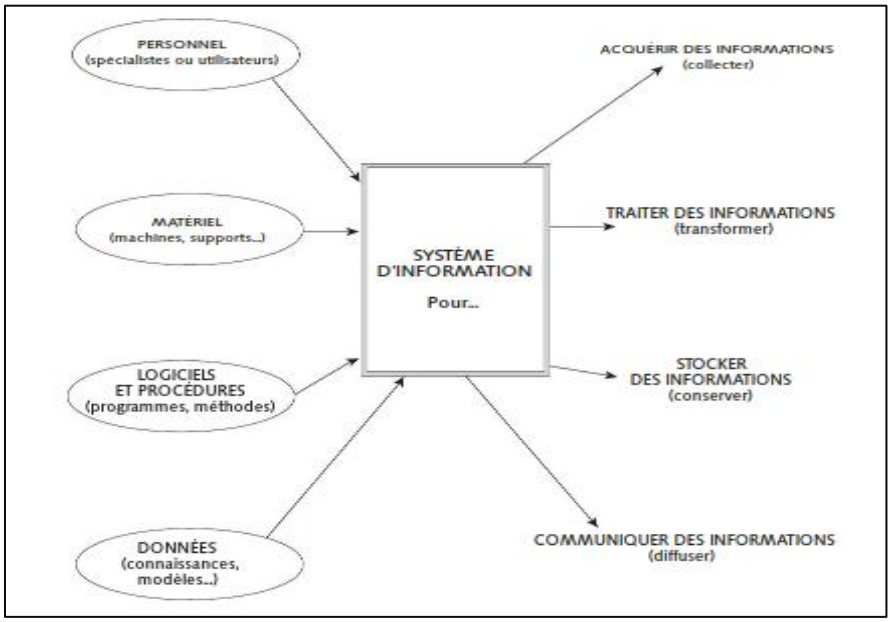
• Utilisateurs et professionnels de l'informatique ;
• Un rôle important dans la formation numérique et les bonnes pratiques numériques qui sont congruents avec les besoins de fonctionnement optimal.

Composante technologique :

• Dimensions matérielles : ordinateurs, tablettes, Smartphones, scanners, armoires, serveurs, etc. selon les exigences ;
• Dimensions logicielles : applications professionnelles, PGI, logiciels de sécurité avec suivi et mises à jour régulières.

Le SI se compose de trois composants interconnectés.

Figure 01 : La notion de système d'information



(**Source** : DCG 8 Systèmes d'information de gestion edition 2 -2022)

1.4 Les différents types de système d'information dans l'organisation

Une organisation est composée de sous-systèmes interconnectés, d'un système de pilotage, d'un système d'information, et d'un système opérant. Ces sous-systèmes fonctionnent ensemble pour assurer le bon fonctionnement global de l'organisation dans son ensemble.

- Le système opérant : C'est la base de toute organisation. Ce système est responsable de transformer l'information dans le but de la restituer à la personne appropriée. Il convient à de nombreux services aux entreprises.

- Le système de pilotage : ce système contrôle et guide le fonctionnement de l'organisation. Il occupe une place centrale dans le système d'information, chargé de fixer les objectifs de l'organisation et de prendre les décisions pour les atteindre.
- Le système d'information : ce système a le rôle de lien entre deux autres systèmes au sein d'une organisation. Il est responsable de collecter, traiter, stocker, de transformer et de diffuser des données et des informations entre le système d'exploitation et le système de pilotage.

1.5 Les facteurs clés d'un Si et si management un SI idéal est :

- S'est-il nécessaire que les systèmes d'information soient en alignement avec la stratégie globale et les objectifs opérationnels de l'organisation

- Conforme aux obligations légales en vigueur.
- Sécurisé ;
- Facile à utiliser ;
- Fiable ;
- Evolutif ;
- Pérenne ;
- Disponible ;
- Efficace

1.6 Le rôle de système d'information :

L'objectif du SI est de s'assurer que les informations peuvent être saisies, stockées, traitées et transmises afin que, dans l'organisation, on ait accès en temps opportun aux données nécessaires pour accomplir efficacement ces tâches. Le SI répond aux besoins actuels, aide à la décision et prépare à vos propres besoins (veille informationnelle, gestion des connaissances). Bien que le SI englobe L'ensemble de l'organisation gère uniquement des informations gérables et standardisées tout au long de ses opérations. Et généralement isolées de l'environnement (ex : humeur du patron ou motivation des salariés).

La performance de toute organisation est fortement impactée par son Système d'Information.

Le système d'information (SI) agit comme la base des opérations internes et les interactions de l'organisation avec les parties prenantes (fournisseurs, clients, agences gouvernementales) en sont fortement influencées. Le système d'information (SI) est un instrument multidimensionnel qui, lorsqu'il est utilisé efficacement, peut procurer un avantage concurrentiel significatif à l'entreprise.

Tableau 02 : Le Rôle Du Système D'information

SI STRATEGIQUE	SI OPÉRATIONNEL
Il est important d'assurer l'alignement avec la stratégie globale et d'évoluer et de servir cette stratégie, plutôt que l'inverse. Par exemple, une organisation qui participe à la vente uniquement sur Internet, rachète une filiale à l'étranger ou fusionne avec une autre entreprise doit pouvoir mettre en œuvre son projet à l'aide d'un système d'information adaptable et flexible.	● Pour assurer des échanges sécurisés pendant le transport, diverses actions doivent être entreprises ● Ces actions comprennent la fourniture de services, la gestion des connexions inter-entités et la mise en place d'un système de mobilité clientèle unifié." ● Le partage des applications et des données est également nécessaire pour faciliter des opérations efficaces ● Des processus de résolution de problèmes doivent être mis en place pour résoudre tout problème qui survient ● Les transferts de données électroniques peuvent améliorer l'efficacité et rationaliser les opérations.

Source :DCG 8 Systèmes d'information de gestion edition 2 (2022)

2- La notion d'audit :

2.1 Définition d'audit :

D'après (Mikol Alain.2000), Le latin donne un sens très précis à auditer « *audire* », qui signifie écouter, et le verbe « to audit » lui-même a le sens de vérifier, de contrôler et de surveiller.

La pratique d'évaluation des informations financières, des processus, des systèmes et des opérations d'une organisation ou d'une entreprise, est connue sous le nom d'audit. Il est effectué par une personne ou une équipe indépendante de l'organisation pour garantir raisonnablement l'exactitude, la fiabilité et la conformité de ces informations, conformément aux normes et exigences en vigueur.

2.2 Définition d'audit interne :

L'institut Français de l'Audit et du Contrôle Internes (l'IFACI, 21 mars 2000) Déterminé l'audit comme *« Une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité. »*

2.3 Les typologies usuelles de l'audit interne :

2.3.1. L'audit comptable et financier :

Un audit comptable et financier consiste à comparer les informations de L'Else aux normes établies telles que les lois, les règles et les directives de gestion afin d'examiner l'exactitude et l'authenticité des données financières. Les activités d'Else affectant la préservation des actifs, le traitement comptable et l'information financière font l'objet de l'audit. L'auditeur interne évalue les contrôles comptables internes d'Else pour déterminer l'authenticité, la conformité et la sincérité des informations financières et comptables de l'entreprise.

2.3.2. L'audit opérationnel :

L'audit opérationnel est un examen fréquent, continu et impartial de toutes les activités organisationnelles conçu pour aider les gestionnaires à améliorer la performance de leurs unités administratives. Il est basé sur une évaluation objective des opérations et l'élaboration de suggestions pertinentes. L'évaluation des facteurs de gestion tels que la planification, l'organisation, la direction et le contrôle sont inclus dans l'audit opérationnel. Cela englobe les objectifs, les projets, les structures organisationnelles, les règles et les procédures, les systèmes et les processus, les contrôles, les personnes et les ressources physiques. Le but de l'audit opérationnel est de confirmer la réalité des opérations plutôt que de se fier exclusivement à l'image fournie par la comptabilité. Cette méthode permet à l'organisation de rivaliser avec les meilleures pratiques.

2.3.3 L'audit de direction ou de management :

L'évaluation de l'audit de management reste ambiguë : pour certains, elle n'est réalisable que sous forme de compilation de plusieurs audits opérationnels. D'autres estiment que l'audit de management est ce qu'un président ferait s'il avait le temps et les ressources pour examiner toutes les parties de l'administration d'une entreprise. Cependant, dans tous les cas, il ne s'agit pas d'auditer le management général en portant un jugement sur ses options stratégiques et politiques. "En aucun cas l'auditeur ne peut s'intéresser à la substance des choses : ce n'est pas son objectif et il n'a pas la compétence pour le faire.

Il convient de dire que l'existence d'un service d'audit interne ne modifie en aucune façon la liberté de choix et de décision de la direction générale. En revanche, observer les choix et les décisions, les comparer, mesurer leurs conséquences et attirer l'attention sur les risques ou les incohérences relèvent de l'audit interne.

Par conséquent, l'audit de management nécessite des niveaux élevés d'expertise, une connaissance approfondie de l'organisation et une autorité suffisante pour être entendu par les personnes responsables des suggestions qui peuvent être formulées dans ce domaine.

2.4 Définition de l'audit de système d'information :

L'audit des systèmes d'information est considéré comme un domaine d'étude qui fait appel à différentes formes de connaissances, notamment l'audit traditionnel, les systèmes de management d'information, les systèmes comptables, l'informatique et les sciences du comportement. Cette combinaison de compétences permet aux auditeurs de comprendre les différents aspects des systèmes d'information et de procéder à des évaluations rigoureuses de leur efficacité et de leur conformité.

Selon Ron Weber (2010), un audit du SI est le processus d'acquisition et d'évaluation des preuves pour évaluer si un système fonctionne, les ordinateurs peuvent sécuriser les actifs, maintenir l'intégrité des données, favoriser efficacement la réalisation des objectifs de l'organisation et utiliser efficacement les ressources. Plusieurs aspects examinés dans un audit de système d'information tels que l'efficacité, l'efficience, la disponibilité du système, la fiabilité, confidentialité et intégrité, aspects de sécurité, audits de processus, modifications de programmes, audits de sources de données et de fichiers de données.

2.5 Pourquoi faire un audit de système d'information :

À l'ère actuelle, le système d'information de toute organisation détient la clé de son succès et de son avancement. Un système d'information efficace, flexible et à la pointe de la technologie peut s'avérer être un atout précieux pour une entreprise, ouvrant la voie à d'importantes opportunités de croissance. En fait, une étude récente a montré que 54 % des organisations en expansion attribuent à leurs systèmes numériques la croissance de leurs revenus en 2021.

D'un autre côté, un système d'information obsolète et rigide peut entraver les progrès et obstruer la voie du succès. Remédier à cette situation nécessiterait un investissement important et les managers doivent avoir une parfaite compréhension des enjeux, opportunités et obstacles liés à leur système d'information.

2.6 L'importance de l'audit de système d'information :

Selon (weber ,2006) Les facteurs qui justifient l'importance de l'audit des systèmes d'information sont :

- Détecter les pratiques de gestion informatique peu dirigées.
- Déterminez les risques de perte de données.
- Identifier les risques de prise de mauvaises décisions résultant d'informations erronées, lentes ou incomplètes issues du traitement des données par le système informatisé.
- Protéger les actifs de l'entreprise, qui ont généralement une grande valeur, notamment les équipements, les logiciels et le personnel.
- Détecter les risques d'erreurs informatiques.
- Détecter les risques de fraude informatique.
- Maintenir la confidentialité des données.
- Améliorer la maîtrise de l'évolution des pratiques informatiques.

2.7 Objectifs de l'audit du système d'information

- Assurer que les données stockées dans le système sont fiables et peuvent être utilisées en toute confiance.
- Assurer l'efficacité du système en répondant aux besoins des utilisateurs avec un de ressources d'information, ce qui a un rôle crucial dans la prise de décision.

- Assure que le système est équipé de mesures de sécurité suffisantes pour protéger les informations stockées dans le système contre tout accès ou utilisation non autorisé, ainsi que contre les pertes ou les dommages accidentels.
- S'assurer que le système d'information satisfait aux exigences de l'entreprise afin qu'il puisse soutenir l'organisation dans l'accomplissement de ses objectifs stratégiques.
- Atteindre les objectifs de respect des normes concernant la confidentialité, l'intégrité, la disponibilité et la conformité.
- Atteindre les objectifs de performance en s'assurant que les programmes sont développés et acquis conformément à l'autorisation de la direction, et que les modifications sont effectuées avec son approbation.
- Assurer que les informations stockées dans le système sont précises, complètes et conformes aux politiques de gestion établies.

2.8 Périmètre des audits des systèmes d'information :

L'audit des systèmes d'information peut être soit un sous-domaine d'un audit général englobant des domaines tels que les processus organisationnels, la conformité, etc., soit l'axe principal de la mission, couvrant des aspects tels que l'application, le projet, la sécurité et conformité légale.

A. L'audit des SI à l'occasion de missions « généralistes » :

1. L'audit d'une organisation :

Aujourd'hui, les entités et les administrations s'appuient quotidiennement sur les technologies de l'information, Ces outils informatiques ont un rôle crucial dans le bon fonctionnement de l'entité et sont souvent au centre de sa performance. Cependant, toutes les entités ne sont pas pleinement conscientes de leur importance, et même celles qui le sont peuvent ne pas toujours comprendre parfaitement comment les gérer, les exploiter et les sécuriser efficacement.

Par conséquent, un audit d'entité doit évaluer la manière dont l'informatique est utilisée pour identifier les besoins de l'entreprise, allouer des ressources et faire correspondre la structure et les pratiques organisationnelles avec des exigences informatiques fonctionnelles, adaptables, sécurisées et efficaces.

2. Les audits de processus

La dépendance des processus vis-à-vis de la technologie de l'information se transforme en plus évidente. Il est essentiel d'avoir un système qui répond à leurs besoins spécifiques. Par conséquent, lors de la réalisation d'un audit d'un processus, il est nécessaire d'évaluer les outils informatiques qui le supportent. L'audit doit comprendre une évaluation des données et des informations impliquées tout au long du processus, y compris celles d'autres processus, programmes qui assistent ou automatisent certains travaux ou procédures, et l'infrastructure informatique sous-jacente utilisée pour le traitement et la communication.

B. Les missions d'audit dont l'objet principal appartient au domaine des SI :

1. Les audits d'application :

Les applications sont des programmes informatiques créés et gérés par des personnes au sein d'une organisation ou par des entités extérieures. Ils peuvent être utiles à un ou plusieurs processus métier ou entraver leur efficacité. De plus, les applications peuvent soit contribuer soit perturber l'uniformité globale du système informatique, créant parfois à la fois des avantages et des vulnérabilités.

Par conséquent, lors de l'audit d'une application informatique, il est essentiel d'évaluer dans quelle mesure les composants logiciels et matériels fonctionnent ensemble et de déterminer si le système informatique s'aligne sur les objectifs stratégiques de l'organisation.

2. Les audits de projets informatiques

Au cours d'un audit SI, un auditeur peut être amené à rencontrer un projet portant atteinte à l'homogénéité du système d'information, provoquant chaos ou incohérence. Dans de tels cas, l'auditeur doit évaluer la fiabilité des exigences présentées et la méthode utilisée pour les rassembler et les interpréter pour le projet. Cette évaluation est essentielle car les recommandations de l'audit doivent tenir compte du contexte du projet.
Lorsqu'un audit est lancé en raison de circonstances insatisfaisantes, il peut soulever des doutes sur plusieurs aspects du projet, notamment :

- Les techniques employées pour articuler et recueillir les besoins métiers,
- La méthodologie de classement et de sélection des efforts conflictuels,
- Le processus d'acquisition de sous-traitants informatiques.

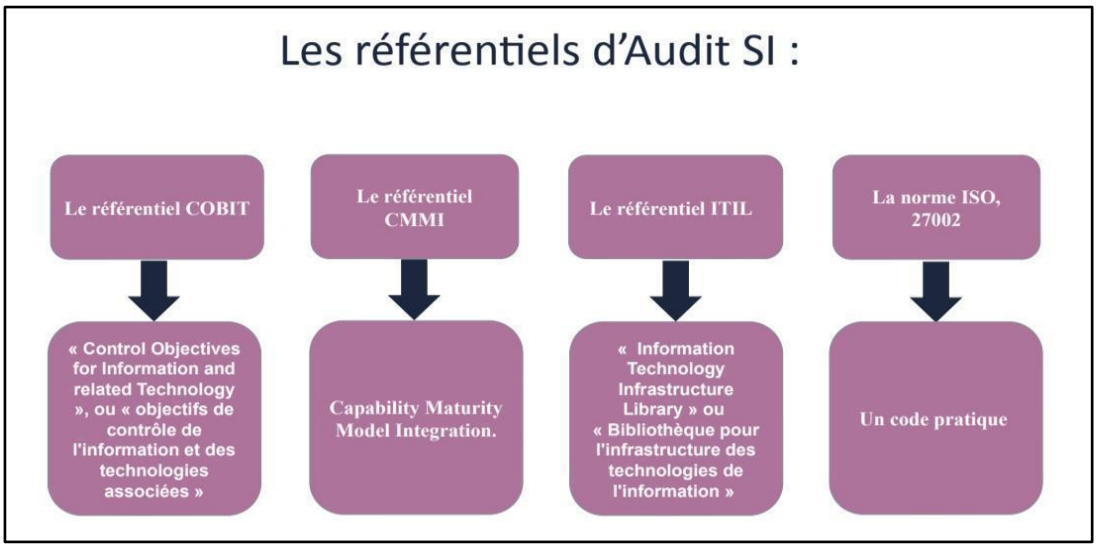
- La supervision des procédures au sein de l'organisation, en particulier celles qui se rapportent au projet examiné.
- Il peut être nécessaire de revoir la gestion de la fonction informatique et de réorganiser le processus audité.

2.9 L'organisation de l'activité Audit de système d'information

2.9.1 Les méthodes et les normes d'audit des systèmes d'information :

Les méthodes d'audit des systèmes d'information sont un ensemble de techniques et de procédures utilisées pour évaluer la sécurité, la qualité, la sécurité et l'efficacité des systèmes d'information d'une organisation. Ces méthodes sont essentielles pour garantir l'intégrité et la fiabilité des données, ainsi que pour identifier et corriger les vulnérabilités éventuelles dans les systèmes informatiques.

Figure 02 : Les référentiels d'Audit



Source: GTAG 2ème édition , Les contrôles et le risques des systèmes d'informations

Plusieurs normes sont applicables aux systèmes d'information et divers référentiels peuvent être intégrés à un audit du SI. Au niveau mondial, la norme COBIT s'impose comme la référence la plus utilisée dans ce domaine.

Le COBIT (Control Objectives for Information and related Technology) :

Le COBIT est un cadre de référence pour la gouvernance et le contrôle des systèmes d'information, créé en 1996 par l'ISACA. Il est développé par des experts reconnus dans

ce domaine et peut être utilisé en complément d'autres référentiels tels que le COSO pour apporter des objectifs de maîtrise du SI plus précis.

COBIT fournit un ensemble d'objectifs de contrôle des SI largement acceptés pour aider les auditeurs à développer une politique d'analyse et de management des risques SI.
Le périmètre du COBIT ne se limite pas seulement à la direction des SI dans l'organisation, y compris les directions générales, les directions métiers et les actionnaires.

Le référentiel ITIL (Information Technology Infrastructure Library) :

ITIL est une compilation de meilleures pratiques et est un cadre de bonnes pratiques pour le management des services IT. Qui visent à améliorer l'efficacité des services IT. Bien qu'il ait été développé à l'origine pour le secteur public, il est désormais utilisé dans le secteur privé. Ce cadre de référence peut être intégré dans le processus d'audit.

Selon Axelos, l'organisme d'accréditation officiel d'ITIL, ITIL est défini comme suit :
"*Un ensemble de pratiques détaillées pour la gestion des services informatiques (ITSM) qui vise à aligner les services informatiques sur les besoins de l'entreprise. ITIL décrit des processus, des procédures, des tâches et des listes de contrôle qui ne sont pas spécifiques à l'organisation, mais peuvent être appliqués par une organisation pour établir une intégration avec la stratégie de l'organisation, offrir de la valeur et maintenir un niveau de compétence minimum".*

Les normes ISO (Organisation internationale de normalisation) :

Les normes ISO sont considérées comme le principal cadre de référence à l'échelle internationale. Dans la zone de couverture de COBIT 5, on peut mentionner les normes de la famille ISO 20000 qui concernent la gestion des services informatiques. Ces normes décrivent les processus de gestion nécessaires pour offrir de manière efficace et efficiente des services informatiques à l'entreprise et à ses clients, tout en respectant les exigences d'ITIL.

La norme iso 19011 :

La norme ISO 19011 est une ressource précieuse pour les entreprises qui souhaitent auditer leurs systèmes de management. Il fournit des instructions sur les audits internes et externes et sur les principes de l'audit, tels que gérer efficacement un programme d'audit et réaliser des audits du système de management.

La norme ISO 19011 conseille en outre les organisations sur la manière d'évaluer la compétence des personnes participant au processus d'audit, allant des responsables du programme d'audit aux auditeurs et aux équipes d'audit. Ainsi, les organisations peuvent être sûres que leurs audits sont effectués efficacement tout en maintenant l'efficacité, la cohérence et l'amélioration des performances du système de management.

En fin de compte, l'utilisation de la norme ISO 19011 aide les organisations à améliorer leurs activités d'audit, ce qui se traduit par une transparence, une responsabilité et une fiabilité accrues.

La norme iso 27000 :

L'ensemble de normes ISO 27000 garantit que les entreprises maintiennent la sécurité de leurs informations. Ils permettent à une organisation de gérer plus facilement la sécurité des informations, notamment des informations personnelles, données financières et documents protégés par la propriété intellectuelle, ainsi que les informations qui vous sont confiées par d'autres parties.

La famille de normes iso 27000 :

Tableau 03 : La famille de normes iso 27000

ISO 27001	Décrit le processus permettant le management de la sécurité de l'information (SMSI).
ISO 27002	Donne un catalogue des bonnes pratiques de sécurité
ISO 27003	Décrit les phases initiales qui doivent être accomplies afin d'atteindre un système de gestion comme dans la norme ISO 27001
ISO 27004	Permet de définir les contrôles d'exploitation du SMSI
ISO 27005	Décrit les processus de management des risques
ISO 27006	Décrit les exigences relatives aux organismes qui auditent et certifient les SMSI des sociétés

Source : Audit du système d'information - les normes 2018-2019

Manuel de vérification informatique 2014 WGITA :

Le Manuel d'audit informatique est un guide compilé par l'équipe de l'INTOSAI sur l'audit IT (WGITA) et l'Initiative de développement de l'INTOSAI (IDI).
Son objectif principal est d'aider les auditeurs à planifier et à réaliser des audits IT. Il fournit outil de travail QUI suit les principes d'audit généraux énoncés dans les Normes internationales des institutions supérieures de contrôle des finances publiques (ISSAI), et a été spécialement conçu pour les institutions supérieures de contrôle (ISC).

Le manuel d'audit IT peut être utilisé en plus d'autres cadres tels que le modèle COBIT, l'Organisation internationale de normalisation (ISO) ou les normes, guides et manuels d'autres ISC. Cet outil a été remis aux équipes de travail de la cour des comptes algérienne. C'est un allié précieux pour les auditeurs IT, leur permettant d'effectuer des audits avec plus d'efficacité et de précision

2.9.2 Définition de la charte d'audit :

La charte de l'audit interne est élaborée conformément à la norme 1000 du référentiel international des pratiques professionnelles en matière d'audit interne, qui spécifie
D'après *(*CRIPP édition 2017*) « La mission, les pouvoirs et les responsabilités de l'audit interne doivent être formellement définis dans une Charte d'audit interne, être cohérents avec la définition de l'audit interne, le code de déontologie ainsi qu'avec les normes. Le responsable de l'audit interne doit revoir périodiquement la charte d'audit interne et la soumettre à l'approbation de la Direction générale et du Conseil d'Administration ».*

2.9.3 La mission d'audit et ses différentes phases :

2.9.3.1 Définition de la mission :

Du latin mittere la Mission, c'est : envoyer, le Petit Larousse définit la comme : *« Fonction temporaire et déterminée dont un gouvernement charge un agent spécial … par exemple : ce que l'on est chargé d'accomplir dans l'intention de Dieu ou d'après la nature des choses ».*

Il est préférable de ne pas généraliser à partir de cette description et de qualifier les auditeurs de « *divins* ».

2.9.3.1.1 Le champ d'application :

La portée d'une mission d'audit diffère considérablement en fonction de deux facteurs : son objet et sa fonction.

➢ **L'objet** : il permet de faire une distinction claire entre s'il s'agit d'une mission spécifique ou générale.

-**La mission générale** : la mission générale n'a aucune limite géographique. Exemple :

✓ Audit des SAP,

✓ Audit des centres informatiques

- **La mission spécifique :** Se concentrer sur un point précis dans un lieu déterminé. Par exemple :

✓ Audit du SPA CONDOR Electronics de Bordj Bou Arreridj ;

➢ **La fonction :**

Il existe deux types de missions, uni-fonctionnelles et polyfonctionnelles.

▪ **Uni-fonctionnelle** : Une mission d'audit uni-fonctionnelle se concentre juste sur une seule fonction, tels qu'une mission spécifique ou générale,

▪ **Plurifonctionnelle** : Une mission d'audit multifonctionnelle implique que l'auditeur examine nombreuses fonctions au sein d'une même mission. Plutôt que de se concentrer sur une seule fonction.

2.9.3.1.2 La durée :

Plusieurs facteurs peuvent influencer la durée d'une mission d'audit, ce qui peut entraîner des variations significatives dans sa durée., comme l'étendue de l'audit, la disponibilité des informations, le nombre d'auditeurs impliqués, la complexité et la taille de l'organisation auditée, et tout problème inattendu pouvant survenir. Lors de la vérification. La durée peut varier de dix jours à dix semaines. Le temps peut être mesuré en heures, jours ou semaines par auditeur selon le niveau de détail des statistiques.

Généralement la durée d'une mission d'audit interne varie en fonction de l'envergure du sujet à traiter ou à auditer, ainsi que du nombre d'auditeurs impliqués, pouvant aller de quelques jours à plusieurs mois.

Par conséquent, il est difficile de fournir un calendrier définitif pour une mission d'audit puisque chaque mission est unique et peut avoir son propre ensemble de circonstances.

2.9.3.2 Les trois phases fondamentales de la mission d'audit interne

Ces trois phases sont traditionnellement désignées :

- Phase de préparation ;
- Phase de réalisation ;
- Phase de conclusion.

Dans une analyse détaillée, nous verrons que chaque phase est divisée en périodes, mais nous pouvons dire que toutes nécessitent des auditeurs avec des compétences spécifiques. Ces compétences peuvent ne pas être possédées par un seul auditeur, et donc, la meilleure mission est toujours réalisée par une équipe d'auditeurs.

A-La phase de préparation

Au cours de la phase de préparation, l'auditeur interne élaborera un plan pour la mission d'audit. Cela comprend l'identification des objectifs de l'audit, la détermination de la portée de l'audit et l'élaboration d'un calendrier pour l'achèvement de l'audit.

L'auditeur recueille des informations sur l'organisation auditée, y compris sa structure, ses politiques, ses procédures et son personnel clé. Ces informations sont essentielles pour comprendre les opérations de l'organisation et identifier les domaines de risque qui peuvent devoir être traités lors de l'audit.

De plus, l'auditeur définit la méthodologie d'audit et développe les procédures d'audit à suivre pendant la phase de travail sur le terrain. L'auditeur doit recueillir des informations provenant de différentes sources et utiliser son imagination pour anticiper les problèmes qui peuvent se présenter au cours d'une mission d'audit. Ils doivent être en mesure de rassembler ces informations de manière logique et de les aider à planifier efficacement l'audit.

À la fin de la phase de préparation, l'auditeur doit comprendre clairement des objectifs et de la fonction de la mission d'audit, ainsi qu'un plan pour mener à bien l'audit de manière efficace et efficiente. Dans_cette phase, l'auditeur va mettre en place son référentiel pour atteindre un résultat effectif de sa mission.

1. L'ordre de mission

L'ordre de mission selon l'IFACI est une instruction donnée par le directeur général pour informer les principaux responsables de l'imminence de l'intervention des commissaires aux comptes. Cependant, dans le cas d'une mission externe, il s'agit d'une « lettre de mission » qui est un document contractuel entre l'entreprise et l'auditeur interne.

L'ordre de mission remplit 2 fonctions :

•Fonction de mandat

•Fonction d'information

1. La prise de connaissance des points à auditer

Cette étape est cruciale car elle conditionne si une mission d'audit s'est bien ou mal déroulée trois thèmes sont généralement abordés au pendant cette phase :

- L'organisation, c'est-à-dire l'analyse de l'organigramme de Domain d'audit
- Les finalités de la fonction à auditer
- Les techniques adaptées par l'auditeur dans le cadre de sa mission.

On peut également appeler cette étape la phase de familiarisation et comprend les actions suivantes :

Avoir une vue d'ensemble de l'organisation, y compris le but de la mission (l'objectif à atteindre) et son environnement.

- Évaluer les contrôles internes mis en place.
- Identification des risques majeurs qui y sont liés.
- Définir les objectifs de la mission

-Outils de travail de l'auditeur

Afin de remplir leur mission, les auditeurs se servent d'un éventail d'outils de travail, tels que, des listes de vérification, des questionnaires, les logiciels d'audit, des entrevues et des analyses de données. Pour recueillir les informations nécessaires à leur travail, les auditeurs établissent un questionnaire de sensibilisation et se réfèrent aux rapports d'audit antérieurs, aux notes de service et à tout autre document pertinent pouvant donner un aperçu du fonctionnement de l'entité auditée.

Quand les informations sont collectées, l'auditeur élabore un plan d'approche, sous format tabulaire détaillant les tâches et les objectifs de chaque activité à auditer. Il est à noter que

le plan d'approche n'est que la première partie d'un autre outil nommé tableau d'approche, qui comporte notamment des tableaux des risques, des forces et des faiblesses.

3. L'identification des risques

L'étape d'identification des risques, également connue sous le nom d'identification des zones à risques, a pour objectif de repérer les risques pouvant se diffuser plutôt que d'analyser les risques eux-mêmes.
En règle générale, la stratégie mise en place pour l'identification des risques prend en compte trois facteurs :

1 -L'exposition concerne les risques liés aux biens de l'entreprise, tels que les pertes financières découlant d'incidents

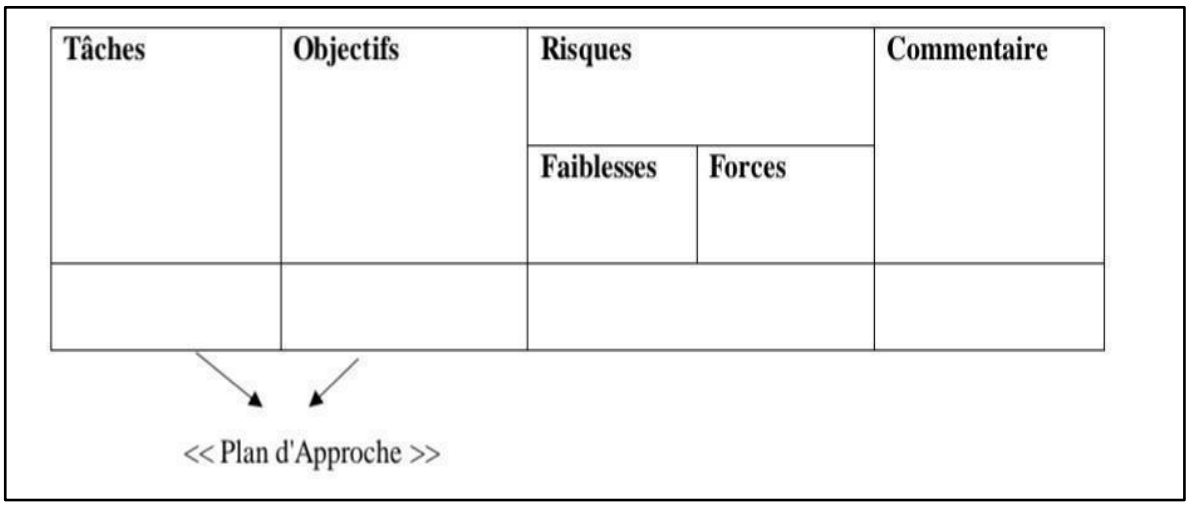
2-L'environnement prend en compte les risques associés à différentes opérations

3-La menace, quant à elle, est souvent difficile à prévoir comme c'est le cas avec les fraudes

Devant identifier les risques, l'auditeur doit analyser les informations, les processus et les chiffres significatifs collectés lors de la phase précédente afin d'établir le Tableau des Forces, Faiblesses et des Actions à entreprendre (T. F.F.A). Ce point ultime conclut la phase d'identifier des risques, effectuée conformément aux objectifs définis dans le Plan d'Approche.

La T. F.F.A représente les conclusions de l'auditeur sur chacun des sujets examinés dans une synthèse et une argumentation. Il représente l'état actuel des faiblesses et forces, réelles ou potentielles, et permet une classification des risques en préparation du Rapport d'Orientation.

Figure 03 : Le rapport d'orientation.



Source : Article de les 3 phases de la mission d'audit interne

-Le rapport d'orientation

Le Rapport d'Orientation reprend les éléments utilisés pour identifier des risques sous forme d'un document. Il détermine les objectifs de la mission en se basant sur trois catégories :

- **Les objectifs généraux** : démontrent les objectifs fondamentaux du contrôle interne. Dans ce contexte, l'auditeur doit vérifier que les opérations de contrôle interne sont correctement appliquées au sein de l'entité auditée.

- **Les objectifs spécifiques** : concrétiser les dispositifs de contrôle interne qui seront testés. L'auditeur crée les grandes lignes du questionnaire de contrôle interne qui sera utilisé lors de la phase suivante sur la base de la détermination de ces objectifs spécifiques.

Conclusion de la phase de préparation :

En plus des méthodes déjà utilisées, plusieurs autres outils sont employés au cours de cette phase, tels que le diagramme de circulation, l'organigramme, le questionnaire de contrôle interne et les analyses économiques et financières.

B -La phase de réalisation

Lorsqu'un auditeur se prépare à effectuer sa mission d'audit, il est crucial qu'il ait des capacités d'observation développées, de communication et de dialogue. Il doit être en mesure d'effectuer des évaluations et des observations approfondies, afin de pouvoir élaborer un plan d'action efficace. Toutefois, avant tout cela, l'auditeur doit s'assurer qu'il est bien accepté par les parties prenantes impliquées dans la mission d'audit, car cela est essentiel pour garantir une intégration réussie.

Dans la phase de réalisation de l'audit, qui se déroule principalement sur le terrain, l'auditeur devra suivre trois étapes :

• La réunion d'ouverture
• Le programme d'audit
• Le travail sur le terrain

1. La réunion d'ouverture

La réunion n'est pas considérée comme le début de la mission d'audit, mais plutôt le début des opérations de réalisation. Pour s'assurer que tout se passe bien, cette réunion doit être planifiée, avec un calendrier et un ordre du jour clairs.

• L'organisation de la réunion : Il est essentiel que cette réunion ait lieu chez l'audité plutôt que chez l'auditeur. Il réunit à la fois les auditeurs et les audités. Le chef de mission encadre les auditeurs, qui sont généralement composés de plusieurs personnes, comme les auditeurs seniors et les auditeurs juniors. Au cours de cette réunion, ils présenteront leur plan de travail aux audités. Les audités sont des responsables directs du service auditée, ainsi que le DG de l'entreprise, Afin de donner une légitimité à la mission et de renforcer la position de l'auditeur, il est recommandé de désigner un rapporteur parmi les participants pour préparer le compte rendu de la réunion

• L'ordre du jour : Il est primordial que le plan de travail soit remis aux participants dans un délai suffisant (environ 8 jours) pour qu'ils puissent se préparer. Au cours de la réunion, cela encourage la conversation et l'interaction entre les auditeurs et les audités.

Le rapport d'orientation, établi par les auditeurs lors de la phase précédente, est la base de l'ordre du jour de la réunion. Celui-ci aborde plusieurs points tels que :

- Présentation du rapport d'orientation
- Rendez-vous et contact
- Logistique de la mission
- Rappel sur la procédure d'audit.

2- Le programme d'audit

Le programme d'audit, également nommé programme de vérification ou plan de réalisation, décrit les nombreuses activités que les auditeurs sont tenus d'exécuter. Il s'agit d'un document de service d'audit interne qui crée un plan d'activité d'audit par l'équipe d'audit. Plusieurs objectifs doivent être atteints par le programme d'audit, notamment :

• C'est un accord contractuel qui définit les grands objectifs de la mission et permet de constituer la structure de l'équipe d'audit.
• C'est le guide principal entre les nombreuses activités et fonctions.
• C'est un horaire de travail.
• Il permet le suivi des travaux réalisés.

• Il sert de source de documentation.

Au cours de cette étape, l'auditeur utilise différents outils dont le questionnaire de Contrôle Interne et des outils d'interrogation et de description.

3- Le travail sur le terrain

Durant la première étape de l'audit, l'auditeur se rend sur le terrain. Ils doivent avoir l'esprit ouvert et aborder toutes les perspectives avec attention. Des évaluations approfondies sont nécessaires pour détecter les risques et les préoccupations utilisant des outils comme les FRAP (Feuille de Révélation et d'Analyse des Problèmes).

• **Les observations :** Dans le cadre de sa mission d'audit, l'auditeur réalise deux étapes d'observation distinctes :

• **L'observation immédiate** : vous permettant de révéler et d'évaluer la qualité de votre travail et de votre organisation.

•**L'observation spécifique** : Revenant au domaine de risque précédemment défini, l'auditeur réalise des tests portant sur des opérations significatives et caractérisant un processus critique.

• La preuve en audit interne :

Lors de l'évaluation d'un constat, l'auditeur est constamment préoccupé par le respect ou non des critères d'évaluation et de validation. En effet, la norme d'audit exige qu'une découverte soit réputée prouvée dès qu'elle est confirmée et remplit ainsi les règles suivantes :

Les informations doivent être :

- Fiables
- Indispensable
- Vérifier
- Pertinentes
- Être Utiles

• Cohérence et validation

Une fois que l'auditeur assure que ses observations sont cohérentes et pertinentes avant de les valider. Cela permet de garantir la qualité des conclusions et des recommandations qui seront présentées dans le rapport final d'audit.

C -La phase de conclusion

Dans la phase de conclusion, l'auditeur doit avoir d'excellentes compétences rédactionnelles et de synthétiser efficacement les informations.et qu'il soit important de noter que la communication avec les autres est également importante. Une fois que tous les matériaux nécessaires ont été rassemblés, l'auditeur commencera à développer et à présenter son produit final. C'est l'étape où toutes les informations recueillies seront organisées et un rapport sera rédigé pour résumer les résultats. Le rapport sera principalement basé sur les défauts FRAP découverts lors de l'audit.

1. Le projet du rapport d'audit

Le rapport d'audit s'appuie sur les FRAP (Fiches de Révélation et d'Analyse des Problèmes) des auditeurs, mais il est essentiel de rappeler que les remarques et observations qu'ils ont relevées ne sont définies qu'une fois confirmées. De plus, comme il s'agit d'un rapport intermédiaire, il est incomplet car il n'inclut pas encore les réponses des audités.

2-La réunion de clôture

Selon IFACI « *c'est la présentation orale par le chef de mission aux principaux responsables de l'entité audité, les observations es plus importantes, elle est effectuée à la fin du travail sur le terrain* »

Cette réunion a pour but de revoir le projet de rapport d'audit qui a été envoyé à chaque participant quelques jours avant la tenue de cette réunion.

Pour assurer le succès de cette réunion, l'auditeur doit respecter un ensemble de principes, dont l'un est d'éviter d'inclure dans le rapport tout ce qui n'a pas été présenté aux audités. L'objectif est de s'assurer que les conclusions et les recommandations du rapport sont fondées sur des faits et des observations partagés par toutes les parties concernées.

3- Le rapport d'audit

Selon les normes de l'IFACI, à la fin de la mission d'audit, le rapport final est présenté aux responsables clés pour faire une action et à la direction pour les informations. Ce rapport expose les conclusions de l'audit sur la capacité de l'organisation auditée à atteindre ses objectifs, tout en mettant en évidence les lacunes et les dysfonctionnements qui nécessitent des actions correctives pour améliorer les performances de l'organisation.

4- Le suivi des recommandations

L'IFACI recommande que le rapport d'audit soit donné aux principales parties prenantes et à la direction les conclusions relatives à la capacité de l'organisation auditée à remplir sa mission, en mettant en évidence les domaines de dysfonctionnement qui nécessitent des améliorations. En outre, une mise à jour de l'état d'avancement de la mise en œuvre des recommandations d'audit doit être communiquée régulièrement à la direction, y compris tout résultat obtenu grâce aux actions correctives prises par l'organisation auditée.

Conclusion de la phase de conclusion

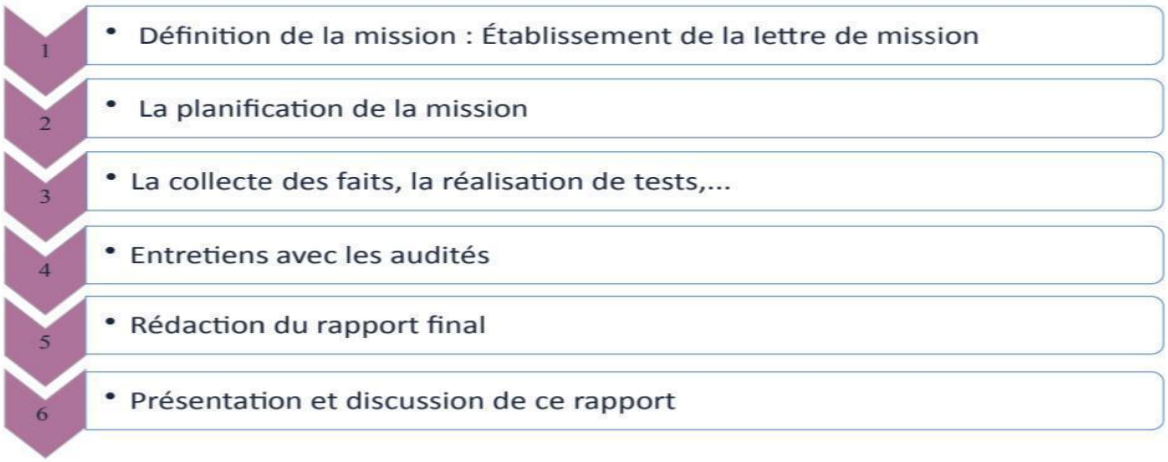
Au fil du temps, le domaine de l'audit a connu différentes évolutions, passant d'un simple objectif de protection des actifs d'une entreprise à un ensemble de techniques de plus en plus sophistiquées, guidées par des normes spécifiques, dans le but de fournir une opinion sur les opérations d'une organisation.

Ces changements ont permis à l'audit de s'adapter aux nouveaux défis et exigences de l'environnement économique, et de mieux répondre aux besoins des parties prenantes, en offrant une plus grande précision et une plus grande fiabilité dans ses évaluations.

2.9.3.3 La démarche d'audit SI

La mission comporte plusieurs étapes. Dans un premier temps, la mission d'audit doit être préparée en définissant le périmètre de l'investigation par une analyse préalable à l'audit afin d'identifier les questions à traiter. S'ensuit la rédaction d'une lettre de mission détaillée reprenant les principaux points à auditer. Pour mener à bien un audit IT, il existe ces six étapes de suivre décrites ci-dessus sous :

Figure 04 : La démarche d'audit SI



Source : GTAG 2ème édition, Les contrôles et le risques des systèmes d'informations

1. **Etablissement de la lettre de mission d'audit :**

La lettre de mission d'audit est un document autorisé par le responsable des exigences d'audit et l'auditeur, qui identifie les questions et les préoccupations du demandeur d'audit et L'auditeur contribue souvent à sa rédaction.

2. **Planification des missions :**

Cette étape consiste à définir une approche détaillée qui sera suivie et aboutira à un plan ou à une proposition d'audit. Le plan d'audit est rédigé par l'auditeur et sa validation par le demandeur d'audit. Lorsque le consensus est atteint, l'audit peut passer à l'étape suivante.

3. **Recueil des faits et réalisation de tests :**

La collecte de faits incontestables est une partie importante du processus d'audit. L'auditeur doit être en mesure d'identifier et de vérifier ces faits par des tests.

4. **Entretiens avec les audités :**

Cette étape consiste à mener des entretiens avec les opérationnels pour recueillir des informations complémentaires et vérifier les faits précédemment collectés. Cette étape peut être difficile, car les informations recueillies auprès du personnel opérationnel peuvent être davantage fondées sur des opinions que sur des faits.

5. **Rédaction du rapport d'audit :**

Le rapport d'audit est un long document qui présente les constatations et les recommandations de l'auditeur.

6. **Présentation et discussion du rapport d'audit :**

La dernière étape consiste à présenter et à discuter du rapport d'audit avec le demandeur de l'audit, la direction de l'organisation ou l'équipe de gestion informatique.

Cette approche est essentielle pour l'auditeur car elle fournit une base pour la réussite de l'audit. Cependant, il est également bénéfique pour l'organisation, car le processus d'audit encourage la participation active de toutes les parties prenantes, favorise le travail d'équipe et l'apprentissage organisationnel. Cela conduit finalement à une attitude plus positive envers le changement et à une volonté de s'adapter aux nouveaux défis.

4 - L'USAGE DE NORME ISO 20000 DANS L'AUDIT SI

4.1 LE SERVICE IT

4.1.1 Définition De Service IT :

Selon le (ITSM, Guide, par Jeffrey T. Barnes)"*Un service IT est une fonction organisée qui fournit des technologies de l'information et de la communication pour répondre aux besoins des utilisateurs dans une organisation, en s'efforçant de maximiser la valeur ajoutée pour l'entreprise tout en minimisant les risques. Les services IT peuvent inclure la gestion de l'infrastructure informatique, la fourniture d'applications, la gestion de la sécurité des systèmes, le support technique aux utilisateurs, la formation, la planification stratégique et la gestion de projets informatiques*."

4.1.2 Définition De Fourniture Des Services IT :

Selon le (Axelosen ,2019 ITIL Foundation Handbook)"*La fourniture de services IT est le processus consistant à offrir des solutions technologiques pour répondre aux besoins des utilisateurs dans une organisation. Cela peut inclure la mise en place et la gestion de l'infrastructure informatique, la fourniture d'applications, la maintenance des systèmes, la gestion de la sécurité, la formation des utilisateurs et le support technique. L'objectif de la fourniture de services IT est de maximiser la valeur ajoutée pour l'entreprise tout en minimisant les risques*."

4.2 Généralités d'ISO 20000 :

La norme ISO/IEC 20000 est un standard international qui définit les exigences pour un système de gestion des services informatiques (SGSI). Cette norme fournit un cadre pour la prestation de services informatiques de qualité et efficaces, qui répondent aux besoins des clients et des parties prenantes.

Dans le cadre de l'audit, l'utilisation de la norme ISO 20000 peut être très bénéfique pour les entreprises qui cherchent à évaluer leur capacité à fournir des services informatiques conformes aux exigences de qualité et de sécurité.

L'audit de conformité à la norme ISO 20000 permet de mesurer la performance de l'organisation en fonction de gestion des services IT, de déterminer les écarts par rapport aux exigences de la norme, et de fournir des recommandations pour améliorer la qualité du système de gestion des services IT.

En outre, la norme ISO 20000 peut également être utilisée comme un outil de référence pour l'audit interne de l'organisation.

L'audit interne permet de vérifier la conformité des pratiques internes de l'entreprise avec les exigences de la norme ISO 20000, de détecter les éventuels écarts et de proposer des actions correctives.

En résumé, l'utilisation de la norme ISO 20000 dans l'audit permet de garantir que l'entreprise à la capacité de fournir des services IT de qualité et efficaces, répondant aux besoins des clients et des parties prenantes, dans le respect des exigences de sécurité et de conformité réglementaire.

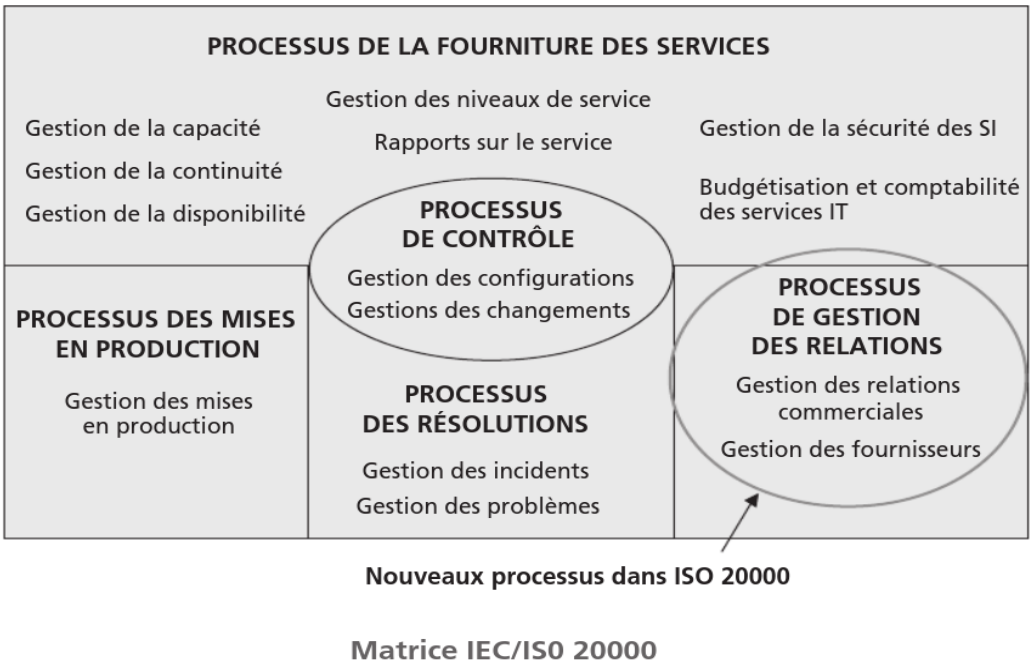
4.3 Les processus de l'ISO/IEC 20000

Répondre aux différentes attentes des clients oblige les entreprises à travailler en mode processus, ce que la norme ISO/IEC 20000 recommande fortement.

Le style de fonctionnement pertinent est basé sur de multiples activités interactives.

La norme ISO/IEC 20000 est fortement influencée par la norme ITIL V3 et la norme ISO 9001 :2000, qui mettent toutes deux l'accent sur la gestion des processus, la satisfaction client et le développement continu

Figure 05 : processus de la fourniture des services IT



Source : Guide commenté des normes et référentiels-Teneau, Gilles • Ahanda, Jean-Guy 2009

La norme ISO/IEC 20000 présente l'avantage supplémentaire de fournir à la fois l'accréditation et la certification des installations de production informatique.

La norme ISO/IEC 20000 est divisée en îlots :

- PDCA de services ;
- Département de soutien ;
- Service d'approvisionnement ;
- Relation pour les services informatiques.

La notion de gestion de la qualité de service cède la place au concept de gestion des services. Il faut considérer le service comme une véritable activité avec ses clients, son organisation, son environnement informatique et ses marchés.

Les normes ISO/CEI 20000 sont numérotées de 1 à 10.

Toutes les exigences doivent être validées pour qu'une organisation soit certifiée ISO/CEI 20000.

4.Évaluation des risques des systèmes d'information :

4.1 L'audit interne et l'évaluation des risques des systèmes d'information :

Dans un premier abord L'IIA a bien défini le risque comme la « possibilité que se produise un événement qui aura un impact sur la réalisation des objectifs. Le risque se mesure en termes de conséquences et de probabilité ». Selon le Guide pratique d'audit des technologies de l'information (2008).

Il est crucial pour les organisations de réaliser régulièrement une évaluation des risques auxquels elles sont confrontées. Cela permet au responsable de l'audit et à l'équipe d'audit de bien identifier les points clés suivants :

- Prendre en compte les objectifs de l'entreprise.
- Tenir compte de la stratégie relative aux systèmes d'information.
- Examiner le domaine des systèmes d'information.

4.2 Analyse SWOT :

La matrice SWOT est une méthode pour combiner les aspects de diagnostic externes et internes d'une entité. C'est un élément important dans la réussite de l'entreprise est la manière dont elle manage ses ressources internes (ses forces et ses

faiblesses) par rapport à son environnement externe (production d'opportunités et de menaces

En pratique, il est souvent compliqué de faire la distinction avec précision diagnostic internes et externes d'une entreprise.

Entre opportunités et menaces car cela dépend du point de vue adopté. L'essentiel est d'identifier les changements d'environnement susceptibles d'apporter une modification ou un bouleversement aux règles du jeu compétitif. Ces changements peuvent permettre à de nouveaux acteurs d'entrer sur le marché, pour changer de produits, innover et changer les limites de l'industrie. Pour les concurrents déjà établis, cela peut créer une menace.

De plus, l'analyse interne repose sur déterminer les forces et les faiblesses de l'entreprise via une évaluation des opérations et des résultats antérieurs.

Ce processus permet également de découvrir et d'auditer les caractéristiques distinctives de l'entreprise, telles que les savoir-faire, les ressources et les actifs qui la distinguent substantiellement et durablement de ses concurrents.

Cette étude doit vous permettre d'évaluer si votre organisation est capable de répondre aux éléments majeurs de succès, ainsi que si elle est capable de les modifier et d'établir de nouvelles règles de base.

CHAPITRE II :
MÉTHODOLOGIE
ET
ORGANISME D'ACCUEIL

Ce chapitre vise à expliquer la méthode utilisée ainsi que les techniques de collecte et de traitement des données, dans le but de répondre aux questions posées.

SECTION 01: Choix Méthodologiques Pour La Recherche

Dans cette section , nous détaillerons les étapes que nous avons suivies pour mener à bien nos recherches, y compris les techniques de recherche que nous avons sélectionnées, les approches de collecte de données que nous avons utilisées pour atteindre nos objectifs de recherche et les méthodologies que nous avons mises en œuvre pour examiner les résultats .

1. Objet

Chaque organisation dispose de systèmes d'information et d'une infrastructure IT uniques, ce qui nécessite la mise en place d'une procédure d'audit adaptée à leurs besoins et exigences spécifiques. Les systèmes d'information sont un élément clé de la réussite des entreprises dans le contexte économique actuel. Par conséquent, la mise en place d'une procédure d'audit des SI efficace peut constituer une contribution précieuse pour toute organisation.

2. Domaine d'application

La méthodologie d'audit interne de Condor Electronics est intégrée à son système de management de l'information (SMI), ce qui implique que les audits se basent sur ce système. Les périmètres d'audit chez Condor Electronics sont l'audit qualité qui existe déjà, l'audit de sécurité informatique et l'audit de fourniture des services IT qui n'existe pas encore. Par conséquent, notre choix de périmètre d'audit se concentre sur la Direction des Systèmes d'Information, avec notamment l'audit de fourniture des services IT se confirmer à la norme ISO 20000.

3. Choix d'entreprise

Nous avons opté pour Condor Electronics en raison de plusieurs facteurs importants. Tout d'abord, cette entreprise est réputée pour utiliser des systèmes d'information et de technologies sophistiquées pour gérer ses activités, ce qui est en adéquation avec notre objectif d'explorer comment ces systèmes peuvent être audités de manière efficace.

Condor Electronics est une entreprise bien établie dans son domaine avec une forte présence sur le marché, ce qui offre une base solide pour notre recherche. En outre, étant donné l'importance de son secteur d'activité et de sa position sur le marché

de l'électronique grand public en Algérie et dans la région MENA, l'entreprise est l'une des plus grandes marques électroniques de la région, ce qui la rend d'autant plus pertinente pour notre étude.

2. La méthode de recherche

La réalisation de cette recherche a été entreprise selon une méthode qualitative.

On appelle qualitative toute étude qui permet d'analyser et d'essayer de comprendre les motivations et le comportement des individus. Elle est basée sur des méthodes issues de la psychologie appliquée (analyse d'entretiens individuels ou de groupe, techniques projectives…).

*"La méthode qualitative est une approche de recherche qui se concentre sur la compréhension des expériences individuelles et collectives à travers des données riches et contextualisées, permettant de donner du sens aux phénomènes étudiés dans leur contexte culturel et soc*ial*".* Selon (Charmaz ,2014)

Selon Mays et Pope, (1995) La recherche qualitative vise à développer des concepts qui aident à comprendre les phénomènes sociaux dans leur contexte naturel, plutôt que dans un contexte expérimental. Cette approche met l'accent sur la signification, l'expérience et la perspective de tous les acteurs impliqués.

5.La méthode de collecte des données :

Dans toutes les recherches qualitatives, il est important de collecter les informations de manière à les analyser et les traiter pour une description complète et détaillée du sujet de recherche, et pour mettre en œuvre les informations qui montrent l'élaboration d'un audit des systèmes d'information.

Pour notre cas, la collecte des données s'est basée sur différentes techniques et une méthode adaptée au contexte et à la nature de notre recherche. Nous avons donc utilisé une approche qualitative basée principalement sur les outils suivants :

•La recherche documentaire ;

•L'entretien semi directif.

5.1 Recherche documentaire :

Nous avons choisi de mener une recherche documentaire comme première étape de notre recherche, et cette décision a servi de base à la suite de notre travail. Nous avons obtenu un maximum d'informations liées à notre étude en interrogeant divers ouvrages, articles et

thèses à travers la bibliothèque de l'ENSM, les bibliothèques numériques et les outils de recherche disponibles sur internet, afin d'obtenir des informations et de développer nos connaissances sur les concepts clés de notre recherche, tels que le système d'information, l'audit des systèmes d'information et de conformité.

De plus, nous avons examiné les documents internes fournis par l'entreprise étudiée, ce qui nous a permis de mieux comprendre, décrire et présenter l'entreprise et d'avoir les informations nécessaires à la réalisation de nos travaux de recherche.

Au final, un élément crucial pour développer une procédure d'audit efficace et efficiente est la recherche documentaire. Cela nous a aidés à mieux comprendre les normes et procédures d'audit pertinentes pour notre domaine d'activité, ainsi qu'à identifier les risques, à découvrir les meilleures pratiques d'audit et à renforcer la concurrence.

5.1.1 Les documents internes de la société que nous avons examinés :

Code / Version	Le nom de document
PR.SMI.03	Procédure d'audit Interne
A.04/PR.SMI.03	Rapport d'audit interne
Version 01	Formation Analyse SWOT
Version 01	Analyse SWOT de la Direction SI – Condor Electronics
A.01/PR.SMSI.07	Tableau de veille réglementaire
Version 01	Tableau de veille technologique
A.01/PL.SI.01	Planning de sensibilisation sécurité de l'information
Version 01	La charte de sécurité de la Direction SI – Condor Electronics
2015	ISO 9001 : 2015
2015	ISO 14001 : 2015
2018	ISO 45001 : 2018

Tableau 04 : Documents internes de la DSI que nous avons examinés (Élaboré par nous même)

5.2 Entretiens :

Après une évaluation minutieuse, nous avons déterminé que faire une recherche qualitative à l'aide d'entretiens serait le moyen le plus efficace d'obtenir des informations importantes. Notre objectif est d'obtenir des informations vitales qui nous aideront à gérer en profondeur les problèmes qui se posent. Nous avons l'intention d'obtenir une compréhension approfondie du sujet en menant ces entretiens et en utilisant ces informations pour tirer des conclusions utiles.

L'entretien est « *L'entretien est une des méthodes qualitatives les plus utilisées dans les recherches en gestion. Un entretien de recherche n'a rien de commun avec une discussion dans laquelle on se laisse porter par l'inspiration du moment*. » (Romelaer, 2005).

L'entretien de recherche est un moyen efficace d'acquérir des données. Cette méthode permet de collecter et d'analyser un large éventail de composantes, dont le point de vue, l'attitude, les sentiments et les représentations de la personne interrogée.

5.2.1 L'entretien semi-directif

L'entretien semi directif, souvent connu sous le nom d'entretien qualitatif ou approfondi, est une approche fréquemment utilisée dans les entretiens qui permet aux enquêteurs de concentrer la conversation avec la personne interrogée sur une variété de thèmes préparés qui sont inclus dans un guide d'entretien. Tout en permettant à la personne interrogée d'exprimer ses idées et ses expériences dans ses propres mots, cette stratégie donne une structure à l'entretien. Le guide d'entretien est un outil qui aide l'intervieweur à s'assurer que tous les sujets pertinents sont couverts tout en laissant une certaine liberté dans le dialogue. Cette méthode nous permet, en tant qu'intervieweurs, de collecter des données importantes de manière méthodique et ordonnée.

2.2.2 Le guide d'entretien :

Pour nous aider à mener nos entretiens, nous avons conçu un guide d'entretien. Un guide d'entretien est un document qui propose une liste de toutes les questions ou sujets abordés lors de nos entretiens. Ce guide nous permet de mieux comprendre l'environnement dans lequel nous intervenons, nous permettant de connaître et de comprendre les types de travail, les relations existantes, et d'identifier plus efficacement les problèmes.

Nous sommes éventuellement en mesure de fournir des solutions applicables et des recommandations basées sur les informations recueillies lors des entretiens.

Un guide d'entretien clair est essentiel pour s'assurer que le processus de recherche est bien structuré et que tous les participants se voient poser les mêmes questions dans les mêmes conditions. Cela permet de garantir la fiabilité et l'authenticité des résultats de l'entretien.

Voir (**Annexe 01**)

Notre guide d'entretien s'articule autour des thématiques suivantes :

• Audit des systèmes d'information,
• Elaboration d'un audit selon la norme ISO 20000 (fourniture de services),
• Élaboration d'une procédure pour la réalisation d'un audit IS,
• réalisation d'une mission d'audit en fonction du temps restant.

5.2.3 Les personnes interrogées dans l'entretien :

Nous avons choisi d'interroger un échantillon soigneusement choisi de personnes au sein de Condor Electronics afin de donner une base empirique solide à notre recherche.

Nous avons fait très attention à sélectionner les répondants qui exerçaient des professions pertinentes à notre sujet de recherche, car nous voulions être sûrs qu'ils pourraient fournir des réponses pertinentes et utiles à nos questions.

4.2.3 Tableau des personnes interrogées dans l'entretien

Nous avons mené des entretiens avec un ensemble de personnes travaillant à la DSI et jouant un rôle important dans sa gestion et qui sont en lien avec notre sujet, à savoir :

Les répondants	Durée
Directeur des Systèmes d'information	1 h
Responsable Standard et gouvernance SI	1h30min
Responsable sécurité SI	1h 30 min
Manager Supports SI & Master Data	1h 30 min

Manager Études & Développement SI	30 mins
Manager des infrastructures SI par intérim.	15 mins

Tableau 05 : Les personnes interrogées dans l'entretien (Élaboré par nous même)

3. Le focus group

En plus d'avoir recours à la technique de recherche documentaire et technique d'entretien nous avons également utilisé la technique de groupe de discussion (focus group) pour notre étude.

"*Un focus group est une méthode de recherche qualitative qui implique l'utilisation d'un groupe de personnes sélectionnées pour discuter d'un sujet spécifique dans un environnement contrôlé.*" (Krueger, 1994).

"*Les focus groupes sont une technique de recherche qualitative puissante qui permet d'obtenir des données riches et approfondies sur les attitudes, les croyances et les comportements des participants dans un environnement social interactif.*" (Morgan, 1997).

6. Traitement et analyse des données

Le traitement inductif des données est utilisé dans la recherche qualitative pour rechercher des relations et des faits dans les données qui ont été collectées.

Les témoignages complexes et les données recueillies au cours du processus de recherche peuvent alors être mieux compris par le chercheur. (Paul N'DA, 2015).

Pour les besoins de ce cas particulier, nous avons choisi d'analyser les données de manière thématique. Avec l'aide de cette méthode, nous pouvons analyser les réponses des personnes interrogées avec objectivité et repérer les thèmes ou les modèles qui reviennent sans cesse.

Dans le chapitre suivant, les résultats de notre analyse seront présentés plus en détail. Il est essentiel de garder à l'esprit qu'une analyse appropriée des données est cruciale pour la recherche qualitative afin de fournir des informations significatives et de tirer des conclusions précises. Nous pouvons nous assurer que nos résultats sont exacts et validés en utilisant une méthode d'analyse appropriée.

SECTION 02 : PRÉSENTATION DE LA SAP DE CONDOR

1. Organisme d'accueil

Nous allons aborder dans cette partie une présentation de notre organisme d'accueil et ses différentes composantes.

1.1 Présentation générale de l'entreprise CONDOR Électroniques

Condor Electronics, créée en 2002 avec un capital social de 4 277 000 000,00 DZD, est la plus importante filiale du Groupe Condor. Elle est spécialisée dans la fabrication et la commercialisation d'équipement électronique, électroménager et photovoltaïque.

En plus des plusieurs Directions de soutien (DRH, DFC, QHSE, DSI…), l'entreprise dispose de six (06) Business Units de production, implémentées à Bordj Bou Arreridj :

- BU Réfrigérateurs ;
- BU Cuisson et Transformation Métallique ;
- BU Climatisation, Chauffage et Lavage ;
- BU Transformation Plastique ;
- BU Polystyrène ;
- BU Energie Solaire et éclairage.

Condor Electronics est présent dans 12 pays, sur 3 continents, avec un plan d'expansion qui vise 35 pays.. La société a reçu de nombreux prix et reconnaissances pour sa contribution au développement économique et social de l'Algérie.

1.2. Chiffres clés 31/12/2021 :

Le nombre des employés	4000
Le nombre des employés (Hommes)	3663
Le nombre des employés (Femme)	337
Age moyen des employés	37 ans
Ancienneté moyenne des employés	5 ans

Tableau 06 : Chiffres clés 31/12/2021 (Source : DSI de Condor Electronics)

1.3 Missions, Visions, Valeurs de CONDOR ELECTRONICS:

1.3.1 Les missions :

- Proposer des produits innovants et de qualité ;
    - Augmenter le taux d'intégration ;
    - Assurer la pérennité et le développement de la société ;
    - Travailler en sécurité et limiter les impacts environnementaux ;
- Participer au développement local (sous-traitance, associations, etc.).

1.3.2 La vision :

La vision de l'entreprise est de devenir le leader national sur les marchés et d'être la marque préférée des algériens.

1.3.3 La valeur :

-Sécurité, santé, environnement et responsabilité sociale.
-Esprit d'équipe.
-Satisfaction des clients aux cœurs de nos priorités.
-Innovation.
-Respect et loyauté.
-Excellence.

1.4 L'Organigramme de la société CONDOR ELECTRONICS

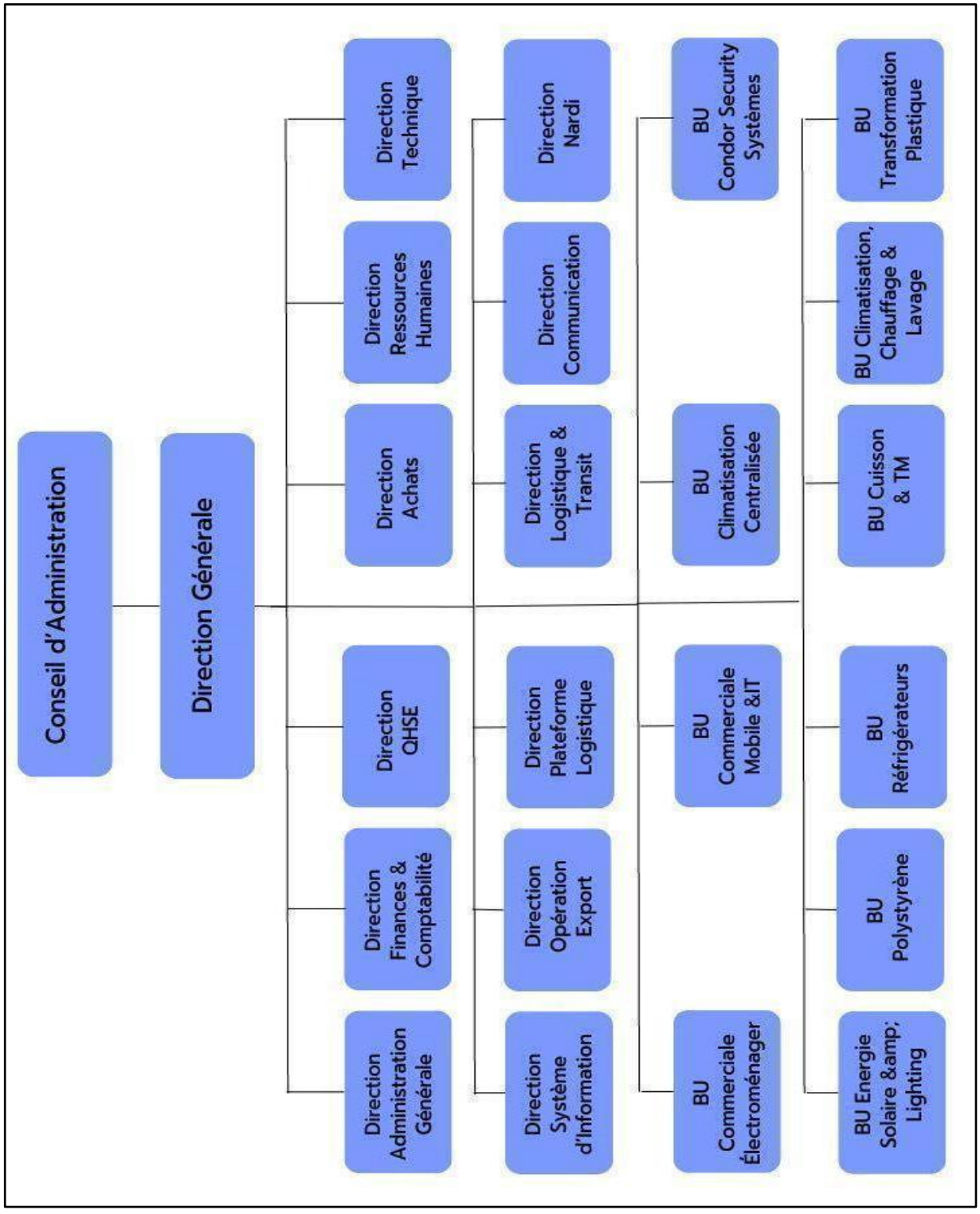


Figure 06 : l'Organigramme de la société CONDOR Electronics

(**Source** : la DSI de Condor Electronics)

1.5 La direction des systèmes d'information

Gère une organisation, des services, des structures IT, des télécoms et les évolutions des systèmes d'information et de télécommunications en fonction des besoins fonctionnels et des objectifs de l'entreprise.

Supervise la conception, la mise en œuvre et le maintien opérationnel (qualité, sécurité, fiabilité, prix et délais) des services informatiques et des systèmes d'information et de télécommunication. Supervise et pilote des projets en systèmes d'information.
La direction des systèmes d'information de l'entreprise condor électronique contient :

- ✓ Système d'information.
- ✓ Plan stratégique SI.
- ✓ Des systèmes ERP (Enterprise Resource Planning), le plus important c'est le SAP.
- ✓ Centre de données.
- ✓ Système Management intégré (SMI) certifié iso 9001 et 14001.
- ✓ Système de gestion de la sécurité de l'information certifié ISO 27001

1.5.1 Missions, vision et objectifs

Selon le Directeur de la DSI, les principales missions, vision et objectifs de la DSI sont :

Missions :

- Définir la vision stratégique en prenant en compte la stratégie de L'entreprise
- Élaborer un plan stratégique de sécurité et de communication relatifs au SI
- Assurer l'intégrité de la sécurité de l'entreprise
- Définir des normes utilisées par l'entreprise
- Définir le budget annuel
- Assurer la veille technologique
- Assurer la réalisation des projets

Vision :

La DSI doit être un prestataire pour les fournisseurs.

Objectifs :

- Mettre à jour la SAP 2022
- Améliorer le cyber sécurité et finaliser des projets
- Développer et refondre le site web de Condor Electronics.

1.5.2 Les activités de la DSI de SAP Condor Electronics :

La gestion et de l'optimisation des systèmes informatiques d'une Organisation. Ses principales activités comprennent :

- La gestion et l'administration des systèmes informatiques.
- Le développement et la mise en œuvre des applications.
- Le support informatique.
- La veille technologique.
- La gestion de projets informatiques.
- La gestion des données.
- La gestion des budgets informatiques .

1.5.3 Les moyens utilisés par la DSI pour atteindre les objectifs :

La Direction des Systèmes d'Information (DSI) met en œuvre différentes approches pour atteindre ses objectifs, qui peuvent varier en fonction de la stratégie de l'entreprise et des particularités de son environnement.

Voici quelques exemples :

- La mise en place de processus et de méthodologies.
- L'utilisation de technologies et d'outils.
- La collaboration avec les autres services de l'entreprise.
- La formation et le développement des compétences.
- La gestion des risque*s.*
- *L'innovation* .

1.5.4 La relation de l'audit interne avec la DSI :

La nature de la relation entre l'audit interne et la DSI peut différer selon les entreprises.

Toutefois, en règle générale, l'objectif de l'audit interne est de garantir une assurance impartiale et désintéressée quant à l'efficacité des processus de gouvernance, de gestion des risques et de contrôle interne de l'entreprise. Dans cette optique, la DSI est une fonction essentielle de l'entreprise, car elle est chargée de la gestion des systèmes d'information, qui sont un élément crucial pour le bon fonctionnement de l'entreprise.

Ainsi, l'audit interne peut collaborer étroitement avec la DSI afin d'évaluer l'efficacité des contrôles internes associés aux systèmes d'information, d'identifier les risques éventuels,

et de formuler des recommandations visant à accroître la sécurité et la fiabilité des systèmes d'information.

Le service d'audit interne peut aussi examiner si la DSI respecte les politiques et les normes de sécurité de l'entreprise ainsi que les règles en vigueur.

1.5.5 L'audit interne a une forte relation avec le management de la DSI de SAP Condor Electronics :

La fonction d'audit interne est intimement liée à la gestion de la DSI, car elle vise à évaluer l'efficacité des processus internes de l'entreprise, y compris ceux de la DSI. Dans cette optique, il est primordial que la gestion de la DSI collabore étroitement avec l'audit interne pour garantir la conformité des processus aux normes et aux politiques de l'entreprise, et pour détecter les domaines nécessitant une amélioration.

1.5.6 Les critères à utiliser pour évaluer les performances de la DSI auditée :

Plusieurs éléments doivent être pris en considération pour évaluer les performances d'une DSI (Direction des Systèmes d'Information) qui fait l'objet d'un audit.

Voici quelques exemples :

- •La qualité des services rendus. •L'efficacité opérationnelle.
- •La sécurité des systèmes. • L'innovation *et la transformation numérique.*
- •*La satisfaction des utilisateurs*.

1.5.7 Les critères seront-ils mesurés et évalués :

Les méthodes de mesure et d'évaluation des critères peuvent être adaptées en fonction des besoins de l'entreprise et des objectifs de l'audit. Cependant, voici quelques exemples de méthodes qui peuvent être utilisées pour évaluer les performances de la DSI :

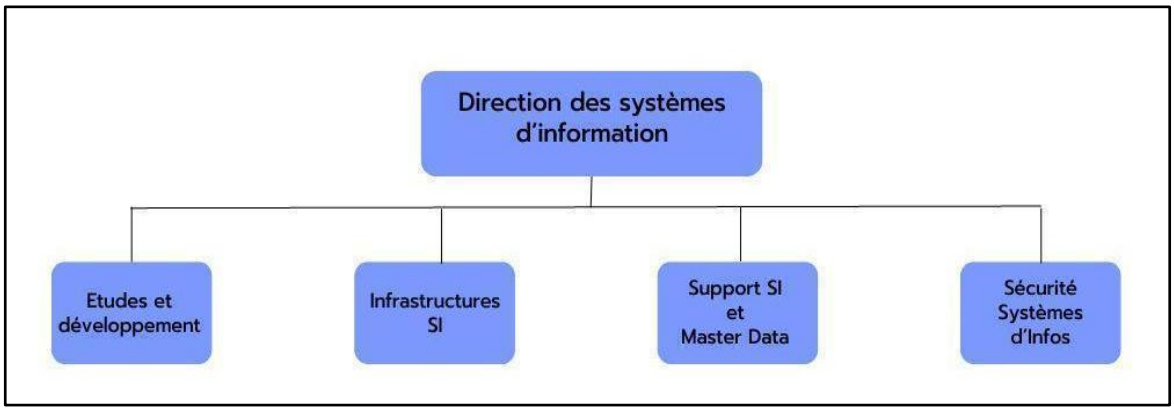
•La satisfaction des utilisateurs : Il est possible de mesurer la satisfaction des utilisateurs finaux des systèmes informatiques de l'entreprise en utilisant diverses méthodes, notamment des enquêtes de satisfaction, des analyses de données comportementales et des commentaires directs des utilisateurs.

Il est possible d'évaluer ces critères en combinant des méthodes quantitatives telles que la mesure d'indicateurs de performance, avec des méthodes qualitatives comme les enquêtes de satisfaction et les feedbacks des utilisateurs .

1.6 L'Organigramme de la Direction des systèmes d'information (DSI) de l'Entreprise CONDOR ÉLECTRONICS

L'organigramme de la direction des systèmes d'information (DSI) est présenté comme suit :

Figure 07 : L'Organigramme de la Direction des systèmes d'information



(**Source** : la DSI de Condor Electronics)

CHAPITRE III :

ANALYSE

ET

DISCUSSION

Dans ce dernier chapitre, nous avons élaboré un audit des systèmes d'information et nous avons fait aussi la réalisation d'une mission d'audit, avec une deuxième variable ISO 20000 fourniture des services IT.

Ainsi, nous allons présenter tous les résultats obtenus lors de notre recherche pratique, tout en suivant notre démarche théorique pour mieux éclairer les résultats.

SECTION 01 : ANALYSE DE L'EXISTANT

D'après notre entretien avec le DSI, la réponse à notre question Voir (**Annexe 1**) était la suivante : « *Nous avons effectué un audit interne qualité en utilisant plusieurs normes différentes (standards)* ». Nous avons bien compris qu'ils n'ont pas fait un audit des systèmes d'information. Pour cela, nous avons décidé d'élaborer une procédure d'un audit SI.

1-Détermination de l'objectif :

Notre objectif principal est d'évaluer la performance du département des systèmes d'information et de déterminer s'il fournit des services informatiques de haute qualité et efficaces aux différents départements et à ses clients.

2-Evaluation des risques :

D'après notre entretien avec le Responsable de Sécurité des Systèmes d'Information, voir (**Annexe 01**) l'une de ses principales tâches consiste à analyser et évaluer les risques liés aux fonctionnalités des SI au sein de l'entreprise.

Ces risques sont liés à deux types de facteurs : les risques internes (liés aux êtres humains, aux matériels et aux logiciels) et les risques externes (comme l'absence d'accords de confidentialité avec les tiers, la publication de services non sécurisés, etc.).

Pour élaborer une procédure d'audit efficace, il est essentiel de comprendre les risques liés aux SI et de les évaluer de manière systématique.

D'après notre entretien avec le RSSI au sein de la DSI, la réponse à notre question voir (**Annexe 01**) était la suivante : « *Nous utilisons plusieurs méthodes pour identifier les risques, telles que l'analyse SWOT, l'analyse PESTEL, l'évaluation des risques et l'analyse des parties prenantes, mais nous utilisons principalement l'analyse SWOT* ».

Nous avons bien compris que l'analyse SWOT est la méthode la plus couramment utilisée parmi celles qui existent surtout pour l'audit.

Pour cela, nous avons décidé de réaliser une analyse SWOT (forces, faiblesses, opportunités et menaces) des SI de l'entreprise. Cette approche nous permettra d'identifier les domaines de sécurité qui nécessitent une attention particulière.

2.1 Analyse SWOT

L'utilisation de l'analyse SWOT est un outil efficace pour identifier les points d'amélioration et élaborer une procédure d'audit fiable pour garantir la conformité à des différentes normes. Ainsi l'analyse SWOT va faire une l'analyse interne de département des systèmes d'information (ses force et faiblesses) et une analyse externe par rapport aux autres départements (les menaces et les opportunités).

Selon la réponse de notre entretien avec le RSGSI au sein de la DSI, elle était la suivante :

« L'audit interne peut couvrir de nombreux risques liés au SI, tels que : la sécurité des données, la conformité réglementaire, la gouvernance et la gestion des risques, La continuité des activités ».

D'après le Responsable Standards & Gouvernance SI Dr Fouad Mohamed, chaque service a sa propre norme et présente des risques de non-conformité. Et Avant chaque audit, il est primordial d'identifier les risques en effectuant une analyse SWOT, afin de garantir l'absence de risques et l'exploitation maximale des opportunités. En outre, si nous disposons d'un plan d'action pour traiter nos faiblesses, nous serons mieux préparés à l'audit et nous pourrons éviter les problèmes.

Pour cette raison, notre travail consistera à analyser les points associés à la norme ISO 20000, en particulier en ce qui concerne la fourniture des services IT par la DSI, afin d'identifier et sélectionner les points à auditer par rapport à la norme

Après avoir effectué une mise à jour de l'analyse SWOT en nous appuyant sur le document "Qualité Version 1" du DSI de Condor Electronics et en intégrant les directives et les exigences de la norme ISO 20000, nous avons identifié les éléments suivants pour l'évaluation et l'analyse de la matrice SWOT :

FAIBLESSES	FORCES
-Pas de Data Center de secours -Absence de contrat de services TI (y compris la maintenance après installation). -Veille technologique formalisée non exploitée -Absence de la notion client TI	-Plan Stratégique SI 2021-2023 -Infrastructures TI (DATACENTER, NETWORK etc...) -Gouvernance des systèmes d'information formalisée (Processus, politiques, procédures, modes opératoires, …) -Création SLA entre DSI et clients TI
RISQUES	**OPPORTUNITÉS**
-Risques liés à la non disponibilité des services informatiques -Risques liés à l'absence de la veille réglementaire -Risques liés à la perte des données à caractère personnel -Risques liés à la non réalisation de la sous-traitance	-Améliorer la fourniture des services TI. -Engagement de la direction générale pour l'évaluation de la fonction SI -Ferme volonté de la transformation digitale de SPA Condor Electronics -Implémentation de l'ISO 27001

Tableau 07: Analyse SWOT (élaboré par nous-même)

2.2 Parties intéressées internes et externes :

Lors de l'élaboration de la procédure d'audit du système d'information de la DSI de Condor Electronics, nous avons en effet identifié les parties prenantes internes et externes, ainsi que leurs attentions et besoins en termes d'informatique, à partir de l'analyse SWOT Qualité et nous avons décidé de garder la même.

La sélection des parties prenantes impacte directement ou indirectement la performance et l'efficacité du système d'information. Les parties prenantes comprennent les prestataires de services, la haute direction, les fournisseurs, les processus commerciaux et l'organisme de certification.

L'identification des parties prenantes et l'établissement d'une relation avec elles favorisent une communication efficace et établissent un climat de confiance et de respect mutuels. Pour chaque acteur pertinent pour le système d'information de la DSI, il est important

d'identifier ses besoins et attentes, et de déterminer ceux qui sont pertinents pour assurer la performance du système d'information. Les exigences contractuelles sont évidemment prises en compte. Les résultats de cette étape sont consignés dans un tableau : identifiant les besoins des parties prenantes vis-à-vis du système d'information de la DSI.

BACK

PARTIES INTERESSEES INTERNES ET EXTERNES

N°	Parties interessées internes et externes	Bessoins / exigences	Attentes
1	Préstaires de services	Accés aux systèmes ettechnologies d'informations	Protection des informations personnels - Protection de la propriété intelectuelle Partenariat et gagnant -gagnant
2	Fournisseurs	Cahier des charges explicites des besoins	Partenariat et gagnant -gagnant
3	Direction générale	Respect des exigences réglementaires-performance des processus	Retour sur invistissement SLA ;
4	Processus Métiers	Assistance, accompagnement, support Technique et formation SI	Fourniture des services fiables, Former, sensibiliser et conseiller sur les SI
5	Organisme de Certification	Respect des Exigences Contractuelles - Respect des dates d'audits - Respect des exigences relatives à l'utilisation du LOGO	Performance du système

Figure 08 : Parties intéressées internes et externes (Élaboré par nous même dans Excel)

2.3 Elaboration d'un plan d'action

A partir de la matrice d'analyse stratégique SWOT on va aboutir un plan d'action pour définir les actions à mener et qu'il s'agit de répondre à la question suivante : quelles sont les actions que doit mener l'organisation pour atteindre ses objectifs ?

L'élaboration d'un plan d'action est une étape critique dans le processus d'audit du système d'information. Il consiste à définir une série de mesures à appliquer (grille d'évaluation) afin de corriger les écarts détectés lors de l'audit et d'améliorer la sécurité et la fiabilité du système.

Pour mettre en place des actions correctives efficaces, il est important de définir des objectifs clairs pour chaque action. Il faut également établir un calendrier réaliste pour la mise en œuvre, identifier les personnes ou les équipes responsables de la mise en œuvre, déterminer les ressources nécessaires et fixer une échéance pour chaque action. Ce processus permettra de garantir que les actions correctives sont mises en œuvre de manière efficace et efficiente.

Le plan d'action doit également comprendre un suivi pour mesurer l'efficacité des mesures mises en place et pour vérifier que tous les écarts ont été corrigés de façon satisfaisante.

Un plan d'action bien élaboré permettra d'améliorer l'efficacité de la fourniture de services fiables par la DSI, ce qui aura un impact positif sur l'ensemble de ses activités.

BACK

PLAN D'ACTIONS / RISQUES

Risques	Action	Responsable	Echéance	Ressources	Etat de mise en œuvre
Risques liés à la non disponibilité des services informatiques	Elaborer un Plan de continuité d'activité SI	DSI	31 décembre 2023	Budget	0%
Risques liés à l'absence de la veille réglementaire	Suivi périodique de la réglementation en vigueur	RSGSI	31 décembre 2023	Ressources internes	100%
Risques liés à la perte des données à cacartère personnel	Etablir et réaliser un Planning de sensibilisation et mettre en place une charte de sécurité SI	RSSI	31 décembre 2023	Ressources internes	30%
Risques liés à la non réalisation de la sous-traitance	Elaborer un modèle de contrat d'engagement avec les sous-traitants de la securite, les infrastructures, ...ect.	RSGSI	31 mai 2023	Ressources internes	10%

Figure 09 :Plan d'action des Risques (Élaboré par nous même dans Excel)

BACK

PLAN D'ACTIONS / FAIBLESSES

Faiblesses	Action	Responsable	Echéance	Ressources	Etat de mise en œuvre
Pas de Data Center de secours	Etude et fesabilité de la mise en place un Data Center de secours (Physique,	Manager Infrastructures SI	31 décembre 2023	Budget Ressources internes	45%
Abscence de contrat de services TI (y compris la maintenance après	Appliquer SLA entre DSI et clients TI	DSI	31 décembre 2023	Budget Ressources internes	5%
Veille técnologique formalisée non exploitée	L'exploitation du tableau veille technologique	RSGSI	31 décembre 2023	Budget Ressources internes	30%
Abscence de la notion client TI	Un plan de formation et de sensibilisation des collaborateurs SI	RSGSI	31 décembre 2023	Budget Ressources internes	20%

Figure 10:Plan d'action des Faiblesses (Élaboré par nous même dans Excel)

BACK	PLAN D'ACTIONS / OPPORTUNITES				
Opportunités	Action	Responsable	Echéance	Ressources	Etat de mise en œuvre
Ameliorer la fourniture des services TI.	Elaborer un Plan d'amélioration continue de services TI	RSGSI	31 juillet 2023	Ressources internes	5%
Engagement de la direction générale pour l'evalution de la fonction SI	Appliquer le Plan Stratégique de la Direction Générale (Finanacement)	DSI	31 décembre 2023	Budget Ressources internes	20%
Ferme volonté de la transformation digitale de SPA Condor Electronics	Appliquer le Plan Stratégique de la Direction Générale (Allignement stratégique)	DSI	31 décembre 2023	Budget Ressources internes	20%
Implimentation de l'ISO 27001	Un plan d'action pour l'impliméntation de la norme ISO 27001	RSSI	31 décembre 2023	Budget Ressources internes	86%

Figure 11 : Plan d'action des Opportunités (Élaboré par nous même dans Excel)

2.4 Grilles D'évaluation

Pour établir une évaluation efficace de la Fourniture des services SI au sein du la DSI, nous avons utilisé un cadre d'évaluation standard qui mesure divers aspects de la performance. Ce cadre est également utilisé par le service IT pour évaluer les performances du système et évaluer les opportunités et les risques, ainsi que les interactions avec les parties prenantes internes et externes que nous avons identifiées lors de notre analyse SWOT. Voir **(Annexe 03)**

Notre objectif étant de respecter les normes ISO 20000 et les directives de notre superviseur, M. Fouad, nous avons prévu de mettre en place un bilan qui mesure la performance de notre système d'information. Pour établir cette grille d'évaluation, nous avons identifié les points à auditer qui ont été détectés lors de notre analyse SWOT, les avons évalués en fonction de leur gravité, et avons pris en compte leur impact sur la gestion du système d'information. Cette grille nous permettra d'identifier les actions d'amélioration de notre système d'information audité, d'assurer l'adéquation de la stratégie de notre DSI avec les besoins et les parties prenantes de l'entreprise et de garantir le succès à long terme de la stratégie de notre DSI.

Evaluation des Risques

RISQUES	Evaluation : C= G*P		
	Gravité	Probabilité	Criticité
Risques liés à la non disponibilité des services informatiques	3	4	12
Risques liés à l'absence de la veille réglementaire	2	3	6
Risques liés à la perte des données à cacartère personnel	3	2	6
Risques liés à la non réalisation de la sous-traitance	3	3	9

Figure 12 : L'évaluation des Risques (Élaboré par nous même dans Excel)

Évaluation des opportunités

OPPORTUNITES	Evaluation : V= I*O		
	Importance	Occurrence	Vraisemblance
Ameliorer la fourniture des services TI.	4	4	16
Engagement de la direction générale pour l'evalution de la fonction SI	4	4	16
Ferme volonté de la transformation digitale de SPA Condor Electronics	3	4	12
implimentation de l'ISO 27001	4	3	12

Figure 13 : L'évaluation des opportunités (Élaboré par nous même dans Excel)

Évaluation des parties intéressées

PARTIES INTERESSEES INTERNES ET EXTERNES

N°	Parties interessées internes et externes	Bessoins / exigences	Attentes	Evaluation : P= (IN*DI)*DP			
				Influence	Dialogue	Dépendance	Pertinence
1	Préstaires de services	Accés aux systèmes ettechnologies d'informations	Protection des informations personnels - Protection	4	2	3	24
2	Fournisseurs	Cahier des charges explicites des besoins	Partenariat et gagnant -gagnant	3	2	3	18
3	Direction générale	Respect des exigences réglementaires-performance des processus	Retour sur invistissement SLA ;	5	4	5	100
4	Processus Métiers	Assistance, accompagnement, support Technique et formation SI	Fourniture des services fiables, Former, sensibiliser et	3	4	4	48
5	Organisme de Certification	Respect des Exigences Contractuelles - Respect des dates d'audits - Respect des	Performance du système	3	3	3	27

Figure 14 : L'évaluation des parties intéressées ((Élaboré par nous même dans Excel))

2.5 Approche d'audit SI

Après avoir effectué une analyse SWOT interne et externe de la DSI, la DSI doit choisir la partie la plus intéressante à auditer, soit les risques ou les opportunités externes, ainsi que les faiblesses internes. Après notre discussion avec notre encadrant, M. Toumi et notre responsable de stage Dr M. Fouad, sur le choix des points à auditer, nous avons décidé de nous concentrer sur les risques et les opportunités

Selon notre entretien avec le directeur au sein de la DSI, la réponse à notre question était la suivante : « *Nous utilisons trois phases pour mener une mission d'audit : la phase de préparation, la phase de réalisation et enfin la phase de conclusion* ». Nous avons bien compris comment mener une mission d'audit en suivant ces trois phases.

Section 02: Le déroulement d'audit des systèmes d'information au sein de la DSI de CONDOR ELECTRONICS :

1-Préparation de procédure d'audit des systèmes d'information

D'après la réponse du RSGSI au sein de la DSI : « *Nous avons une procédure que nous utilisons avec ses étapes pour organiser notre travail* ». Nous avons compris que cette procédure contient des étapes à suivre pour élaborer un plan d'audit, telles que l'objet et le domaine d'application, les documents de référence, les responsabilités, les documents exigés pour l'audit SI, l'échantillonnage et le déroulement des audits SI. Après avoir examiné le document sur la procédure d'audit interne du département SI de Condor (PR.SMI.03), nous avons élaboré un ensemble complet de procédures pour auditer les systèmes d'information au sein du département informatique. Notre procédure décrit un processus étape par étape pour mener un audit SI efficace. La procédure fournit des indications sur les responsabilités des personnes impliquées dans le processus d'audit, les documents requis pour l'audit et les méthodes d'échantillonnage utilisées pour sélectionner les systèmes et les processus à examiner.

La procédure décrit également la sélection et la planification des auditeurs, ainsi que les étapes de la réalisation de l'audit à blanc et de l'examen des résultats. En suivant cette procédure, la DSI peut s'assurer que leurs systèmes d'information fonctionnent de manière optimale, et que tout problème ou risque potentiel est identifié et traité rapidement.

Voici la procédure d'audit des systèmes d'information (SI) que nous avons préparée : voir **(Annexe 2)**

1- Objet

La présente procédure définit les exigences d'audit des systèmes d'information et ce conformément à la réglementation et aux bonnes pratiques en matière de management des systèmes d'information.

2- Domaine d'application

Cette procédure s'applique sur les systèmes d'information de la DSI de Condor Electronics.

3- Documents de Références

- **ISO 19011 : 2018** : Norme internationale qui établit des directives pour l'audit des systèmes de management.
- **ISO 20000 :2018** : Norme de système de management des services (SMS).

4- Responsabilités

Fonction	Responsabilités
Directeur des Systèmes d'information	Le Directeur des Systèmes d'information est responsable de l'approbation de cette procédure.
Responsable d'audit SI	Le Responsable d'audit SI est chargé de l'application de cette procédure de sa mise à jour lorsque c'est nécessaire.
Les Audités	Les audités de la Direction SI veillent à l'application de cette procédure.
Observateurs	Les observateurs sont responsables du respect et de la compréhension de cette procédure.

Tableau 08: les Responsabilités durant la mission d'audit SI (Élaboré par nous même)

7. Les documents exigés pour l'audit SI

La liste des documents suivante est requise pour l'audit des systèmes d'information, c'est une liste non-exhaustive :

- L'ensemble de la documentation ITSMS approuvées par la direction SI,
- L'ensemble de la documentation qui couvre les domaines suivants :
  - La maîtrise documentaire ;
  - La manipulation des actifs informationnels ;
  - L'acquisition, le développement et la maintenance des SI ;
  - Protection contre les logiciels malveillants ;
  - Sauvegarde et restauration des données informatiques ;
  - La gestion des plateformes de messagerie électronique ;
  - La gestion des accès logiques (Réseaux, Systèmes et Applications)
  - La gestion des changements ;
  - La gestion des projets SI.
- L'inventaire du parc informatique (Logiciels & Matériels).

7. Echantillonnage

Les critères d'échantillonnage pour chaque type de composante du système d'information à auditer doivent être bien définis et justifiés. Le processus de collecte, d'analyse, d'interprétation et de documentation de l'information est contrôlé afin de confirmer que les objectifs d'audit sont atteints et que l'objectivité de l'auditeur est maintenue.

8. Déroulement des Audits SI

8.1 Sélection des Auditeurs SI

- Les équipes d'audit sont désignées par le Directeur SI selon les critères suivants :
    - Avoir les compétences requises selon le champ et les critères d'audit ;
    - Avoir les connaissances requises à la gestion des risques des systèmes d'information ;
    - Le volume et la complexité des systèmes d'information à auditer.
- Les responsables d'audit SI sont sélectionnés par le Directeur SI.
- Sur décision du Directeur SI et information de l'audité, un ou plusieurs observateurs peuvent être présents à titre de formation/ qualification aux techniques d'audit SI.
- La DSI peut faire appel à des auditeurs externes. La sélection des Auditeurs Externe pour la réalisation des audits SI doit répondre aux conditions suivantes :
    - Auditeur Tierce Partie en SI ;
    - Certificat de Qualification Valide ;
    - Ayant une expérience de 3 ans dans l'activité des Audits SI Tierce Partie.

8.2 Planification des Audits

Une fois par an, un programme d'audit SI est établi (**Annexe 04**) sur la base des résultats d'audits précédents et compte tenu sur les points suivants :

- L'évolution des systèmes d'information ;
- Les objectifs et enjeux internes et externes ;
- Les besoins et attentes des parties intéressées pertinentes ;
- Les risques et opportunités.

Cette fréquence annuelle peut être revue sur la base du niveau de maturité des systèmes d'information, ou à la suite d'une dysfonction ou changement important.

Nous définissons un Plan d'Audit SI **(Annexe 05)** établies en collaboration avec le RGSI, qui comporte les données suivantes :

- ✓ Objectif d'audit SI ;
- ✓ Critères d'audit SI ;
- ✓ La durée de l'audit SI ;
- ✓ Les systèmes d'information à auditer ;
- ✓ Les exigences et les domaines à auditer ;
- ✓ Affectation des auditeurs ;

Le plan d'audit SI est diffusé par le RSGSI.

8.3 Réalisation de l'Audit

Réunion d'Ouverture

Le responsable d'audit SI doit procéder à une ouverture d'audit en présence des audités. Le responsable d'audit SI doit présenter les points suivants :

- Les objectifs de l'audit SI ;
- Identifier les audités ;
- Expliquer les limites de l'audit SI ;
- Établir la liste de présence ;
- Présenter le plan d'Audit SI ;
- Explique le déroulement et la méthode de l'audit SI .

=Méthode et techniques d'audit SI

Conformément au programme d'audit SI établi à l'étape de la planification, le Directeur SI sélectionne l'équipe d'audit SI et désigne un responsable d'audit SI qui aura la responsabilité de la conduite de l'audit SI.

Les auditeurs sélectionnés réalisent l'audit SI. Selon le périmètre d'audit SI et le plan d'audit SI déjà défini.

=Constats d'Audit SI (Non-conformités, recommandations)

Pour chaque constat d'audit SI, l'**annexe 05** est remplie. Il contient :

- L'énoncé de la non-conformité ;
- Les critères sur lesquels s'appuie la non-conformité ;

- Le risque relatif à l'écart constaté ;
- Les recommandations.

Le formulaire est transmis à l'audité pour communication du constat et formulation de commentaires. Le rapport est discuté au cours de la réunion de clôture en présence de l'audité.

=Rapport d'Audit

Le Responsable d'Audit SI doit élaborer un rapport final d'Audit SI qui contient au minimum les parties suivantes :

- Objectifs et étendue de l'audit SI ;
- Résultats de l'audit SI ;
- Non-conformité ;
- Recommandations ;
- Commentaires de l'audité.

=Fiches non-conformité et Suivi des plans d'actions

Pour chaque audit SI, une/plusieurs fiche(s) de non-conformité(s) est ouverte conformément à la procédure de maîtrise des non-conformités et actions correctives (**PR.SMI.02**), pour les corrections et les recommandations, et un plan d'action est établi par le Manager du département de la DSI concerné par l'Audit SI et suivi par le RSGSI pour évaluation et clôture des actions.

La pertinence et la mise en œuvre des actions menées peuvent faire objet de vérification dans les prochains Audits SI.

Revue

Le Responsable Standards & Gouvernance SI examine cette procédure si nécessaire ou à la suite de tout changement organisationnel, technique ou législatif.

2-Les trois phases d'une mission d'audit :

A-La phase de préparation d'audit des systèmes d'information :

1. Le programme d'audit des systèmes d'information :

Selon notre entretien avec le directeur au sein de la DSI, la réponse à notre question était la suivante : « *Nous avons effectué des audits au sein de notre direction chaque année, parfois deux fois par an et parfois une fois par an, surtout ces dernières années* ». Nous avons bien compris que les audits ont lieu chaque année, une ou deux fois par an. La DSI (Direction des Systèmes d'Information) établit un programme annuel d'audits internes, qui peut être complété par des audits internes partiels tout au long de l'année. Notamment lorsque les résultats attendus ne sont pas atteints ou lorsque les résultats des audits précédents le justifient.

En outre, nous avons effectué un programme d'audit SI qui a été finalisé le 02/05/2023. Ce programme a été recommandé par le responsable de la gouvernance et des normes SI pour être exécuté deux fois par an. Voir **(Annexe 4)**

2. Préparation de plan d'audit :

Nous avons rédigé un document décrivant un plan d'audit pour le département Systèmes d'Information (SI) de Condor Electronics, qui porte sur la fourniture de services SI. Notre plan prévoit que le responsable de l'audit du SI (RSSI) sera chargé de mener l'audit, tandis que nous participerons en tant qu'observateurs. L'objectif de cet audit est d'évaluer la pertinence, l'adéquation et l'efficacité permanente des processus SI, sur la base des critères définis par la norme ISO 20000:2018.

L'audit aura lieu le 9 mai 2023 et devrait durer une journée. La réunion d'ouverture débutera à 9h00 et sera suivie d'une série de rencontres avec différents responsables de différents aspects du fonctionnement de la DSI.

Au cours de l'audit, les domaines identifiés sur la base des risques et opportunités identifiés dans l'analyse SWOT seront examinés, en particulier en ce qui concerne les exigences et les mesures que nous avons mentionnées dans le tableau.

L'audit se terminera par une réunion de clôture à 11h30, au cours de laquelle l'équipe d'audit présentera ses conclusions dans un rapport décrivant ses observations, y compris les domaines nécessitant des améliorations pour assurer la conformité aux normes ISO 20000:2018, Voir **(Annexe 06)**

Domaine d'Application Audit SI : Les systèmes d'information de la Direction SI de Condor Electronics
Champ d'Audit SI : La fourniture des services informatique (Processus SI)
Critères d'audit SI : Politiques, procédures associées, et toutes autres exigences légales applicables (ISO 20000 : 2018)**.**
Responsable Audit SI : RSSI **Équipé Audit :** RSSI + Observateurs
Nom & Prénom Elyes MATOUG
Nom & Prénom : Hanane BOUDISSA (ObN°1)
Nom & Prénom : Randa Lamis LEGHLEM (ObN°02)
Date d'Audit SI : 09/05/2023 **Durée Audit SI (h/jrs) :** 01 jour
Objectifs de l'audit SI : Évaluation de la pertinence, l'adéquation et l'efficacité continues.

Date : 09/05/2023

Réunion d'Ouverture : 09/05/2023 9H00

H/ Durée	Système / Domaine	Auditeurs	Audités	Exigences/ Mesures
9H15	- **8.7.1** Disponibilité des services Infrastructures SI. - **8.2.1** Améliorer la fourniture des services Infrastructures SI.	**RA ObN°1 ObN°2**	**Manager INFRA SI**	- La livraison des services informatiques. - Évaluation de la disponibilité des services informatiques. - Mesure la satisfaction des clients de la DSI.
09H45	- **8.7.1** Disponibilité des services supports SI & Master Data. - **8.2.1** Améliorer la fourniture des services supports SI & Master Data.		**Manager S&MD**	
10H15	- **7.2** Réalisation de la sous-traitance. - **8.7.3** La sécurité des applications développées		**Manager E&D SI**	- Établir des contrats. - Établir des cahiers de charges explicites des besoins.

				- Test de sécurité des sites web & applications.
10H45	- **5.2** Engagement de la direction générale pour l'évaluation de la fonction SI		**RSGSI**	- Respect des exigences réglementaires-performance du processus SI.
11H30	**Réunion de Clôture : Présentation Rapport de Constatation**			

Figure 15 : Plan d'audit 09 mai 2023 (Élaboré par nous même)

B- La phase de la réalisation d'audit SI :

La phase de la réalisation de cette mission audit SI, qui est un audit à blanc, contient les étapes suivantes :

1. Réunion d'ouverture

La réunion d'ouverture a eu lieu le mardi 9 mai 2023 à 9h dans la salle de conférence de la Direction des Systèmes d'Information.

Parmi les participants, le Directeur des Systèmes d'Information, le Responsable d'Audit ainsi que la sécurité du système d'information, les audités ainsi que nous, en tant qu'observatrices.

Au début de la réunion d'ouverture, notre responsable a présenté les pilotes de processus qui sont les membres de l'équipe d'audit et a expliqué leurs rôles et responsabilités, ainsi que le but de cette mission, la portée et l'approche d'audit qui sera utilisée (voir Annexe de procédure). Ensuite, le plan et le référentiel ISO 20000.

Le responsable d'audit Mr ***Elyes MATOUG*** – Responsable Sécurité SI (Certifié ISO 27001 LE).

Prise la parole pour présenter l'équipe d'audit, et expliquer

Quelques points:

-L'objectif de l'audit.

-Les référentiels applicables lors cet audit (iso 20000).

-Les audités qui sont :

- ***Abdelhalim BENSALEM*** – Manager S&MD ;
- ***Ammar BLIZAK*** – Manager Infra SI ;
- ***Belkacem CHENITI*** – Manager E&D SI ;
- ***Mohammed FOUAD*** – RSGSI,

- Les observatrices d'audit SI qui sont :

- ***Hanane BOUDISSA*** – Stagiaire ;
- ***Randa Lamis LEGHLAM*** – Stagiaire,

-Rappeler que l'audit ce n'est pas un jugement de personne.

-Confirmer l'accord de tous les participants concernant le plan d'audit.

-Confirmer la date et l'heure de la réunion de clôture pour le 09 Mai 2023 à 11h30

2. Travail sur terrain

Le responsable d'audit a procédé à une évaluation des audités et a posé des questions concernant les domaines des risques et d'opportunités qui ont été identifiés dans l'analyse SWOT (norme ISO 20000) que nous avons déjà définie dans la plan d'audit voir **(Annexe 6)**

2.1 Manager Infrastructure Si

L'évaluation initiale a commencée à 9h15 avec le Manager d'infrastructure SI qui est basé sur deux domaines : 1- La disponibilité des services d'infrastructure SI

2-Améliorer la fourniture des services d'infrastructure IT

L'auditeur a posé les questions suivantes concernant le premier domaine :

- En se concentrant sur l'exigence de livraison des services informatiques, la première question que le responsable d'audit a posée était : **En tant que fournisseur de services SI en interne, quels sont les moyens disponibles pour assurer la livraison des services informatiques (la pertinence de ces moyens) ?**

Selon le Manager d'infrastructure SI, il existe quatre types de moyens :

« *1-Des ressources humaines en interne qui sont des experts, des ingénieurs et des techniciens dans le domaine informatique*

2-Des moyens externes : tous les fournisseurs de services externes (des fournisseurs externes qui livrent des services pour les clients internes)

3-Des processus organisationnels : il existe des politiques et des procédures

4-Des moyens technologiques et des services IT »

- La deuxième question dans le cadre de l'évaluation de la disponibilité des services informatiques était ***:*** **En tant que fournisseur de services SI en interne, quelles sont les mesures de performance adoptées ?**

Le manager a annoncé « *On utilise des KPI (indicateurs clés de performance) dans le domaine des systèmes de management intégrés calculés mensuellement en temps réel, ainsi que la surveillance monitoring hors et en les heures de travail (surveillance en temps réel*».

Ensuite, le responsable a montré la fiche de processus SI qui contient les indicateurs de disponibilité côté infrastructure, certains d'entre eux étant :

- Le taux de clôture d'un ticket.
- Le taux de réponse moyenne.
- Le taux de disponibilité des Data Centres.
- Le traitement des incidents (incidents liés à la performance).
- La disponibilité des actifs réseaux.

Comme preuve de la surveillance en temps réel, il a montré une capture d'écran de la surveillance en temps réel.

- Pour le deuxième domaine dans le cadre de la mesure de la satisfaction des clients SI, la question était : **Quelles sont les mesures de performance adoptées (les KPI, les plans d'action, etc.) ?**

La réponse était : «*il existait des SLA (Service-Level Agreement) définis par les KPI. Pour les clients, il y a un temps très défini pour répondre à leur demande (un intervalle de temps pour répondre) ainsi que la traçabilité de l'état de leur demande et une Plateforme pour exprimer leurs besoins ou les utilisateurs peuvent suivre toutes les réponses de la DSI* ».

2.2 Manager Support & Master Data

L'audit de manager Support & Master Data a commencé à 09H45 qui a était basé sur deux domaines : -1 Disponibilité des services supports SI & Master Data.

-2 Améliorer la fourniture des services supports SI & Master Data.

Concernant le premier domaine l'auditeur a posé les questions suivantes :

- En se concentrant sur l'exigence de livraison des services informatiques, la première question que le responsable d'audit a posée était : **En tant que**

fournisseur de services SI en interne, quels sont les moyens disponibles pour assurer la livraison des services informatiques (la pertinence de ces moyens) ?

Le Manager Support & Master Data mentionne *« il y a une ressource humaine qui se traduit par une équipe dynamique et compétente, ainsi que des compétences techniques et des outils pour assurer le suivi et l'intégrité des services. Il y a également des outils techniques pour la gestion des incidents qui affectent la disponibilité et l'intégrité des services, ainsi qu'un catalogue de services qui contient les services fournis par l'équipe Support & Master Data à l'utilisateur*».

Et comme une preuve : un catalogue de service (un document public dans le site web du Condor Electronics) .

- Le responsable d'audit a posé une autre question concernant **l'équipe actuelle, à savoir si elle est suffisante pour gérer tout le catalogue de services en cas d'absence, de maladie ou de diminution d'effectifs.**

Dans ce cas, le manager a mentionné « *Mon équipe essaie d'assurer la polyvalence pour éviter toute absence de personnel qui pourrait causer un manque dans le service* ».

- La deuxième question dans le cadre de l'évaluation de la disponibilité des services informatiques était : ***En tant que fournisseur de services SI en interne, quelles sont les mesures de performance adoptées ?***

L'audité annonce qu'il s'appuie sur des indicateur de performance telle que :

-Taux moyen de la première réponse ne dépasse pas la première heure pour assurer que la demande client est plait en charge,

-la réponse est dans le même jour .

- la durée moyen de résolution et pour assurer la productivité d'équipe Support et Master Data la résolution d'incident de client est dans 3 heures.

- Comme question supplémentaire, il a demandé **s'il y a un moyen technique de suivre ces indicateurs en temps réel ?**

La réponse est : «*il existe un tableau de bord spécialisé pour le suivi de l'équipe Support & Master Data qui mis à jour 4 fois par jour et qui contient tous les indicateurs de performance nécessaires pour assurer la fiabilité et la disponibilité des services*».

Cette information est appuyée par une preuve, comme indiqué dans (**l'Annexe 07).**

- Pour le deuxième domaine dans le cadre de la mesure de la satisfaction des clients SI, la question était : **Quelles sont les mesures de performance adoptées (les KPI, les plans d'action, etc.) ?**

Le manager a reconnu que: *« pour faire face aux incidents et demandes répétitifs, mon service de données a lancé un plan de formation et de sensibilisation à destination des clients*». De plus, le manager a déclaré que l'équipe interne de son service est régulièrement évaluée pour garantir un suivi optimal.

- Il a également répondu à la question de l'auditeur qui demandait **s'il existait un indicateur de suivi des réclamations des utilisateurs** avec *« ceux-ci n'ont pas de moyen pour saisir leurs réclamations. et que le réclamant n'a pas le droit de faire une réclamation d'une façon technique* »
- En guise de dernière question, l'auditeur a demandé **si le Manager Support & Master Data a déjà un objectif annuel (plan d'Actions/Formations) dans le domaine de l'amélioration continue de la fourniture de services**.

La réponse était négative donc l'absence d'exécution d'un plan d'action recommande début de l'année.

2.3 Le manager E&D SI :

Après avoir audité les deux managers précédents, le responsable d'audit (RSSI) a procédé à l'audit du troisième manager chargé de l'étude et du développement des systèmes d'information.

Il a commencé à 10h15 en posant des questions en relation avec ce domaine :

• La réalisation de la sous-traitance.

•Les sous domaine /exigences sont :

1-Etablir des contrats.

2-Etablir des cahiers de charges.

- Se concentrant sur les exigences, la première question posée par le responsable d'audit était liée au premier sous-domaine c'est : **il y a-t-il des contrats établis avec des sous-traitant ?**

La réponse du manager était la suivante : *« Actuellement non, il n'y a pas des contrats en place, mais l'édition est largement sous-traitée, par exemple lorsqu'un besoin est externalisé pour privilégier le développement interne. Cela fait deux ans qu'une équipe de*

développement est en place, car avant cela, nous n'avions pas d'équipe dédiée au développement depuis deux ans».

« L'objectif est d'avantage axé sur la satisfaction des besoins métier en interne, avec une forte orientation vers le développement en sous-traitance. En ce qui concerne les contrats, les applications et les systèmes existants, il peut y avoir des contrats de maintenance établis avec les éditeurs, tout comme pour les systèmes de PC. Si vous avez un besoin spécifique de développement ou si vous rencontrez un problème ou un incident, n'hésitez pas à contacter directement les éditeurs concernés ».

Il a présenté une preuve sous la forme d'un cahier des charges de maintenance comme une preuve.

- La deuxième question posée par le responsable d'audit était liée au deuxième sous-domaine c'est : **il y a-t-il des cahiers des charge établis avec des clients ?**

La réponse était la suivante : « *Oui, la démarche d'étude et développement est très importante dans le cycle de vie d'un projet, qui comprend l'orientation, l'étude et le développement. Qui sont deux départements ou équipes qui gèrent les systèmes déjà existants, tels que les ERP et les CRM, par exemple, ainsi, il y a toujours un besoin spécifique qui nécessite le développement ou l'ajout de fonctionnalités dans ces systèmes, comme c'est le cas pour les équipes d'édition et de développement. Pour le développement des applications ou des logiciels, il est nécessaire de suivre le cycle de vie de développement. Le déclencheur de cycle de vie c'est bien un besoin d'un cahier des charge* ».

«*En réalité, il est rare de trouver un cahier des charges complet qui respecte toutes les exigences. Cependant, il est possible de recevoir des besoins sous forme de mails ou de manière informelle par téléphone ou par mail. Nous pouvons organiser une réunion afin de spécifier les besoins. En fonction de la réunion, nous pouvons ensuite réaliser un procès-verbal ou un cahier des charges pour formaliser ces besoins. Si le besoin est petit, nous n'avons pas besoin de faire un cahier des charges. Il suffit simplement de réaliser un document qui exprime le besoin, comme une explication des changements à apporter sur un site web ou une application mobile. En revanche, pour un grand projet, la première étape consiste à faire un cahier des charges. En général, le cahier des charges est spécifique aux grands projets tels que la réalisation d'un site web ou d'une application mobile*».

"Dans le cycle de vie de réalisation d'un projet, il existe un document critique qui est la charte de projet, qui contient les besoins, les objectifs et les plannings initiaux des clients».

- En résumé, les besoins ne sont pas toujours formalisés sous forme de cahier des charges, mais peuvent également être décrits dans des documents.

• **Un exemple :** Le cahier des charges de la DSI de Condor Electronics était la réalisation d'un site web, pour lequel un cahier des charges complet avait été établi.

-La plateforme GLPI (GLPI est un logiciel libre de gestion des services informatiques et de gestion des services d'assistance utilisent par les directions de condor)

- La question suivante concernant le deuxième domaine qui est La sécurité des applications développées. Avec le sous domaine ; Le test de sécurité des sites web & applications. , En se concentrant sur l'exigence la question que le responsable d'audit a posée était la suivante : **Il y a-t-il des rapports des tests des applications/sites web ?**

La réponse du Manager était la suivante :

«*Oui, il y a une tâche principale et des tests de développement qui ont été sélectionnés par les développeurs. Nous avons fait un choix critique pour couvrir certains aspects liés à la sécurité. Avant de valider les projets, nous effectuons les tâches et les tests métier. En ce qui concerne les tests de sécurité, nous les partageons avec le RSSI.*»

2.4 Le Responsable Standards et Gouvernance SI :

Après avoir audité les trois managers précédents, le responsable d'audit (RSSI) a commencé l'audit avec le dernier responsable qui est en charge des Standards et de la Gouvernance des SI à 10h45.

Le premier domaine dont on parle est celui de : L'engagement de la direction générale pour l'évaluation de la fonction SI.

•Les sous domaine : Respecte des exigences réglementaires/ performance de processus SI.

- La question concernant l'audité était la suivante : **Quels sont les preuves (politiques, procédures,…) qui sont appliquées dans la DSI pour concrétiser l'engagement de la DG ?**

Voici la réponse donnée :

« Comme première preuve, nous pouvons présenter la procédure de la stratégie de gouvernance des SI qui a été validée par le directeur général (DG). Cette procédure c'est

une cadre de travail de la standard et gouvernance dans la DSI (procédure V3) cette procédure était en 2020 et nous avons fait la mise à jour en 2021 et 2022, la procédure contient la gestion d'un plan stratégique des SI (R° : procédure gouvernance PR.SI.01) et le logigramme et l'activité de gouvernance SI de la DSI».

- L'auditeur a posé cette question : ***Est-ce que le plan stratégie déjà établis*** **?**

Voici comment la réponse a été formulée :

« oui, il est établi qu'une première version a été créée, mais elle n'a pas été mise à jour entre 2019 et 2021, Procédure manuelle du standard. »

- *il a ajouté question supplémentaire :* ***Comment vérifier les standard il est met dans le site ?***

La réponse était la suivante :

« *Non, Il n'y en a pas, mais il y a un projet en cours, et voici la preuve du projet. Les moyens techniques de partage de l'information sont : le partage et le SharePoint* ».

Les limites d'audit SI

Sur la base de notre évaluation précédente, il est apparu que l'approche actuelle des audits des systèmes d'information (SI) est limitée dans sa portée, se concentrant uniquement sur les trois principaux risques et opportunités identifiés dans l'analyse SWOT.

Pour améliorer la qualité et la rigueur de notre processus d'audit, il est crucial de mettre en place une méthodologie plus fine. Cette approche révisée englobe un plus large éventail de risques et d'opportunités, assurant un examen complet de l'infrastructure des SI de l'organisation.

C- La phase de conclusion d'audit interne :

1. Préparation les conclusions d'audit :

Avant la réunion de clôture, nous avons tenu une réunion de consolidation qui s'est étendue sur une heure et demie. Pendant cette réunion, le responsable d'audit a passé en revue toutes les observations et preuves tangibles collectées lors de l'audit SI .

Cette phase vise à formuler et classer les conclusions de l'audit, en suivant le classement défini dans la procédure d'audit SI de la DSI de SAP Condor pour classer les constats d'audit :

•Les points forts.

•Non-conformité.

1.1 Les points forts :

Audités	Domaine	Points Forts
Manager Support et Master Data SI	Disponibilité des services supports SI et Master Data	1-Le catalogue de service
		2-Équipe humaine compétente dynamique.
	Améliorer la fourniture des services Support et Master Data	1-Gestion des demandes et incidents uniques.
		2-Les sessions de formations des utilisateurs.
Manager Etude et Dev SI	-Réalisation de la sous traitance	1--La charte de projet
		2-contrôle des éditeurs de solution TI
		3-Les réunions d'ouverture
		4-La codification des projets uniques et standardisés
		5-La plateforme de gestion des projets qui répond au besoin actuel
	-La sécurité des applications développées	1-Existence de Rapport de test avec des outils techniques (Nisus) et de plusieurs sites et applications qui sont développés avec des tests de sécurité
		2-Il y a de pinterest qui était programmé à une date ultérieure pour refaire des tests externe par rapport à ces applications et sites web
	Engagement de la	1-Exécution des plans des réunions de la DSI à 87

RSGSI	direction générale pour l'évaluation de la fonction Sl	%
		2-Existence un Manuel des Standards pour : -Infrastructure -Etude et développement -Sécurité -Support et Master Data
		3-Existence des Moyens de collaborations et de communication pour tous les utilisateurs SI (partage + SharePoint)
		4-Existence de la documentation Formelle
		5-un planning de réunions très riche qui gère : -L'état d'avancement des projets -Les problèmes rencontrés -Les situations d'urgence
Manager Infra SI	Disponibilité des services infrastructure SI	Evaluation et monitoring en temps réel
	Améliorer la fourniture des infrastructures SI	//

Tableau 09 : Des points forts des audités (élaborés par nous meme)

1.2 Les non-conformités :

En l'absence de la formation ITIL V4, les deux managers n'ont pas suivi la formation ITIL V4, bien qu'ils aient mentionné des notions liées à ITIL V4 lors de l'audit. Cela a conduit à un niveau de maturité inférieur des éléments de la DSI en raison de l'absence de formation ITIL V4.

Manager Support et Master Data SI	Absence de la formation ITIL V4
Manager Infra SI	Absence de la formation ITIL V4

Tableau 10 : Les non-conformités des audités

2. La réunion de clôture :

La clôture de l'audit interne a été marquée par une réunion qui s'est tenue conformément au plan d'audit interne le 9 mai 2023 à 13h dans la salle des réunions.

Cette réunion, qui a duré 1h15, a été inaugurée par le directeur général de la DSI qui a exprimé sa gratitude envers le responsable d'audit ainsi que tous les participants, lesquels étaient identiques à ceux présents lors de la réunion d'ouverture.
L'objectif de cette réunion est de susciter un débat entre les personnes qui effectuent l'audit et celles qui sont auditées, afin de communiquer et de valider les constats obtenus.

3 Le rapport d'audit :

Sous la supervision de notre superviseur de stage (RSGSI) et du responsable d'audit, nous avons rempli les rapports d'audit, qui ont été partagés par RSGSI avec tous les managers après la réunion d'audit. Le partage du rapport avait pour but de rechercher leur accord sur les conclusions ou de fournir des justifications en cas de désaccord ou de non-conformité avec le processus.

Le rapport a également été envoyé aux Managers de processus et au directeur des systèmes d'information le 09 mai 2023. Voir (**Annexe 05**)
Le rapport de Constatation d'Audit Sl du 09/0512023 de Condor Electronics comprend :

- Le responsable d'audit ;
- L'Audité ;
- Les Non-conformités ;
- Critère (Documents de Références) ;
- Recommandations ;
- Commentaires de l'audite (doit être rempli par l'Audité) ;
- Justification du choix ou autres commentaires ;
- Recommandation mise en œuvre durant l'Audit Sl ;

- Recommandation en cours de la mise en œuvre ;

SSECTION 03: Résultats et Recommandations :

Suite à l'élaboration d'un rapport d'audit, les résultats de l'évaluation ont révélé de nombreux axes d'amélioration importants dans la gestion des Systèmes d'Information (SI) de la DSI, sous forme de recommandations.

L'auditeur doit confirmer l'état d'avancement de la mise en œuvre des recommandations avec les audités et s'assurer que les activités suggérées ont été réalisées par le biais de tests et faire des plans d'action et une mise à jour d'analyse SWOT.

Si des recommandations spécifiques n'ont pas été mises en œuvre, l'auditeur doit analyser les raisons et les difficultés rencontrées lors de leur mise en œuvre.
Les recommandations suivantes ont été faites :

Manager Support et Master Data SI	-Améliorer la fréquence de mise à jour de tableau de bord -plate-forme technique de réclamation des clients SI standardisés
Manager Infra SI	-Un système de sondage des utilisateurs Si La gestion de réclamations des utilisateurs SI
Manager Etude et Dev SI	-Exiger un cahier de charge standardisé pour les expressions des besoins des clients SI Un pinter est globale pour les systèmes et les applications SI
RSGSI	-Mise à jour de plan stratégique SI -établissement de comité stratégique SI -réunion de gouvernance SI /métiers Contrôle des standards en vigueur non formalisé

Tableau 11 : Les recommandations

Conclusion

Nous concluons notre travail en rappelant nos objectifs initiaux, la méthodologie adoptée pour répondre à la question de recherche, les résultats obtenus et les recommandations formulées.

L'objectif initial de cette recherche était de développer une procédure d'audit interne des systèmes d'information (SI) et de mener cette mission en respectant les exigences de la norme ISO 20000:2018, tout en appliquant les lignes directrices de la norme ISO 19011:2018 au sein de la Direction des Systèmes d'Information (DSI) de Condor ÉLECTIONICS.

Pour atteindre ces objectifs, nous avons divisé notre travail en deux parties : une partie théorique et une partie pratique. La partie théorique comprenait une revue de la littérature et l'exploration des principaux concepts liés aux systèmes d'information, à la norme ISO 20000 et à l'audit des systèmes d'information, ainsi que les étapes nécessaires pour réaliser un audit SI efficace selon les exigences de la norme ISO 20000. Le deuxième chapitre a porté sur le choix de l'entreprise et la méthodologie de recherche.

La partie pratique s'est concentrée sur l'élaboration de la procédure d'audit des systèmes d'information (SI) et sur le déroulement de la mission d'audit des systèmes d'information pour vérifier le niveau de conformité du fournisseur des services IT de l'organisme.

L'audit SI est un dispositif essentiel pour détecter, éliminer et prévoir les non-conformités et les dysfonctionnements, tout en identifiant des pistes d'amélioration continue. En conclusion, l'audit des systèmes d'information selon la norme ISO 20000 permet non seulement de garantir la conformité du système de management de l'entreprise, mais aussi d'identifier les lacunes éventuelles et les domaines à améliorer. Cela permet de mettre en place des actions correctives et d'assurer la continuité des services IT, contribuant ainsi à la satisfaction des clients et aux exigences des parties prenantes.

Les résultats de notre recherche sont les suivants :

1. Élaboration d'une procédure d'audit interne des systèmes d'information (SI) pour se conformer à à la norme ISO 20000:2018.
2. Mise en place d'une mission d'audit des systèmes d'information pour évaluer le niveau de conformité du fournisseur des services IT.
3. Identification des domaines de conformité et des éventuelles non-conformités ou lacunes dans les systèmes d'information.

4. Formulation de recommandations spécifiques pour remédier aux non-conformités identifiées et améliorer les pratiques et les processus des systèmes d'information.
5. Contribution à la pérennité et à l'efficacité des systèmes d'information au sein de l'organisme.
6. Identification des opportunités d'amélioration continue dans la gestion des systèmes d'information.
7. Amélioration de la satisfaction des clients envers les services IT.

Enfin, il est important que chaque organisme prenne conscience de l'importance de réaliser un audit SI au moins une fois par an afin de mesurer l'efficacité de l'information au sein de la DSI et de garantir sa pérennité. Cela contribue à assurer la satisfaction des clients et à répondre aux attentes des parties prenantes.

RÉFÉRENCES BIBLIOGRAPHIQUES

Ouvrage :

1. Axelos. (2019). Qu'est-ce qu'ITIL? Extrait de : https://www.axelos.com/fr/itil-framework/what-is-itil.
2. CRIPP - Cadre de référence internationale des pratiques professionnelles - Edition 2017.
3. Hudin-Hengoat, Oona, Le Gallo, Nathalie, & Vidalenc, Sylvie. (2022). DCG 8 Systèmes d'information de gestion, édition 2, pages 5-6.
4. Demeure, Claude & Berteloot, Sylvain. (2015). Aide à la mémoire - Marketing.
5. Soutenain, Jean-François, Echeviller, Jean-Louis, Balny, David. DSCG 5 - Management des systèmes d'information, pages 334, 339.
6. Garrette, B., Dussauge, P., & Durand, R. (2016). STRATEGOR, 2009.
7. GTAG - 2ème édition, Les contrôles et les risques des systèmes d'informations.
8. Teneau, Gilles & Ahanda, Jean-Guy. (2009). Guide commenté des normes et référentiels.
9. Guide pratique du CHAI - Guide d'audit des systèmes d'information, Version 1.0, juin 2014.
10. Weber, Ron. (2010). Information Systems Control and Audit, 1er Edition.
11. Barnes, Jeffrey T. (2017). Information Technology Service Management (ITSM) - A Practitioner's Guide. CRC Press.
12. ISO/IEC 20000-1:2018 - Technologies de l'information - Gestion de services. Récupéré depuis https://www.iso.org/fr/standard/70636.html
13. Axelos. (2019). ITIL Foundation Handbook: ITIL 4 Edition. TSO (The Stationery Office).
14. Selmer, Caroline. (2019). La matrice SWOT. In La boîte à outils du contrôle de gestion.
15. Romelaer, Pierre. (2005). L'entretien de recherche. In Management des ressources humaines, Chapter 4.
16. Mikol, Alain. (2000). "Forme d'audit : L'audit interne." In Encyclopédie de comptabilité, contrôle de gestion et audit. Economica, Paris, page 733.
17. Reix, Robert, Fallery, Bernard, & Kalika, Michel. (2011). Systèmes d'information et management des organisations, edition 6, pages 4-5.
18. Reix. (n.d.). Système d'information et management des organisations, Ed 6.
19. Renard, J. (2009). Théorie et pratique de l'audit interne, 7ème édition. Eyrolles, Paris.
20. Renard, J. (2011). Théorie et pratique de l'audit interne, 9ème édition. Eyrolles, Paris.
21. Garrette, B., Lehmann-Ortega, L., Leroy, F., Dussauge, P., Durand, R., et al. (2016). STRATEGOR: L'analyse interne et externe : le modèle SWOT. Paris:Dunod.
22. Wachyu, Wahid & Winarto, Adi (2022). Audit Sistem Informatis**.**

Articles de revues :

23.Andry & Setiawan, 2019 et Arisanti, 2011, utilisation d'un audit avec approche informatique à l'aide des techniques d'audit assistées par ordinateur. : Information System and Emerging Technology Journal. Vol.2,No.2,December 2021)

24. BEN BOUBAKARY,2020,AUDIT INTERNE ET PERFORMANCE DES ENTREPRISES : International Journal Of Economics and Management Research, Volume N°1, N°2 Juillet-Décembre 2020

25. Oktania Purwaningrum, Baitun Nadhiroh, Siti Moukaromah,2021,Revue littérature de l'audit des systèmes d'information : Jurnal Informatika dan Sistem Informasi (JIFoSI) Vol. 2, No. 3. November 2021

26. Putu Dhanu Driya,IGusti Lanang Agung Raditra Putra, IMade Ardwi Pradnyana,2021,Techniques de collecte de données sur l'audit des systèmes d'information à l'aide du cadre COBIT : :Information System and Emerging TechnologyJournal. Vol.2,No.2,December 2021

27. Younes EL KHATTAB ,Youness ZOUAIR,2021,Audit interne et gestion des risques opérationnels. : Revue du Contrôle de la Comptabilité et de l'Audit ,Vol 5, No 4 page : 408-432

28. Ziani Abdelhak,2019,Le rôle de l'audit interne dans l'amélioration de la gouvernance d'entreprise : Revue du Contrôle de la Comptabilité et de l'Audit ,No 8 :Mars 2019.

Webographie :

29. https://www.scribbr.fr/methodologie/entretien-recherche/ Consulté le 29 avril à 19.44.

30. https://www.axelos.com/fr/itil-framework/what-is-itil. Consulté le 29 avril à 15.30.

31. https://inspirit-digital.com/audit-systeme-information Consulté le 29 avril à 17 :45.

32.Ccomptes.dz/wp-content/uploads/2022/03/GUIDE-AUDIT-INFORMATIQUE. Consulté le 29 avril à 20 :30.

ANNEXES

Annexe 01 : Guide d'entretien

Guide d'entretien

PREMIÈRE PARTIE :

Dans cette partie, nous allons présenter l'interviewer, le sujet de recherche et l'interviewé. Cette étape de l'entretien permet aux deux interlocuteurs de se présenter et d'introduire l'objectif de l'entretien ainsi que celui de la recherche.

DEUXIÈME PARTIE :

Les questions détaillées.

- Les questions de la DSI de SAP Condor Electronics.

Quel est la mission de la direction des systèmes d'information ?

Quel est la vision de la direction des systèmes d'information ?

Quels sont les objectifs stratégiques de la DSI de SAP Condor Electronics ?

Quelles sont les activités de la DSI de SAP Condor Electronics ?

Quel sont les moyens que vous utilisez pour atteindre les objectifs ?

-L'audit interne.

Question principale 1 : pourriez-vous nous décrire le fonctionnement de votre département ? Sous questions:

- Quelles sont les responsabilités liées à votre poste?
- Quelle est votre procédure de travail ?

Question principale 2 : comment est la relation de l'audit interne avec la DSI de SAP Condor ? Sous questions :

- Quelle est la date de la mise en place de la fonction d'audit interne dans la DSI SAP Condor Electronics ?
- Quels sont les différents audits internes faits par la DSI de SAP Condor Electronics ?
- Est-ce que l'audit interne a une forte relation avec le management de la DSI de SAP Condor Electronics ?

Question principale 03 : Quels sont les critères à utiliser pour évaluer les performances de la DSI auditée ?

Sous questions:

-Comment ces critères seront-ils mesurés et évalués ?

Question principale 04 : Quels sont les risques les plus importants auxquels la direction est confrontée ?

-Quelle sont les méthodes utilisé pour identifier les risques ?

-Comment et avec quels méthodes vous gérer les risques ?

Question principale 05: Comment se passe le processus de conduite d'une mission d'audit interne au sein de la DSI (Condor) ?

sous questions:

-Quelle sont les principales phases d'un audit ?

-Comment élaborer un audit au sein de la DSI (Condor) ?

-Comment faire la procédure d'audit ?

-Questions globales.

- Quels sont les principaux risques liés au SI que l'audit peut couvrir ?
- Quelles sont les bonnes pratiques identifiées pour le SI après un audit interne ?

Annexe 02 : PROCÉDURE D'ÉLABORATION D'UN AUDIT SI

Condor Electronics

CONDOR ELECTRONICS
SPA au Capital social de 4 277 000 000,00 DA
Fabrication, commercialisation et SAV d'appareils électroménagers, électroniques produits informatiques et panneaux photovoltaïques
Conception et développement de produits frigorifiques et de climatisation

TÜVRheinland CERTIFIED
ISO 9001:2015
ISO 14001:2015
ISO 45001:2018
Management System
www.tuv.com
ID 9105081967

Direction des systèmes d'information

Procédure d'Audit

Des Systèmes d'Information

Version	Date	Par	Contexte
01	09/03/2023	Hanane BOUDISSA Randa Lamis LEGHLAM	Rédaction
01	14/03/2023	Mohammed FOUAD - RSGSI	Vérification
02	14/04/2023	Mohammed FOUAD - RSGSI	Vérification
02	30/04/2023	Djamila TOUMI - Prof	Validation
02	04/05/2023	Hocine BOULAFRAKH - DSI	Approbation

SPA - Condor Electronics
Direction Systèmes d'Informations
- N° 02 -
Zone d'Activités - B-B-Arréridj

Condor Electronics

CONDOR ELECTRONICS
SPA au Capital social de 4 277 000 000,00 DA
Fabrication, commercialisation et SAV d'appareils électroménagers, électroniques produits informatiques et panneaux photovoltaïques
Conception et développement de produits frigorifiques et de climatisation

SOMMAIRE

1- Objet

La présente procédure définie les exigences d'audit des systèmes d'information et ce conformément à la réglementation et aux bonnes pratiques en matière de management des systèmes d'information.

2- Domaine d'application

Cette procédure s'applique sur les systèmes d'information de la DSI de Condor Electronics.

3- Documents de Références

- ISO 19011 : 2018 : Norme internationale qui établit des directives pour l'audit des systèmes de management.
- ISO 20000 :2018 : Norme de système de management des services (SMS).

4- Définitions et Abréviations

4.1 Définitions

Preuves d'audit : Enregistrements et énoncés de faits qui se rapportent aux critères d'audit et qui sont vérifiables. Les preuves d'audit peuvent être d'ordre qualitatives ou quantitatives.

Critères d'audit : Politiques, procédures ou toutes autres exigences déterminées par rapport auxquelles la conformité du système est évaluée.

Plan d'audit : Les étapes et les activités nécessaires pour réaliser un audit, préparé par le responsable d'audit.

Champ d'audit : Le champ qui décrit les limites, généralement les lieux, les unités organisationnelles, les activités et les processus.

4.1 Abréviations

ITSMS : Système management des services TI ;
DSI : Direction des Systèmes d'Information ;
SI : Systèmes d'Information ;
SMI : Système de Management Intégré ;
RSGSI : Responsable Standards &Gouvernance SI ;
PR.SMI.02 : Procédure de maitrise des non-conformités et actions correctives.

5.Responsabilités

Fonction	Responsabilités
Directeur des Systèmes d'information	Le Directeur des Systèmes d'information est responsable de l'approbation de cette procédure.
Responsable d'audit SI	Le Responsable d'audit SI est chargé de l'application de cette procédure de sa mise à jour l'lorsque c'est nécessaire.
Les Audités	Les audités de la Direction SI veillent à l'application de cette procédure.
Observateurs	Les observateurs sont responsables du respect et de compréhension de cette procédure.

6. Les documents exigés pour l'audit SI

La liste des documents suivante est requise pour l'audit des systèmes d'information, c'est une liste non-exhaustif :

- L'ensemble de la documentation ITSMS approuvées par la direction SI,
- L'ensemble de la documentation qui couvre les domaines suivants :
  - La maitrise documentaire ;
  - La manipulation des actifs informationnels ;
  - L'acquisition, le développement et la maintenance des SI ;
  - Protection contre les logiciels malveillants ;
  - Sauvegarde et restauration des données informatiques ;
  - La gestion des plateformes de messagerie électronique ;
  - La gestion des accès logiques (Réseaux, Systèmes et Applications)
  - La gestion des changements ;
  - La gestion des projets SI.
- L'inventaire du parc informatique (Logiciels & Matériels).

7. Echantillonnage

Les critères d'échantillonnage pour chaque type de composante du système d'information à auditer doivent être bien définis et justifiés. Le processus de collecte, d'analyse, d'interprétation et de documentation de l'information est contrôlé afin de confirmer que les objectifs d'audit sont atteints et que l'objectivité de l'auditeur est maintenue.

8. Déroulement des Audits SI

8.1 Sélection des Auditeurs SI

- Les équipes d'audit sont désignées par le Directeur SI selon les critères suivants :
  - Avoir les compétences requises selon le champ et les critères d'audit ;
  - Avoir les connaissances requises à la gestion des risques des systèmes d'information ;
  - Le volume et la complexité des systèmes d'information à auditer.
- Les responsables d'audit SI sont sélectionnés par le Directeur SI.
- Sur décision du Directeur SI et information de l'audité, un ou plusieurs observateurs, peuvent être présents à titre de formation/ qualification aux techniques d'audit SI.
- La DSI peut faire appel à des Auditeurs Externe. La sélection des Auditeurs Externe pour la réalisation des audits SI doit répondre aux conditions suivantes :
  - Auditeur Tierce Partie en SI ;
  - Certificat de Qualification Valide ;
  - Ayant une expérience minimum de 3 ans dans l'activité des Audits SI Tierce Partie.

8.2 Planification des Audits

Une fois par an, un programme d'audit SI est établi (**Annexe 01**) sur la base des résultats d'audits précédents et compte tenu sur les points suivants :

- L'évolution des systèmes d'information ;
- Les objectifs et enjeux internes et externes ;
- Les besoins et attentes des parties intéressées pertinentes ;
- Les risques et opportunités.

Cette fréquence annuelle peut être revue sur la base du niveau du maturité des systèmes d'information, ou à la suite d'une dysfonction ou changement important.

Le RSGSI définit un Plan d'Audit SI (**Annexe 02**), qui comporte les données suivantes :

- ✓ Objectif d'Audit SI ;
- ✓ Critères d'audit SI ;
- ✓ La durée de l'audit SI ;
- ✓ Les systèmes d'information à auditer ;
- ✓ Les exigences et les domaines à auditer ;
- ✓ Affectation des auditeurs ;

Le plan d'audit SI est diffusé par le RSGSI.

8.3 Réalisation de l'Audit

Réunion d'Ouverture

Le responsable d'Audit SI doit procéder à une ouverture d'audit en présence des audités. Le responsable d'audit SI doit présenter les points suivants :

- Les objectifs de l'audit SI ;
- Identifier les audités ;
- Expliquer les limites de l'audit SI ;
- Établir la liste de présence ;
- Présenter le plan d'Audit SI ;
- Explique le déroulement et la méthode de l'audit SI ;

Méthode et techniques d'audit SI

Conformément au programme d'audit SI établi à l'étape de la planification, le Directeur SI sélectionne l'équipe d'audit SI et désigne un responsable d'audit SI qui aura la responsabilité de la conduite de l'audit SI.

Les auditeurs sélectionnés réalisent l'audit SI. Selon le périmètre d'audit SI et le plan d'audit SI déjà défini.

Constats d'Audit SI (Non-conformités, recommandations)

Pour chaque constat d'audit SI, l'**annexe 03** est rempli. Il contient :

- L'énoncé de la non-conformité ;
- Les critères sur lesquels s'appuie la non-conformité ;
- Le risque relatif à l'écart constaté ;
- Les recommandations.

Le formulaire est transmis à l'audité pour communication du constat et formulation de commentaires. Le rapport est discuté au cours la réunion de clôture en présence de l'audité.

Rapport d'Audit

Le Responsable d'Audit SI doit élaborer un rapport final d'Audit SI qui contient au minimum les parties suivantes :

- Objectifs et étendue de l'audit SI ;
- Résultats de l'audit SI ;
- Non-conformité ;
- Recommandations ;
- Commentaires de l'audité.

Fiches non-conformité et Suivi des plans d'actions

Pour chaque audit SI, une/plusieurs fiche(s) de non-conformité(s) est ouverte conformément à la procédure de maitrise des non-conformités et actions correctives (PR.SMI.02), pour les corrections et les recommandations, et un plan d'action est établi par le Manager du département de la DSI concerné par l'Audit SI et suivi par le RSGSI pour évaluation et clôture des actions.

La pertinence et la mise en œuvre des actions menées peuvent faire objet de vérification dans les prochains Audits SI.

9. Revue

Le Responsable Standards & Gouvernance SI examine cette procédure si nécessaire ou à la suite de tout changement organisationnel, technique ou législatif.

Annexe 03 : Grille d'évaluation standardisée

Occurrence ou probabilité du risque		Négligeable	Perceptible	Important	Fatale	Criticité
		1	2	3	4	
Improbable	1	1	2	3	4	C≤4
Rare	2	2	4	6	8	6≤C≤8
Probable	3	3	6	9	12	
Certaine	4	4	8	12	16	C≥9

Occurrence ou probabilité de l'opportunité		Non importante	importance faible	Important/possible	importance haute	vraisemblance
		1	2	3	4	
Improbable	1	1	2	3	4	V≤4
Peu probable	2	2	4	6	8	6≤V≤8
probable	3	3	6	9	12	
très probable	4	4	8	12	16	V≥9

Si C≥9	Menaces significatifs	Objectifs, efficacité et efficience non atteint (Action exigée)	Si V≥9	Opportunités pertinente	Opportunité claire raisonnable et certaine, se réalise à court terme sur la base de l'organisation actuelle (Action exigée)
Si 6≤C≤8	Menaces peu significatifs	Objectifs et efficience non atteint (Action exigée)	Si 6≤V≤8	Opportunités peu pertinente	Opportunité à atteindre mais demande une organisation attentive (Action exigée)
Si C≤4	Menaces faibles	Objectifs, efficacité et efficience atteint	Si V≤4	Opportunités de faibles pertinences	Opportunité à faible probabilité de succès contenu des ressources organisationnelles actuelles

GRILLE D'EVALUATION DES PARTIES INTERESSEES

INFLUENCE	DIALOGUE	DEPENDANCE
1 = Influence nulle	1 = Absence de dialogue	1 = Dépendance nulle
2 = Influence faible	2 = Dialogue régulier	2 = Dépendance faible
3 = Influence moyenne	3 = Dialogue fréquent	3 = Dépendance moyenne
4 = Influence forte	4 = Dialogue permanent	4 = Dépendance forte
5 = Influence Considérable		5 = Dépendance vitale

SEUIL DE PERTINENCE
Si P ≥ 48 Partie Intéressée Pertinente
Si 19 ≤ P ≤ 47 : Partie Intéressée Peu Pertinente à prendre en compte
Si P≤ 18 : Partie intéressée non pertinente

Annexe 04 : Programme d'Audit des Systèmes de l'information

CONDOR ELECTRONICS

SPA au Capital social de 4 277 000 000,00 DA

Fabrication, commercialisation et SAV d'appareils électroménagers, électroniques produits informatiques et panneaux photovoltaïques

Conception et développement de produits frigorifiques et de climatisation

Annexe 1 : Programme d'Audit des Systèmes de l'information

Date : 02/05/2023

N° Audit	Août	Sept.	Oct.	Nov.	Déc.	Jan.	Fév.	Mars	Avril	Mai	Observations
01								09/05			
02				/							

Visa du Directeur SI

Annexe 05: Plan d'audit

Plan d'Audit SI du 09/05/2023

Domaine d'Application Audit SI : Les systèmes d'information de la Direction SI de Condor Electronics

Champ d'Audit SI : La fourniture des services informatique (Processus SI)

Critères d'audit SI : Politiques, procédures associées, et toutes autres exigences légales applicables (ISO 20000 : 2018).

Responsable Audit SI : RSSI

Équipé Audit : RSSI + Observateurs

Nom & Prénom Elyes MATOUG

Nom & Prénom : Hanane BOUDISSA (ObN°1)
Nom & Prénom : Randa Lamis LEGHLEM (ObN°02)

Date d'Audit SI : 09/05/2023

Durée Audit SI (h/jrs) : 01 jour

Objectifs de l'audit SI : Evaluation de la pertinence, l'adéquation et l'efficacité continues.

Date : 09/05/2023

Réunion d'Ouverture : 09/05/2023 9H00

H/ Durée	Système / Domaine	Auditeurs	Audités	Exigences/ Mesures
9H15	- **8.7.1** Disponibilité des services Infrastructures SI. - **8.2.1** Améliorer la fourniture des services Infrastructures SI.	RA ObN°1 ObN°2	Manager INFRA SI	- La livraison des services informatiques. - Évaluation de la disponibilité des services informatiques. - Mesure la satisfaction des clients de la DSI.
09H45	- **8.7.1** Disponibilité des services supports SI & Master Data. - **8.2.1** Améliorer la fourniture des services supports SI & Master Data.		Manager S&MD	
10H15	- **7.2** Réalisation de la sous-traitance. - **8.7.3** La sécurité des applications développées		Manager E&D SI	- Établir des contrats. - Établir des cahiers de charges explicites des besoins. - Test de sécurité des sites web & applications.
10H45	- **5.2** Engagement de la direction générale pour l'évaluation de la fonction SI		RSGSI	- Respect des exigences réglementaires-performance du processus SI.
11H30	**Réunion de Clôture : Présentation Rapport de Constatation**			

SPA - Condor Electronics
Direction Systèmes d'Informations
- N° 02 -
Zone d'Activité ... B.P-Arrédj

Annexe 06: Rapport de constatation d'audit SI

Manager Infra SI

Rapport de Constatation d'Audit SI du 09/05/2023

Préparé par : RSSI		**Vérifié par :** RSSI	
Non-conformités			
01 / 7.3	Manque De formation ITIL V4		
02			
03			
04			
Critère (Documents de Références)	**Risque (conséquences éventuelles pour la DSI)**		
Recommandations			
01 /8-2.1 02	- Un système de sondages Des Utilisateurs SI		
02 /8-2.1 01	- La gestion De Reclamations des Utilisateurs SI		
03			
04			
Commentaires de l'audité (doit être rempli par l'audité)			
☑ **D'accord avec les non-conformités et recommandations**	☐ **D'accord seulement avec les non-conformités**	☐ **En désaccord avec la ou les non-conformités, préciser celles avec lesquelles vous êtes en désaccord**	☐ **En désaccord avec la ou les recommandations préciser celles avec lesquelles vous êtes en désaccord**
Justification du choix ou autres commentaires			
..... R.A.S			

Recommandation mise en œuvre durant l'Audit SI	**Oui**	**Non**	**Recommandation en cours de mise en œuvre**	**Oui**	**Non**

Le Responsable d'Audit SI
Date et visa

Condor
MATOUG Elyes
Responsable de la Sécurité S.I.
Direction des Systèmes d'Information

le Manager du département de la DSI auditée
Date et visa

BLIZAK Ammar
Manager des Infrastructures SI DSI

Managers et MD

Rapport de Constatation d'Audit SI du 09/05/2023

Préparé par :	Vérifié par :
Non-conformités	
01 / 7.3	Manque de formation Itil V4 / bons pratiqus recommandés
02	
03	
04	
Critère (Documents de Références)	**Risque (conséquences éventuelles pour la DSI)**
Recommandations	
01 / 9.4	Ameliorer la Frequence de Mise a jour De tableau De bord (chaque 4h)
02 / 7.2	Plateforme technique de Reclamation des Utilisateurs SI standarisée
03	
04	

Commentaires de l'audité (doit être rempli par l'audité)

☑ D'accord avec les non-conformités et recommandations	☐ D'accord seulement avec les non-conformités	☐ En désaccord avec la ou les non-conformités, préciser celles avec lesquelles vous êtes en désaccord	☐ En désaccord avec la ou les recommandations préciser celles avec lesquelles vous êtes en désaccord

Justification du choix ou autres commentaires

.....
.....
.....

Recommandation mise en œuvre durant l'Audit SI	Oui	Non	Recommandation en cours de mise en œuvre	Oui	Non

Le Responsable d'Audit SI
Date et visa

Condor
MATOUG Elyes
Responsable de la Sécurité S.I.
Direction des Systèmes d'Information

le Manager du département de la DSI auditée
Date et visa

Condor
BENSALEM Abdelhalim
Manager Support & Master Data DSI

Manager E et D

Rapport de Constatation d'Audit SI du 09/05/2023

Préparé par : RSSI		**Vérifié par :** RSSI	
Non-conformités			
01			
02			
03			
04			
Critère (Documents de Références)	**Risque (conséquences éventuelles pour la DSI)**		
Recommandations			
01 /8-2.1	Exiger Un cahier de charge standarisé pour Les Expressions de Besoin Des clientsde la DSI		
02 /8.7-3	Recommender Un pintrest globale pour les systémes et les Applications SI		
03			
04			
Commentaires de l'audité (doit être rempli par l'audité)			
☒ D'accord avec les non-conformités et recommandations	☐ D'accord seulement avec les non-conformités	☐ En désaccord avec la ou les non-conformités, préciser celles avec lesquelles vous êtes en désaccord	☐ En désaccord avec la ou les recommandations préciser celles avec lesquelles vous êtes en désaccord
Justification du choix ou autres commentaires			
RAS			

Recommandation mise en œuvre durant l'Audit SI	**Oui**	**Non**	**Recommandation en cours de mise en œuvre**	**Oui**	**Non**

Le Responsable d'Audit SI
Date et visa

Condor
MATOUG Elyes
Responsable de la Sécurité S.I.
Direction des Systèmes d'Information

le Manager du département de la DSI auditée
Date et visa

CHENITI Belgacem
Directeur S.I

RSGSI

Rapport de Constatation d'Audit SI du 09/05/2023

Préparé par : RSSI	**Vérifié par :** RSSI

Non-conformités	
01	
02	
03	
04	
Critère (Documents de Références)	**Risque (conséquences éventuelles pour la DSI)**
Recommandations	
01 / 5.2	Mise Ajour de plan Stratégique SI
02 / 5.2	L'Etablissement de comité strategique SI
03 / 9.1	Reunion De gouvernance DSI/Metiers
04 / 9.2	Controle Des standard en vigueur non Formalisé (Projet encours)
Commentaires de l'audité (doit être rempli par l'audité)	

☑ **D'accord avec les non-conformités et recommandations**	☐ **D'accord seulement avec les non-conformités**	☐ **En désaccord avec la ou les non-conformités, préciser celles avec lesquelles vous êtes en désaccord**	☐ **En désaccord avec la ou les recommandations préciser celles avec lesquelles vous êtes en désaccord**

Justification du choix ou autres commentaires

R.A.S

Recommandation mise en œuvre durant l'Audit SI	**Oui**	**Non**	**Recommandation en cours de mise en œuvre**	**Oui**	**Non**

Le Responsable d'Audit SI
Date et visa

Condor
MAHOUG Elyes
Responsable de la Sécurité S.I.
Direction des Systèmes d'information

le Manager du département de la DSI auditée
Date et visa

Condor
Mohammed FOUAD
Responsable Standards & Gouvernance SI
- Direction SI -

ANNEXE 07 : PREUVE (Tableau de bord spécialisé service Support et Master Data)