MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

ÉCOLE NATIONALE SUPÉRIEURE DE MANAGEMENT

ENSM. Pôle Universitaire de KOLÉA

MEMOIRE DE FIN D'ETUDES

Master en management stratégique et système d'information

MODÉLISATION ET ÉVALUATION DE CONFORMITÉ DES PROCESSUS DE CONTROLE DE SÉCURITÉ SI SELON LE STANDARD CSP SWIFT

CAS : AL'SALAM BANQUE ALGERIE

Élaboré par :

RACHEM MOHAMED

Encadré par : Mme TOUMI DJAMILA

Année 2020/2021

Résumé

Les Technologies de l'Information et de la Communication croissent d'une façon très rapide ce qui rend l'environnement des SI très complexe, très turbulent, vulnérable plus exposé aux risques, moins securisé.la gestion des risques et la sécurité SI sont devenues plus une nécessité qu'un choix.

La DSSI au sein d'AL SALAM BANQUE ALGERIE vise comme objectif la sauvegarde et préservation du SI à travers la mise en place d'un dispositif de sécurité prenant en charge tous les aspects inhérents à l'intégralité, la disponibilité et la confidentialité des informations liées à l'activité de la banque. En parallèle elle doit assurer la gestion et le suivi de la politique de sécurité du SI à travers la mise en conformité avec le standards CSP SWIFT. L'objectif de notre travail de recherche est de proposer et développer un processus relatif aux contrôles de la quatrième mesure du programme SWIFT qui va aider le contrôleur à optimiser l'effort , le temps et les ressources, pour mettre en place ce processus optimisé on doit définir les facteurs de risque associé au contrôle et identifier les différents acteurs et leurs rôles et faire une évaluation de la conformité des contrôles à travers l'exploitation des résultats tiré de notre étude qualitative afin de modéliser les processus de contrôle

Mots clés : sécurité des systèmes d'information, gestion des risques, DSSI, conformité, Standards CSP SWIFT, contrôle, processus optimisé, facteur de risque

ABSTRACT

Information and communication technology are growing very fast which makes the information system environment very complex, very turbulent, vulnerable, more exposed to risk, less secure. Risk management and information system security have become more of a necessity than a choice**.**

The DSI Department within AL SALAM BANK ALGERIA aims at safeguarding and preserving the information system through the implementation of a security system taking care of all aspects inherent to the completeness, availability and confidentiality of information related to the bank's activity. In parallel, it must ensure the management and monitoring of the information system security policy through compliance with the CSP SWIFT. The objective of our research work is to propose and develop a process related to

the fourth control of the SWIFT program that will help the controller to optimize effort, time and resources to implement this optimized process we must define the risk factors associated with the control and identify the different actors and their roles carry out an assessment of the conformity of the controls through the use of the results drawn from our qualitative study in order to model the control processes

Keywords: Risk management, DSSI Department, compliance, SWIFT CSP standards, control, optimized process, risk factors, information security

ملخص

تنمو تقنيات المعلومات والاتصالات بسرعة كبيرة مما يجعل بيئة نظم المعلومات معقدة للغاية، ومضطربة وهشة، وأكثر عرضة للمخاطر، وأقل أمانًا للغاية، أصبحت إدارة المخاطر وأمن نظم المعلومات ضرورة أكثر من كونها خيارًا الهدف من عملنا البحثي هو اقتراح و تطوير نموذج للسيطرة على الرقابة الرابعة لبرنامج سويفت و التي تساعد المراقب على تحسين الجهد و الوقت و الموارد، لإعداد هذه العملية، يجب علينا تحديد عوامل الخطر المرتبطة بها، مراقبة وتحديد الجهات الفاعلة المختلفة وأدوارها و إجراء تقييم لمطابقة الضوابط من خلال استخدام النتائج المستمدة من دراستنا النوعية من أجل انجاز نموذج عمليات الرقابة

الكلمات المفتاحية :ادارة المخاطر، نظم المعلومات، برنامج سويفت، عوامل الخطر، الطريقة النوعية، تقرير الامتثال

REMERCIEMENTS

Nous tenons à remercier, en premier lieu, Dieu de nous avoir donné la force et le courage d'accomplir ce modeste travail à terme.

En deuxième lieu, Nous tenons à remercier chaleureusement nos familles pour leur soutient, ainsi que tous ceux qui ont contribués de prêt ou de loin à la réalisation de ce mémoire de fin d'études.

Nos remerciements s'adressent également :

Notre encadreur, Mme TOUMI Djamila, qui en étant qu'encadreur s'est toujours montrée à l'écoute et disponible tout au long de la réalisation de ce mémoire ;

Mr YAHYA HAMIZI ; Mr ADEL BOUROUIS cadre au sein de la banque AL'ASALAM ALGERIE pour leur générosité ;

A l'ensemble des enseignants de l'ENSM, qui ont accompagnés tout au long de notre formation.

Table des matières

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ABREVIATION, SIGLES ET ACRONYMES

CSP : Customer Security Programme

SWIFT : Society For Worldwide Interbank Financial Telecommunications

DSSI : Direction de sécurité des systèmes d'information

SI : Système d'information

ASBA : Al salam banque algeria

ISO : International organization for standardization

EBIOS : Expression des besoins et identification des objectifs de sécurité

MEHARI : Méthode harmonisés d'analyse des risques

PDCA : Plan de continuité d'activité

CIGREF : Club informatique des grandes entreprises françaises

PCI-DSS : Payment card industry data security standard

NIST : National institute of standards and technology

GAB : Guichet automatique de la banque

TPE : Terminaux de paiement électronique

COBIT : Control objectives for information and related technology

SPA : Société par action

COSO : Committee of sponsoring organization of the treadway commission

SOX: Sarbanes-oxley

IFRS: International financial reporting standards

RACI: Responsible, Accontable, Informed, Consulted

CO: Contrôle

MP: Mots de Passe

AMF: authentification multifactorielle

INTRODUCTION

1. L'accroche et l'intérêt du thème

Les banques jouent un rôle très important dans le pays car elles sont là pour servir l'économie, la principale mission de la banque consiste à mobiliser l'épargne à la fructifier par des prêt ou crédits qu'elle accorde aux opérateurs qui en éprouve leur besoin

Le SI est aujourd'hui le cœur métier de toutes les banques grâce à son rôle précieux dans la présentation d'un ensemble de données sous forme de connaissances fiable et dans un moment opportun pour faciliter le processus de décision pour les dirigeants, et aussi il est indispensable pour assurer les transactions vers l'étranger, et pour assurer ces transactions la banque doit sécuriser son SI et protéger ses actifs pour éviter la menace cybernétique qui pèse sur le secteur financier plus forte que jamais

Al'Salam Bank Algeria comme toutes les autres banques a fait un accord de partenariat avec le SWIFT qui fournit désormais un réseau de messagerie interbancaire mondial pour les institutions financières. En 2016, avant la mise en place du CSP, la Banque centrale du Bangladesh, membre du réseau SWIFT, a été victime d'intrusions et de tentatives de détournement de fonds publics, pour cette raison SWIFT a mis en place un plan de sécurité client en 2017, qui oblige ses clients à être conforme vis-à-vis ce programme qui définit 7 mesures de sécurités, chaque mesure contient des contrôles à appliquer, ces points de contrôle doivent être auto-évalués annuellement par le client et audités par un prestataire externe

Donc notre thème est très important car c'est une question qui pose un problème au sein des entreprises. Car, cette année la société SWIFT a lancé des missions d'audit pour vérifier la conformité de ses membres vis-à-vis le CSP SWIFT, donc la conformité de la banque vis-à-vis le CSP SWIFT est devenue une exigence contractuelle de partenariat

2. Contributions théoriques, méthodologiques et managériales :

Cette recherche est consacrée aux études dans le domaine de la gestion de la sécurité des risques des systèmes d'information et les différents standards utilisés dans le domaine et la nécessité de la mise en conformité avec les bonnes pratiques vu son importance dans la sécurité des SI et pérennité de l'entreprise, Nous avons notamment passé en revue de littérature et dans le cadre conceptuel les différentes théories existantes dans la gestion des risques et la sécurité des systèmes d'information, aussi l'ensemble des Normes, Méthodes,

et Standard utilisé dans ce domaine, et ensuite le Framework choisi à appliquer qui celui de CSP SWIFT

Pour répondre à notre question de recherche nous avons fait une évaluation de la conformité de la politique de sécurité de la banque vis-à-vis le CSP SWIFT, où nous avons extrait les métriques de chaque contrôle et faire l'évaluation de la mesure, Aussi, une étude qualitative qui nous a permis de renforcer notre travail qui, s'appuie sur le besoin d'optimiser les contrôles des mesures pour automatiser le travail de contrôleur de la DSSI

L'ensemble des résultats offre de multiples implications managériales notamment en termes de pilotage et justification des budgets de la sécurité, et la quantification de la charge de travail

3. Problématique de la recherche:

Nous avons été amenés à réaliser notre projet de fin d'études au niveau de d'AL SALAM BANK ALGERIA plus précisément dans le département risque et conformité qui est rattaché à la DSSI, ce dernier vise à assurer la gestion et le suivi de la politique de sécurité de SI à travers la mise en conformité avec le standards CSP SWIFT, et nous avons bien repéré le besoin de ce département et proposer une solution de contrôle efficiente grâce aux information fournis par le chef de départements risque et conformité et son intérêt immédiat pour notre spécialité

Nous avons pu tracer notre question principale de recherche comme suit :

Comment peut-on mettre en place un processus optimisé pour le contrôle numéro 4 du programme SWIFT pour assurer une politique efficace en matière de mots de passe et empêcher la violation des facteurs d'authentification ?

Nous avons décomposé cette question principale en sous question :

-Est-ce-que la politique de sécurité de la banque est conforme au contrôle 4 du CSP SWIFT ?

-Quels sont les différents acteurs qui participent dans le contrôle ainsi leurs rôles et les ressources nécessaires ?

-Quels sont les risques associés au contrôle 4 du CSP SWIFT ?

4. Organisation du mémoire :

Ce mémoire est organisé comme suit :

Premier chapitre : nous avons présenté dans la revue de littérature une vision générale sur la gestion des risques des systèmes d'information et dans le cadre conceptuel le processus de gestion des risques SI et les différentes normes, standards et méthodes qui peuvent être utilisées pour protéger les systèmes d'information y compris le CSP SWIFT que nous utiliserons dans notre recherche

Deuxième chapitre : nous avons présenté la méthodologie de recherche suivie pour arriver à répondre à notre question de recherche.

Troisième chapitre : nous allons évaluer la conformité de contrôle numéro 4 du programme SWIFT et proposer un processus optimiser pour le contrôle

CHAPITRE Ⅰ : REVUE DE LITTÉRATURE ET CADRE CONCEPTUEL

1. REVUE DE LITTÉRATURE :

Nous allons essayer à travers ce chapitre de démontrer que notre travail de recherche se réfère à des bases scientifiques et de déterminer les différents concepts clés de notre thématique.

La recherche en SI est une discipline encore jeune , elle commence à peine à prendre ses premières rides, elle intègre plusieurs sciences telles que la science humaines ,la science de l'ingénierie ,ce champ de recherche en l'espace de 25 ans a connu un développement intense et régulier au niveau international grâce à un paradigme qui permet de générer à partir d'un ensemble des assomptions théoriques et méthodologiques des connaissance(Kuhn,1979),ces connaissance offriront des nouvelles perspectives et vision pour le développement SI

Selon (Phelizon et roubier, 2002) la performance de l'entreprise est dû à plusieurs facteurs clés, le SI est l'un des facteurs moderne et grâce à ces fonctionnalité il permet une exécution efficace de la stratégie de l'entreprise et il sert à garantir la sécurité et l'intégrité des données, la traçabilité et l'efficacité des processus de l'organisation

Les SI ont pu gagner une place très importants dans les organisations grâce à l'apparition du big data, cloud, l'évolution du web et le développement technologique

Selon (Deyrieux, 2003) le rôle principale d'un SI est de génère un ensemble d'information fiable qui permet aux décideurs de prendre des décisions appropriées dans les moments les plus adéquats

Le concept de risque varie selon les points de vue, les attitudes et les expériences de chaque individu et il est affecté par sa propre mentalité. Les ingénieurs et les concepteurs regardent risque d'un point de vue technologique. D'autres le regardent d'un point de vue économique et financier ou du point de vue du côté de l'environnement et de la santé (Baloi et Pence, 2003), (Walke, Topkar et Matekar, 2011).

Dans les SI le concept de risque manque également de précision (Wang, X, Williams, M.A, 2010) et d'accord. Les recherches antérieures liées aux systèmes d'information se concentrent principalement sur le développement et les risques de sécurité. (Goldstein, Benaroch, & Tchernobai, 2008)

La gestion des risques est une discipline extrêmement importante dans la gouvernance des systèmes d'information. Ça peut aider organisations avec l'optimisation de leurs coûts dans la mesure où la gestion des incidents nécessitant souvent plus d'efforts. Cependant, il présente un ensemble de défis tant pour les professionnels que pour les chercheurs.

La gestion des risques est «une activité complexe et systématique qui nécessite l'implication de toute l'organisation». (L. Liang, W. Ren, J. Song, 2013). Selon (Simister, 2000), le concept de «gestion des risques» était employé pour la première fois dans des compagnies d'assurance aux États-Unis dans les années 1950. La Gestion des risques passe d'une nécessité à même une obligation qui protège les actifs de l'entreprise mais est également devenue un régulateur obligation dans plusieurs cas. Les risques peuvent être transférés, gérés, minimisés ou partagés, mais ne doivent jamais être ignorés. Face à un risque, nous devons agir. De la même manière, la discipline de gestion des risques a plusieurs définitions qui n'expriment pas forcément le vrai sens et véritable portée de cette discipline. En fait, (Walke, Topkar et Matekar, 2011) affirment qu'il est souvent confus ou limité à l'une des quatre activités suivantes: identification, analyse et suivi et / ou contrôle des risques.

Selon (Dikmen, Birgonul, Anac, Tah, & Aouad, 2008)le processus de gestion de risque est un cycle itératif continu qui passe par: (1) l'identification des risques; dans laquelle les sources d'incertitude sont définies, (2) l'analyse de risque; il s'agit d'évaluer les conséquences d'événements incertains, (3) la réponse au risque: des stratégies appropriées sur la base de l'énoncé des résultats attendus, et 4) l'analyse des résultats du traitement et des risques apparus conduit à une répétition possible des trois premières étapes.

La gestion des risques SI représente une approche structurée de la prise de décision tenant compte des risques de fonctionnement du système d'information de l'entreprise à son appétit pour le risque Dans le même ordre d'idées, le risque Management Guide for US Department of Commerce Information Technology Systems soutient que la gestion des SI doit exister non seulement pour protéger ses actifs informatiques, mais aussi pour «protéger l'organisation et sa capacité à sa mission.

Par conséquent, le processus de gestion des risques ne doit pas être traitée comme une fonction technique exercée par des experts informatiques qui exploitent et gèrent le système informatique, mais comme une fonction de gestion de base de l'organisation. La gestion des risques SI doit être intégrée dans toutes les décisions et opérations

quotidiennes, peut ensuite être utilisé efficacement, considéré comme un outil pour gérer l'information de manière proactive plutôt que réactive

2. Cadre conceptuel :

Le cadre conceptuel selon (Formarier) c'est l'ensemble des connaissances théoriques, qui ont un rapport quelconque avec le sujet de la recherche, nécessitant l'étude de documents qui enrichissent le sujet du mémoire.

2.1 Le concept de gestion des risques SI :

Le concept de gestion des risques (ou risk management) a très certainement fait son apparition à la fin des années 50 aux États-Unis dans le domaine financier, en relation avec des questions d'assurance (Dubois, 1996). Par la suite, la notion de gestion des risques a été étendue à d'autres domaines, citons notamment l'environnement, la gestion de projet, le marketing, ainsi que la sécurité informatique, qui nous intéresse tout particulièrement.

La gestion des risques est définie par l'ISO (ISO/IEC Guide 73) comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque.

De manière générale, la gestion des risques SI a identifié trois objectifs :

1. Améliorer la sécurité des systèmes d'information.

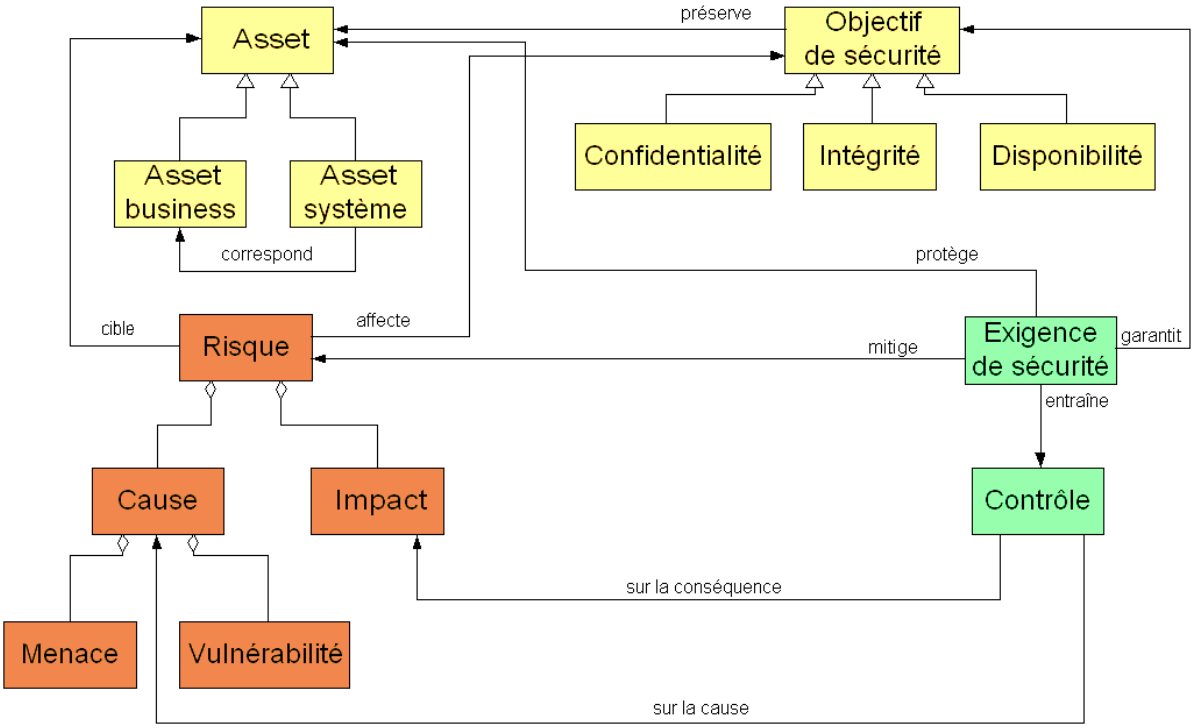
2. Prouver que le budget alloué à la protection du système d'information est raisonnable.

3. Utiliser l'analyse effectuée pour prouver la crédibilité du système d'information.

Bien que beaucoup ne soient plus utilisés ou ne soient plus confidentiels, on estime qu'il existe plus de 200 façons de gérer les risques. Cette diversité a conduit à une grande diversité de méthodes pour faire face aux risques de sécurité.

La gestion des risques « dans sa forme la plus simple » se compose de trois blocs interdépendants. On distingue l'organisation cible de l'étude, qui est définie par ses actifs et ses exigences de sécurité, puis le risque de mise sous pression sur ces actifs, et enfin les mesures prises pour faire face au risque pour assurer un certain degré de sécurité.

Figure 1:Les concepts de la gestion des risques



Source : (Mayer, 2009)

Les assets[1] sont définis comme tous les biens, actifs et ressources qui sont précieux pour l'organisation et nécessaires à son fonctionnement normal. Une distinction est faite ici entre les actifs de niveau métier et les actifs liés à l'informatique. Au niveau des actifs de l'entreprise, nous recherchons principalement des informations (comme les numéros de carte bancaire) et des processus (comme la gestion des transactions ou la gestion des comptes). Les actifs commerciaux d'une organisation sont généralement entièrement (ou presque) gérés via le SI, ce qui fait que ces actifs dépendent de ce dernier. Ceux-ci sont appelés « actifs système ». Dans les actifs du système, nous trouvons des éléments techniques, tels que le matériel, les logiciels et les réseaux, et les environnements de système informatique, tels que les utilisateurs ou les bâtiments. C'est cet ensemble qui forme le SI

Par conséquent, l'objectif de la gestion des risques est d'assurer la sécurité des actifs, qui se manifeste dans la plupart des cas par la confidentialité, l'intégrité et la disponibilité, qui

[1] **Assets** est un anglicisme couramment utilisé dans le domaine qui définit un bien, actif, ressource ayant de la valeur pour l'organisme et nécessaire à son bon fonctionnement.

[2] Synetis : cabinet de conseil en transformation numérique et sécurisation des systèmes d'information

constituent l'objectif de sécurité. Ces actifs protégés présentent des risques pour la sécurité. Le Guide ISO 73 définit le risque par la combinaison de la probabilité d'occurrence d'un événement et de ses conséquences. Cette définition est généralement très large. Nous utilisons ce que l'on appelle « l'équation du risque » pour définir le risque :

Risque = menace * vulnérabilité * impact

Cette équation est l'équation la plus couramment utilisée et reconnue dans le domaine de la gestion des risques. Il joue un rôle important dans l'identification et l'évaluation des risques.

2.2 Terminologies primordiales dans la gestion des risques :

Risque : La norme ISO définit le risque dans les termes suivants : « L'effet de l'incertitude sur l'atteinte des objectifs » (ISO/CEI Guide 73, 2009). Les risques sont généralement caractérisés par des événements et des conséquences potentielles ou une combinaison de ceux-ci. Elle peut être quantifiée en considérant trois éléments : la menace, la vulnérabilité et l'impact

Menace : Une menace peut avoir plusieurs sources, c'est la cause potentielle d'incident, qui peut résulter en un dommage au système ou à l'organisation (ISO/CEI 27002, 2013). Les menaces exploitent les vulnérabilités pour déclencher des attaques qui entraînent des risques

Vulnérabilité : correspond à une faiblesse du système

Impact : est la conséquence directe ou indirecte de l'insatisfaction des besoins de sécurité sur l'organisme et/ou sur son environnement (EBIOS, 2010)

Critères de sécurité :

Les quatre concepts cités peuvent modifier les critères de sécurité, qui sont :

Intégralité : Ce principe vise à garantir l'exactitude et l'exhaustivité des informations et de leurs méthodes de traitement (ISO/IEC 27000, 2016)

• **La confidentialité** : cette condition est de veiller à ce que les informations ne soient pas divulguées ou communiquées à des personnes ou entités qui ne possèdent pas les autorisations appropriées (ISO/CEI 27000, 2016).

• **La disponibilité** : cette notion est la propriété d'être accessible et utilisable sur demande par une entité autorisée (ISO/CEI 27000, 2016).

• **La traçabilité** : cette notion c'est l'assurance que les éléments considérés sont tracés et que ces traces sont conservées pour leur exploitation par les personnes autorisées.

Traitements des risques :

Le traitement du risque est un processus de sélection et de mise en œuvre des mesures de sécurité visant à modifier le risque. Les différents traitements du risque sont :

Optimisation (réduire) : action de diminution de la probabilité, de la conséquence et d'impact qui sont associés à un risque.

Prévention : vise à prévenir l'apparition des risques en utilisant certaines mesures. Les mesures de prévention comprennent la prévention intrinsèque, l'utilisation de dispositifs de protection, d'équipements de protection individuelle, l'information pour l'utilisation et l'installation ainsi que la formation.

Vivre avec (tolérable) : c'est l'acceptation de la charge d'une perte, ou du bénéfice d'un gain ou d'un risque particulier. C'est le risque accepté dans un certain contexte et fondé sur les valeurs admises par la société.

Partage (transfert) : partage avec une autre partie du fardeau de la perte, ou le bénéfice du gain ou d'un risque particulier (Asnar, 2006).

Éviter : décision de ne pas être impliqué ou de se soustraire à un risque. C'est une décision visant à ne pas être impliquée dans une situation à risques, ou à se retirer d'une situation à risques. (ISO/CEI 17799, 2005)

Afin de mitiger ces risques et de protéger les assets, une politique de traitement des risques est mise en place. Elle sera constituée d'exigences de sécurité permettant de répondre aux risques. Ces exigences de sécurité vont ensuite entraîner la mise en place de contrôles (ou contre-mesures) de sécurité à implémenter, afin de satisfaire aux exigences. Les contrôles sont de deux types :

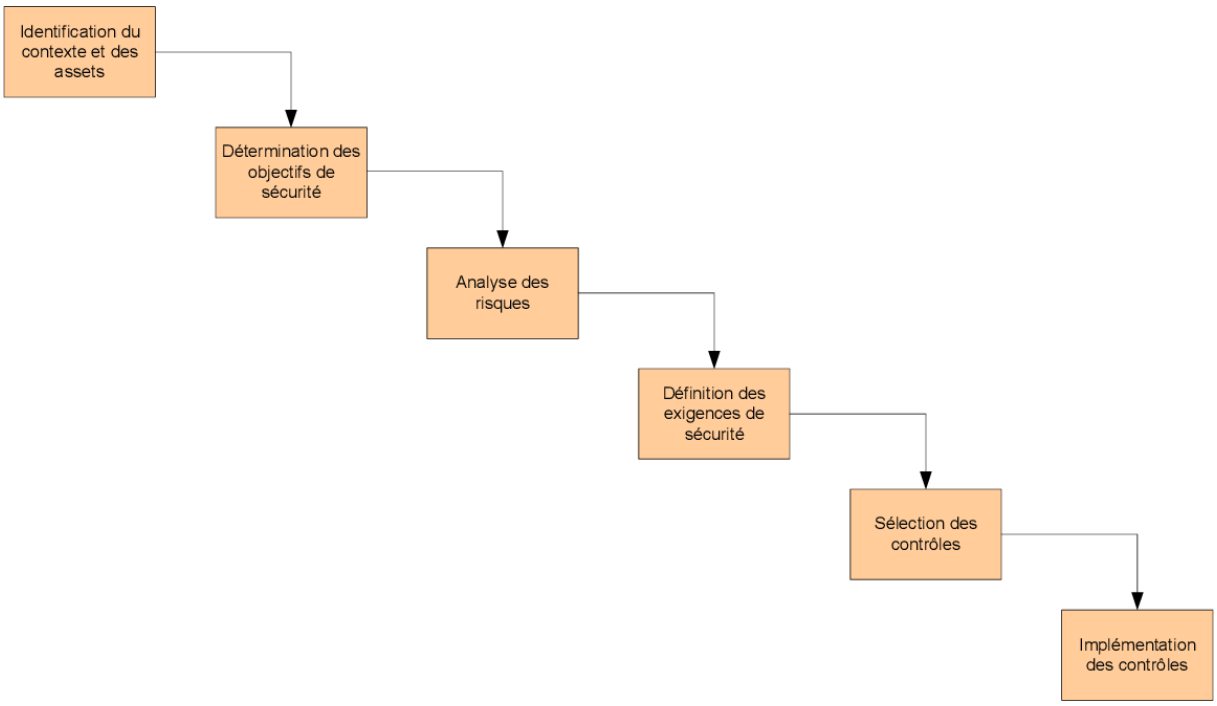
• Sur la menace ou la vulnérabilité, afin de limiter la cause du risque ;

• Sur l'impact, afin de limiter la conséquence du risque.

2.3 Le processus de gestion des risques SI :

Après avoir mis l'accent sur les concepts impliqués dans la gestion des risques, nous pouvons déterminer un processus de haut niveau qui couvre ses activités. Ce processus est presque toujours appliqué aux méthodes réelles de gestion des risques, comme nous le verrons par la suite

Figure 2: le processus de gestion des risques



Source : ISO/ CE 27005. (ISO/ CEI 27005, 2008)

2.3.1 Identification du domaine et des assets :

Dans cette partie, il s'agit de se familiariser avec l'organisation, son environnement et son SI et de déterminer précisément les limites du système sur lesquelles portera la recherche en gestion des risques. Une fois notre système délimité, nous nous efforçons d'abord d'identifier les actifs commerciaux qui constituent la valeur de l'organisation. Ensuite, en reliant ces actifs commerciaux aux actifs systèmes, nous identifierons et corrigerons les risques d'un point de vue technique et organisationnel.

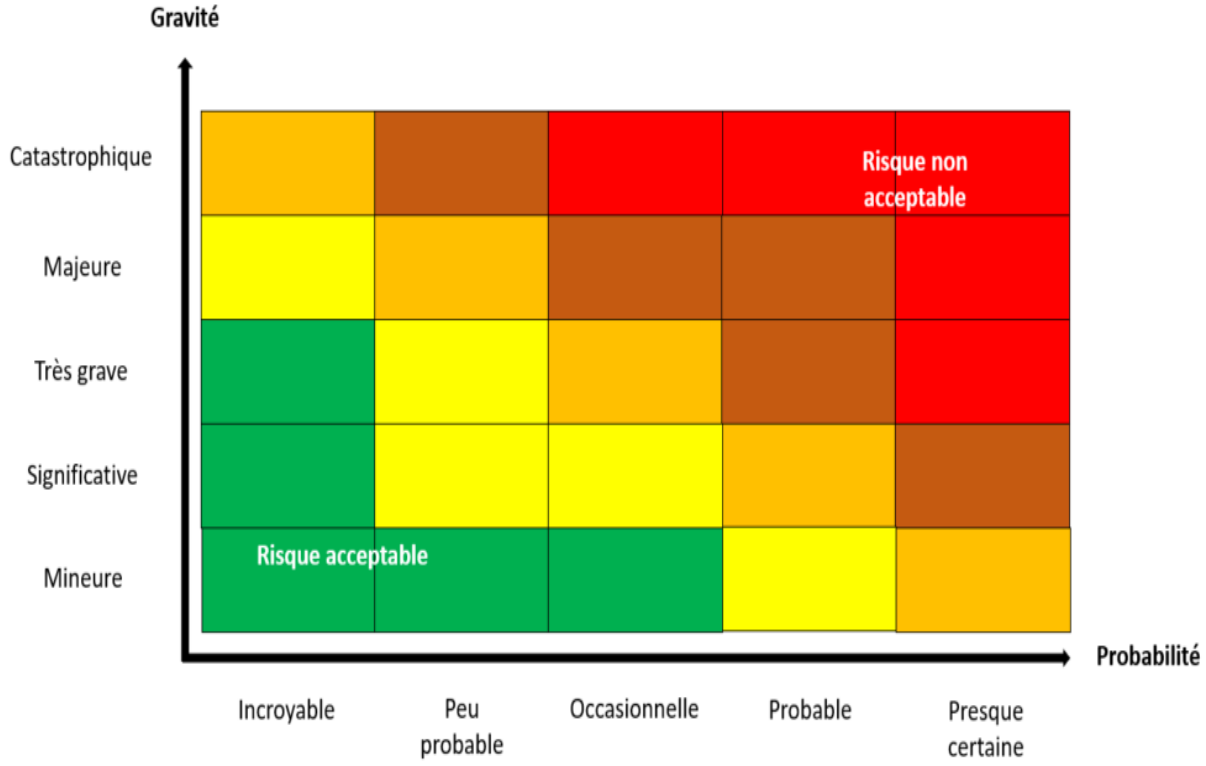
2.3.2 Détermination des objectifs de sécurité : Conçu pour spécifier les exigences de confidentialité, d'intégrité et de disponibilité des actifs, en particulier au niveau de

l'entreprise. Le lien entre les actifs de l'entreprise et les actifs du système est en amont, nous avons donc découvert les exigences de sécurité au niveau du système.

2.3.3 L'analyse des risques :

Constitue le cœur du processus de gestion des risques. Son objectif est d'identifier et d'estimer chaque composante du risque (menace/vulnérabilité/impact) pour évaluer le risque et évaluer son niveau afin de prendre les mesures appropriées (parfois cette étape est appelée « appréciation du risque »). Il existe deux grandes écoles d'identification des risques : soit à travers l'audit du système et de ses différents acteurs, soit à travers une base de connaissances prédéfinie. Pour l'estimation des risques, théoriquement, la distribution de probabilité des menaces et des vulnérabilités peut être utilisée pour les quantifier en estimant le coût de l'impact. En pratique, il s'avère qu'il est difficile de donner des valeurs absolues, et l'on se contente souvent de l'échelle des valeurs relatives

Figure 3:les différentes zones de risque



Source: (DIAMONDE Moussa, 2014)

D'après (Bosworth et Seymour) :

• Le risque de faible incidence et de faible impact est négligeable.

• Il ne doit pas y avoir de risques avec une incidence élevée et un impact significatif, sinon les activités de l'entreprise doivent être remises en question (nous évitons les risques et évitons d'utiliser l'anglais)

• Accepter les risques à forte incidence et à faible impact, et leurs coûts sont généralement inclus dans les coûts d'exploitation de l'organisation (acceptation des risques).

• Les risques de faible taux et d'impact élevé sont transférés. Ils peuvent être souscrits par une assurance ou un tiers (transfert de risque).

• Enfin, d'autres risques, généralement la plupart, sont traités au cas par cas et sont au cœur du processus de gestion des risques. Le but est de réduire le risque en le rapprochant le plus possible de l'origine de l'axe (utiliser des contrôles pour réduire le risque).

3.3.4 La définition des exigences de sécurité :

Réduira les risques identifiés. Comme précédemment, cela dépend de la méthode ou est référencé par les connaissances de l'expert système/sécurité. La définition des exigences de sécurité, en fonction de leur importance et de leur complexité, s'effectue généralement par raffinement incrémental et continu. En effet, il est généralement recommandé de commencer par des exigences générales, qui définiront l'intention de traiter les risques identifiés (au niveau stratégique) puis de les affiner en exigences plus précises (au niveau opérationnel). Cependant, ces exigences sont universelles et s'appliquent à tout système d'information. Il convient également de rappeler que ces exigences d'atténuation des risques sont à la fois liées au système informatique (comme le besoin de cryptage des mots de passe) et à son environnement.

3.3.5la sélection des contrôles (ou contre-mesures) de sécurité :

C'est le dernier niveau de raffinement. Le contrôle est l'instanciation d'exigences de bas niveau sur le système cible à l'étude. Le choix technique de la solution de sécurité est défini ici et est conditionné par le système existant, les compétences disponibles, les coûts de mise en œuvre, etc.

Une mesure de sécurité peut être reconnue comme inefficace, dans ce cas il convient de la

Contrôler pour déterminer si elle doit être retirée, remplacée ou laissée en place par des raisons de coûts par exemple (ISO/CEI 27005:2001).

3.3.6Implémentation des contrôles :

Une fois les mesures de contrôle sélectionnées, elles doivent être mises en œuvre dans le SI et peuvent être testées et évaluées. Il est indéniable qu'il existe une partie du risque, qu'il soit partiellement traité ou non, il constitue le risque dit résiduel.

Ce processus est généralement accepté par diverses méthodes de gestion des risques. Cependant, la terminologie diffère souvent selon une méthode ou une norme. Le processus de comparaison de plusieurs méthodes nécessite une bonne analyse, mais suit généralement le schéma présenté précédemment. Cependant, certaines méthodes diffèrent en ce qu'elles fournissent un cadre légèrement différent ou étendu (tout en prenant généralement comme base le processus général de l'immeuble présenté). Ceux-ci incluent BS 7799-2: 2002, qui traite la gestion des risques comme un processus qui suit le paradigme PDCA ou utilise d'autres méthodes de gestion des risques dans le processus de conception du système.

3. La gestion des risques en pratique : méthodologies normes, standards et Framework :

Le choix d'un standard ou d'une méthode de gestion des risques dans le domaine de la sécurité est généralement un choix structuré et pérenne d'une entreprise en termes de coût, de ressources et d'organisation. L'entreprise doit d'abord analyser en détail ses besoins, l'applicabilité des méthodes existantes à ses besoins et les ressources disponible. (CIGREF ,2002)

Parmi les critères de sélection à retenir, on peut citer : la cible de la méthode, le degré de couverture, qu'il s'agisse des fonctionnalités standards ou non, le caractère transversal du système d'information ou non, le niveau d'adaptation possible à l'organisation, la facilité de mise en œuvre, le coût, la maintenance de la méthode…

Le choix de la méthode est nécessaire mais pas suffisant En effet, la méthode ne doit pas servir d'alibi ni masquer les insuffisances budgétaires, les erreurs techniques, les lacunes organisationnelles ou les défaillances humaines. (CIGREF, 2002)

Il existe de multiples sources et méthodes qui peuvent être utilisées pour protéger les systèmes d'information et gérer les risques des systèmes d'information. Nous distinguons les normes, standards, frameworks et méthodes d'analyse des risques.

Les standards de sécurité : conçues pour fournir un environnement commun pour établir et maintenir des politiques de sécurité qui répondent aux objectifs de sécurité de l'organisation. Ils peuvent être considérés comme des prescriptions de bas niveau décrivant les méthodes utilisées par les utilisateurs pour appliquer leurs politiques de sécurité informatique. Dans la plupart des cas, le gouvernement a établi des standards de sécurité pour s'assurer que ses services administratifs ont un niveau de sécurité adéquat.

Les normes ont le même rôle que les standards, mais elles sont principalement destinées à la certification. Ils ont été créés par des organisations internationales non gouvernementales.

Les méthodes : Ces méthodes définissent le processus d'analyse des risques. Ce processus décrit les phases de mise en œuvre de divers codes et normes de sécurité.

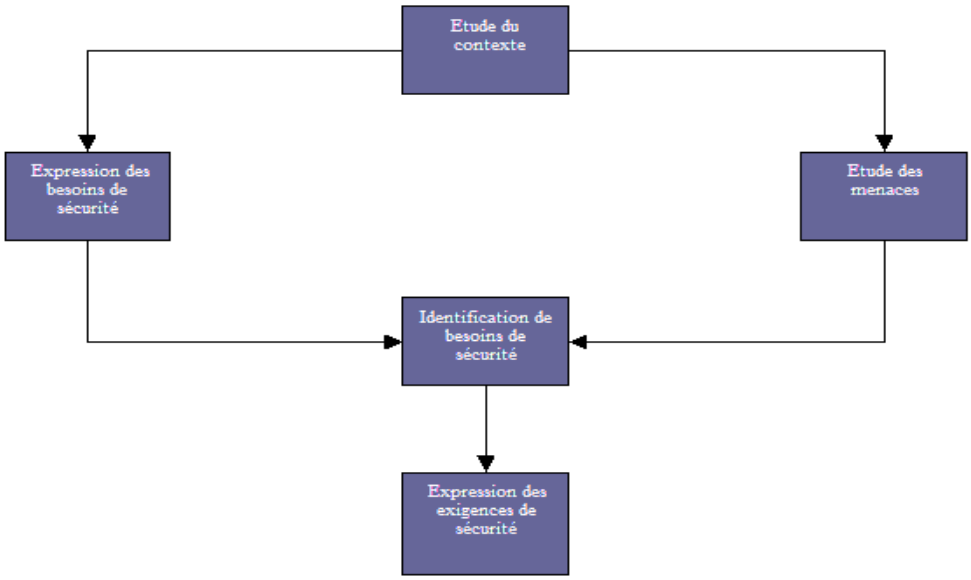
Framework : Est un ensemble de processus documentés utilisés pour définir des politiques et des procédures entourant la mise en œuvre et la gestion continue des contrôles de sécurité de l'information dans un environnement d'entreprise. Fournir un plan détaillé pour construire un plan de sécurité de l'information pour gérer les risques et réduire les vulnérabilités

3.1 Méthodes de gestion des risques :

3.1.1 EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)

Il s'agit d'une méthode développée et maintenue par la DCSSI (Conseil Central de la Sécurité des Systèmes d'Information). La méthode a été créée en 1995 et se compose de cinq guides (introduction, méthodes, techniques, outils d'évaluation des risques et outils de traitement des risques) et de logiciels d'accompagnement. Sa diffusion est gratuite. La méthode a pour objectif formalisation d'objectifs de sécurité adaptés aux besoins du système audité (DIAMONDE Moussa, 2014)

Figure 4: Démarche EBIOS globale



Source : (MAYER, 2006)

EBIOS comprend les risques de sécurité en considérant trois blocs conceptuels de gestion interdépendants proposés par l'amont. Le principe de fonctionnement de cette méthode est de construire les risques, de considérer le contexte de l'organisation cible, de privilégier les frontières du SI, les éléments de base, les fonctions et informations (correspondant aux actifs de l'entreprise), et enfin l'entité (actif). La seconde phase de la méthode permet de dégager les besoins via une grille des services souhaités de sécurité (respect des critères « Confidentialité, Intégrité, Disponibilité»).

Par conséquent, le risque qui correspond à l'organisation est construit et renforcé par la prise en compte relative des vulnérabilités et des menaces applicables aux actifs et considérées comme critiques. L'interdépendance entre ces étapes conduit naturellement à la définition d'exigences de sécurité de haut niveau (appelées ici « cibles ») puis à la définition d'exigences de bas niveau (appelées « exigences »).conformément à ISO 15408 et ISO 17799. Cette dernière phase permet de sélectionner les bonnes contremesures strictement adaptées aux besoins de l'organisation Ainsi, malgré les différences de terminologie, tous les concepts présentés dans la première partie sont présents. Quant au processus de gestion des risques, les 5e et 6e étapes que nous avons vues auparavant n'étaient pas vraiment développées, ce qui ne vérifie pas vraiment l'ensemble du cycle théorique. Dans ce cas, certaines personnes traitent EBIOS spécifiquement comme une méthode d'analyse des risques.

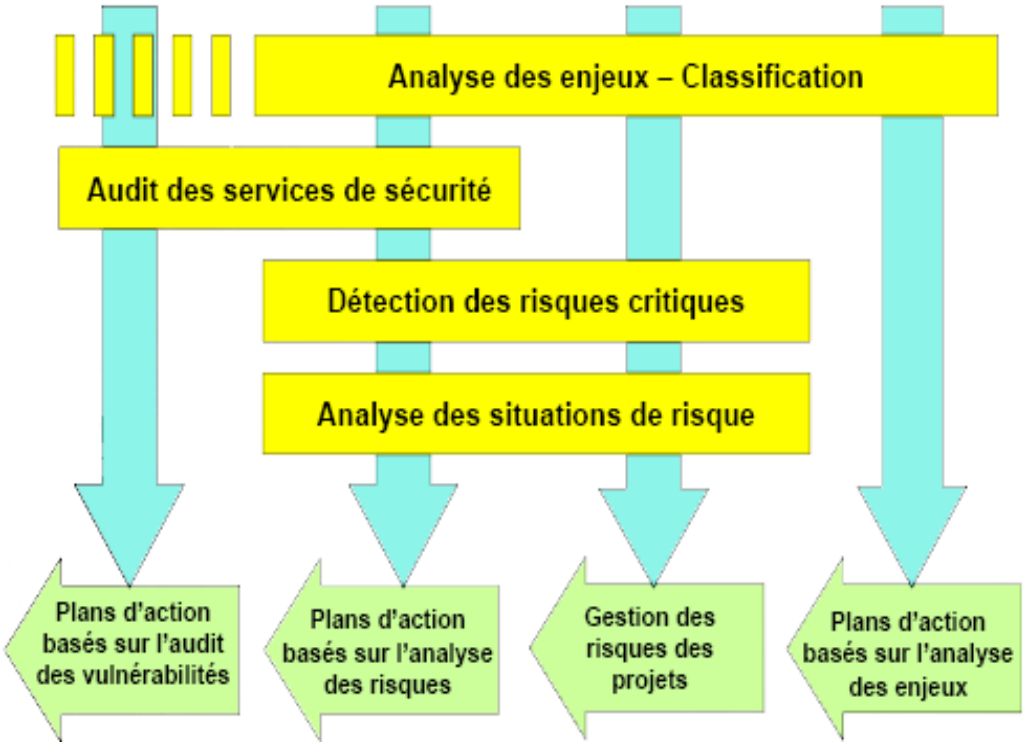
3.1.2 MEHARI (Méthode Harmonisée d'Analyse de Risque) :

MEHARI est encore aujourd'hui l'une des méthodes d'analyse des risques les plus utilisées. Elle est dérivée de deux autres méthodes d'analyse de risque MARION et MELISA MEHARI est maintenue en France par le CLUSIF via notamment le Groupe de Travail dédié à cette méthode (DIAMONDE Moussa, 2014),

MEHARI est une véritable boîte à outils de sécurité du SI qui permet différentes manières d'appréhender les risques au sein de l'organisation et se compose de plusieurs modules. Quelle que soit la méthode de sécurité choisie, ce dernier peut notamment : • Analyser les problèmes de sécurité (en décrivant les types de pannes terribles) et classer les ressources et informations selon trois standards de sécurité de base (Confidentialité, Intégrité, Disponibilité).

• Auditer les services de sécurité pour évaluer l'efficacité et le contrôle de chaque service et détecter les vulnérabilités.

• D'Analyser la situation de risque afin que le potentiel inhérent et les facteurs d'impact et d'atténuation des risques puissent être évalués, puis enfin l'indice de gravité du risque peut être dérivé Figure 5:Démarche MEHARI globale



Source : (CLUSIF, 2010)

MEHARI a fait preuve d'une grande diversité dans l'utilisation de ses modules, dont trois méthodes sont particulièrement importantes : Sur la base d'une analyse détaillée des risques, des plans de sécurité peuvent être mis en œuvre. Cette méthode est applicable aussi bien au niveau stratégique qu'au niveau opérationnel. Le premier niveau permet la cohérence entre les exigences et le contexte de l'ensemble de l'organisation

Le second niveau définit les unités business autonomes au cœur de l'organisation et en charge des décisions nécessaires en matière de sécurité. •. En prenant comme base l'audit de sécurité, ou plus précisément, après le diagnostic de l'état de sécurité, la réalisation du plan d'action peut être favorisée. En fait, la faiblesse identifiée provient directement de l'action à entreprendre. • Lors de la gestion d'un projet spécifique, considérer à nouveau la sécurité en fonction de l'analyse des risques, facilitant ainsi la formulation d'un plan d'action. Les besoins de sécurité sont alors directement intégrés aux spécifications du projet, et à intégrer dans le plan de sécurité global de de l'entité concernée.

3.2 Normes ISO 27005 :

La norme ISO 27005, contrairement à d'autres normes de gestion des risques, permet de construire des résultats qui évoluent avec l'organisation. Tout changement mineur ou majeur peut être intégré au processus de gestion des risques. L'ISO 27005 (ISO 27005, 2011) propose une approche pour la mise en place d'un système de gestion des risques, mais uniquement dans le cadre de sécurité de l'information. Il propose une méthodologie conforme à la norme ISO / CEI 27001 et qui applique le PDCA cycle d'amélioration (planifier, faire, vérifier, agir). Le processus de gestion des risques comprend six phases (Figure 6):

3.2.1.Contexte: définit les champs de gestion des risques, les limites et le processus d'environnement. Au cours de cette phase, des critères de gestion des risques sont établis: les seuils de traitement pour l'évaluation, les seuils de prise en charge rendre compte des risques au regard de leur impact et des seuils d'acceptation.

3.2.2 Évaluation des risques : La première étape de cette phase est de définir le contexte et les éléments qui le composent tels que l'organisation, le système d'information, les éléments essentiels à protéger, les entités qui en dépendent et les différentes contraintes qui peut survenir. Ensuite, il faut exprimer les besoins de sécurité des éléments essentiels, identifier et caractériser en termes d'opportunités les menaces pesant sur le système d'information. Enfin, les risques sont déterminés pour faire face aux menaces pesant sur les

besoins de sécurité. Ces risques sont analysés et évalués afin de fixer les priorités et le calendrier selon leurs critères d'évaluation.

3.2.3 Traitement des risques: Il s'agit du processus de sélection et de mise en œuvre de mesures de sécurité. Cela commence par l'identification des objectifs de sécurité qui constituent les spécifications du processus de traitement de risque. Ensuite, les exigences de sécurité sont déterminées pour répondre aux objectifs de sécurité et pour décrire comment pour faire face aux risques. Pour définir les options de traitement, le risque et le coût du traitement doivent être appariés,

3.2.4 L'acceptation du risque: Il s'agit d'une accréditation de sécurité effectuée par une autorité d'homologation désignée pendant une période de temps spécifiée. Cet agrément nécessite un examen du dossier de sécurité dont le contenu doit être défini.

3.2.5Communication des risques: il s'agit d'un échange et un partage régulier d'informations sur les risques entre le gestionnaire des risques, les décideurs et tous les parties prenantes. Cette communication des risques aide à:

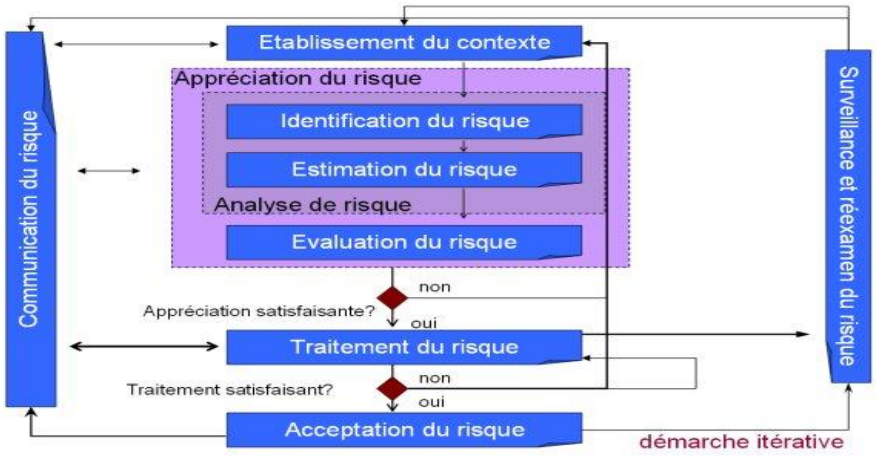
- Réduire les malentendus avec les décideurs

-Acquérir de nouvelles connaissances en matière de sécurité,

-Impliquant la responsabilité des décideurs.

3.2.6 La surveillance et réexamen de risque : pour s'assurer que le processus reste pertinent et adapté aux objectifs de sécurité. Il est également nécessaire d'identifier les changements nécessitant une réévaluation des risques ainsi que les nouvelles menaces et vulnérabilités

Figure 6:processus de gestion des risques



Source: ISO/ CE 27005. (ISO/ CEI 27005, 2008)

3.3 Standard de sécurité PCI-DSS :

PCI-DSS : Payment Card Industry Security Standard (PCI DSS) est un standard de sécurité des données applicable à tous les acteurs de la chaîne de paiement ou la vhaine monétique (Yves B.Desharnais, 2018)

La norme PCI DSS a été développée par les cinq principaux réseaux de cartes (Visa, MasterCard, American Express, Discover Card et JCB) et gérée par le PCI Security Standards Committee (un forum international ouvert pour l'amélioration, la diffusion et la mise en œuvre des normes de sécurité et Protéger les données du compte) Ce standard a été créé afin d'augmenter le contrôle des informations du titulaire de la carte dans le but de réduire l'utilisation frauduleuse des instruments de paiement (Yves B.Desharnais, 2018)

Le standard s'applique à toutes les entités impliquées dans le traitement des cartes de paiement, notamment les commerçants, les entreprise de traitement, les prestataire de service et les émetteurs, il s'applique aussi à toutes les entités qui stockent, traitent ou transmettent les données de titulaires de cartes ou les données d'identification sensibles

3.4 Framework CSP SWIFT :

3.4.1 Qu'est-ce que CSP SWIFT ?

SWIFT (Society for Worldwide Interbank Financial Telecommunication) est une société coopérative de droit belge, créée en 1973 avec l'idée de fournir des standards pour l'échange de données entre les institutions financières. Elle appartient à ses membres, dont les plus grandes banques du monde. SWIFT fournit désormais un réseau de messagerie interbancaire mondial pour les institutions financières (banques, salles de marché, grandes entreprises). (obligatoire ou recommandée).

En 2016, avant la mise en place du CSP, la Banque centrale du Bangladesh, membre du réseau SWIFT, a été victime d'intrusions et de tentatives de détournement de fonds publics. L'objectif initial du pirate était de détourner 1 milliard de dollars américains. Cependant, ils ont éveillé les soupçons de la Deutsche Bank et limité l'impact de la fraude à 81 millions de dollars. Pour SWIFT, la mise en œuvre de mesures de sécurité entre tous les utilisateurs est cruciale, car l'intrusion d'un seul En raison des messages extrêmement sensibles transmis via ce réseau et des menaces croissantes auxquelles l'organisation et ses clients sont confrontés, SWIFT a mis en place un plan de sécurité client en 2017, qui oblige ses

clients à vérifier leur sécurité SI et provoquer une réaction en chaîne sur l'ensemble du réseau

3.4.2 Enjeux du CSP SWIFT :

Ces points de contrôle doivent être auto-évalués annuellement par le client et audités par un prestataire externe tel que Synetis[2]. Si nous prenons une banque comme exemple, il peut y avoir une zone SWIFT sur son réseau qui connectera son back office (qui gère les opérations quotidiennes de la banque) et le reste du monde. Les mesures de sécurité sont basées sur trois objectifs principaux, et ces objectifs eux-mêmes sont soutenus par huit principes de sécurité. La cible représente le cadre général de sécurité dans l'environnement local de l'utilisateur. Des principes connexes précisent l'axe prioritaire de chaque objectif.

Comme tout programme de conformité, le CSP SWIFT a évolué au cours du temps.il devrait intégrer pour fin 2020 une obligation dite d'évaluation indépendante :

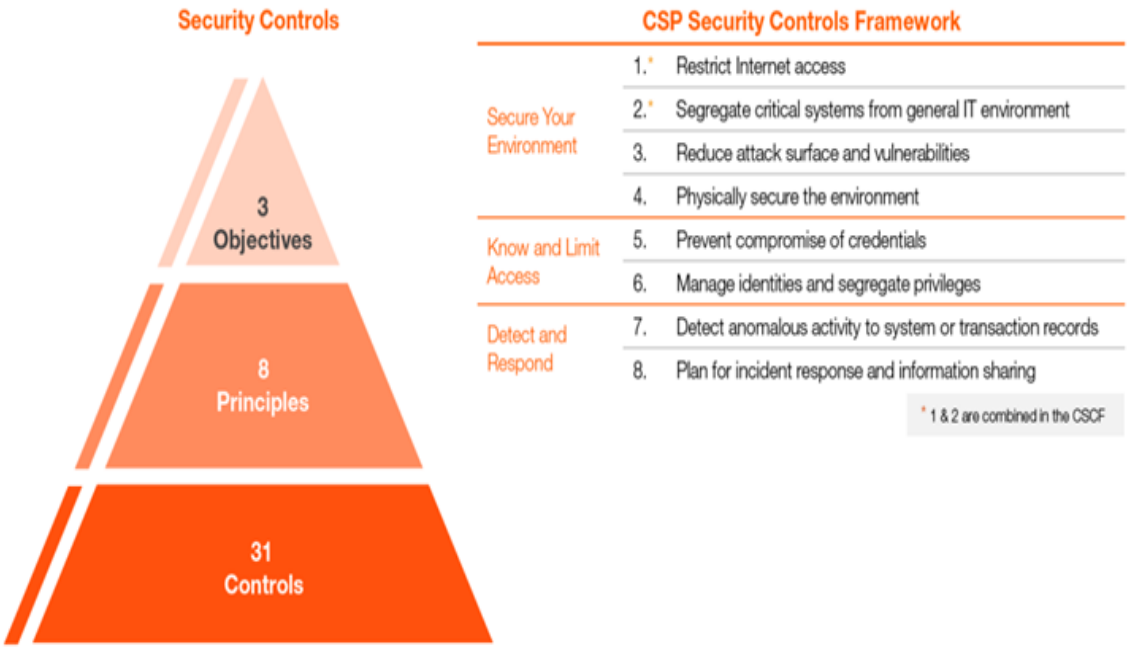
L'Independent Assessment[3] Framework(IAF). L'entrée en vigueur de ce dispositif a été repoussé d'une année pour rentrer en application fin 2021.cette évaluation indépendante, peut-être par réalisée :

•Un organe interne de contrôle, comme l'inspection général ou l'Audit interne, indépendant des opérations SWIFT

•Un auditeur externe disposant des compétences en cybersécurité[4] et gestion des risques d'information

[2] Synetis : cabinet de conseil en transformation numérique et sécurisation des systèmes d'information
[3] Assessment : un ensemble d'outils destinés à évaluer si une personne dispose des compétences requises à l'exercice d'une fonction
[4] Cybersécurité : un néologisme désignant le rôle de l'ensemble des lois, politique, outils, concepts et mécanisme de sécurité, méthodes de gestion des risques et les bonnes pratiques et technologie qui peuvent être utilisés pour protéger les personnes et les actifs informatiques

Figure 7:Les objectifs et les principes de CSP SWIFT



Source : CSP SWIFT(2021)

CSP SWIFT a défini « objectifs principale :

Réduire la surface d'attaque et les vulnérabilités : cela nécessite des partitions réseau solides, de fortes restrictions sur le trafic Internet, des mises à jour et des renforcements du système, et la séparation des méthodes de vérification d'identité des sociétés de réseau.

Gérer les identités et séparer les privilèges : Le réseau SWIFT de l'entité est très sensible, et nécessite une gestion stricte des identités et des autorisations d'accès des opérateurs de la zone (notamment l'utilisation de procédures de contrôle du personnel), et adopte des méthodes d'authentification forte,

Détecter les comportements anormaux sur les systèmes : la traçabilité de toutes les actions (systèmes de même que celles liées au métier) est le point de départ du dispositif de surveillance exigé par le CSP. Et nécessite une application et mécanismes d'intégrité de la base de données. En cas d'incident, la conduite à tenir devra être préalablement écrite.

3.4.3 Les mesures de CSP SWIFT :

Le programme SWIFT définit 7 mesures de sécurité qu'elles doivent être respectées par les membres de réseau SWIFT, ces dernières contiennent un ou plusieurs contrôles de sécurité, les contrôles conseillés sont identifiés par un « A » (ce sont des contrôles facultatifs)

Tableau 1:les mesures de CSP SWIFT

Mesure de sécurité	Contrôle associe à la mesure
1. Limiter l'accès à Internet et séparer les systèmes critiques de l'environnement TI général	**1.1** Protection de l'environnement SWIFT **1.2** Contrôle des comptes à privilèges dans le système d'exploitation **1.3** Protection de la plateforme de virtualisation **1.4** Restriction de l'accès à Internet
2 Réduire la surface d'attaque et les vulnérabilités	**2.1** Sécurité des flux de données internes **2.2** Mises à jour de sécurité **2.3** Sécurisation des systèmes **2.4A** Sécurité du flux de données d'application métier: **2.5A** Protection des données transmises en externe **2.6** Confidentialité et intégrité de la session opérateur **2.7** Analyse des vulnérabilités **2.8A** Externalisation des activités critiques **2.9A** Contrôles opérationnels des transactions **2.10** Sécurisation des applications **2.11**A Mesures opérationnelles RMA
3 Sécuriser physiquement l'environnement	**3.1** Sécurité physique
4 Prévenir les vols d'identifiants	**4.1** Politique en matière de mots de passe **4.2** Authentification à facteurs multiples
5 Gérer les identités et séparer les privilèges	**5.1** Contrôle d'accès logique **5.2** Gestion des jetons **5.3A** Processus Ressources humaines de validation du personnel **5.4** Stockage physique et logique des mots de passe
6 Détecter les activités anormales dans les systèmes ou les relevés d'opérations	**6.1** Protection contre les logiciels malveillants **6.2** Intégrité des logiciels **6.3** Intégrité des bases de données **6.4** Journalisation et surveillance **6.5A** Détection des intrusions
7 Plan d'intervention en cas d'incident et partage d'informations	**7.1** Planification de l'intervention en cas de cyber-incident **7.2** Formation et sensibilisation à la sécurité **7.3A** Tests d'intrusion **7.4A** Évaluation des risques fondée sur des scénarios

Source : CSP SWIFT 2021

'Dans notre cas on va travailler sur la mesure numéro4 « prévenir les vols d'identifiants »'

3.4.4 Intégration avec la gestion de la sécurité et des risques :

SWIFT encourage les utilisateurs à appréhender la gestion des cyber-risques de la manière la plus large possible, et notamment au-delà du cadre de leur infrastructure SWIFT et des mesures de sécurité SWIFT. Pour une gestion optimale des risques, les utilisateurs ne

doivent pas voir la mise en œuvre de ces mesures de sécurité comme une activité ponctuelle ou unique, ni exhaustive ou « tout-en-un ». Au contraire, les utilisateurs doivent intégrer les mesures SWIFT dans un programme continu de gestion des risques de la cyber-sécurité et des risques au sein de leur organisation, basé sur un jugement éclairé et les dernières bonnes pratiques, en tenant compte de l'infrastructure et de la configuration spécifiques de chaque utilisateur. Ainsi, les utilisateurs peuvent réutiliser et tirer profit des politiques, procédures et mécanismes de réduction de risques existants qui ont été mis en place pour gérer d'autres domaines des cyber-risques.

Une approche holistique des cyber-risques sera plus efficace pour prévenir les risques pour l'entreprise, en améliorant ainsi la sécurité globale de chaque organisation individuelle et de la communauté financière dans son ensemble.

En outre, les utilisateurs doivent avoir le niveau de responsabilité et de supervision adéquat pour leurs activités de gestion des cyber-risques. En général, un Responsable de la sécurité des systèmes d'information joue un rôle de premier plan dans ce domaine en définissant les priorités du programme de sécurité et en sollicitant le soutien et les conseils de la direction.

3.4.5 Mise en correspondance des normes de l'industrie :

Le tableau ci-dessous met en correspondance la mesure de sécurité SWIFT (prévenir les vols d'identifiants) qu'on a étudié et les trois cadres de normes de sécurité internationales:

• Le National Institute of Standards and Technology (NIST) est une agence fédérale américaine non réglementaire rattachée au département du Commerce des États-Unis qui a mis au point un «Cadre de cyber-sécurité» pour aider les entreprises à gérer les cyber-risques.

• ISO 27002 ISO/IEC 27002 est une norme de sécurité de l'information publiée par l'organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (IEC).

• La norme de sécurité de l'industrie des cartes de paiement (Payment Card Industry Data Security Standard, PCI DSS) est une norme de sécurité des informations protégées pour les entreprises qui fournissent des cartes de paiement. Le tableau de correspondance ci-dessous montre également le lien entre la mesure de sécurité SWIFT étudié et la mesure similaire prévue par ces normes de l'industrie. Si des utilisateurs sont certifiés par rapport à ces normes, et à condition que leur infrastructure SWIFT soit comprise dans le champ de

cette certification, le tableau montre le rapport entre les mesures prévues par ces normes et les mesures de sécurité SWIFT

Tableau 2:Mise en correspondance des normes de l'industrie

La mesure num4 de Swift (prévenir les vols d'identifiant)	Cadre de gestion de la cyber-sécurité du NIST v1.1	ISO 27002 (2013)	PCI DSS 3.2.1
.1Politique en matière de mots de passe S'assurer que les mots de passe sont suffisamment robustes pour résister aux attaques courantes, en mettant en place et en appliquant une politique efficace en matière de mots de passe.	**Contrôle d'accès (PR.AC)** **PR.AC-1**:Les identités et les identifiants sont gérés pour les périphériques et utilisateurs autorisés	**Contrôle de l'accès au système et à l'application (9.4)** **9.4.3**: Système de gestion des mots de passe	**Condition 2**: Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur **Article(s) applicable(s):2.1** **Condition8**:Identifier et authentifier l'accès aux composants du système **Article(s) applicable(s):8.2**
4.2 Authentification à facteurs multiples Empêcher que la violation d'un facteur d'authentification unique ne permette d'accéder aux systèmes SWIFT, en mettant en place une authentification à facteurs multiples.	Contrôle d'accès (PR.AC) **PR.AC-1:** Les identités et les identifiants sont gérés pour les périphériques et utilisateurs autorisés **PR.AC-6**:Les identités sont confirmées, liées à des identifiants et affirmées dans les interactions **PR.AC-7**: Les utilisateurs, appareils et autres actifs sont authentifiés (par exemple, facteur unique multifacteur) en fonction du risque de la transaction (par exemple, risques	**Contrôle de l'accès au système et à l'application (9.4)** **9.4.2**: Sécuriser les procédures de connexion	**Condition8:** Identifier et authentifier l'accès aux composants du système **Article(s) applicable(s):8.2, 8.3**

	pour la sécurité et la vie privée des individus, et autres risques organisationnels)		

Source : CSP SWIFT 2021

CHAPITRE II :

CADRE MÉTHODOLOGIQUE ET

ORGANISAME D'ACCUEIL

1. A propos d'Al Salam Bank-Algeria :

Banque universelle de droit algérien, Al Salam Bank-Algeria active dans le respect des principes moraux du peuple algérien. Elle propose des produits shari'a compatibles certifiés conformes par le conseil shari'a de la banque.

ASBA est agréée par la banque d'Algérie en septembre 2008. Elle débute son activité avec pour objectif principal d'offrir à sa clientèle des produits et services bancaires innovants.

Al Salam Bank-Algeria œuvre conformément à une stratégie claire visant à soutenir la croissance économique de l'ensemble des secteurs d'activités du pays, elle offre des services bancaires novateurs, aux fins de répondre aux attentes du marché, de la clientèle et des actionnaires. Banque alternative, Al Salam Bank-Algeria se caractérise par son engagement au respect des principes de la sharia dans toutes ses transactions.

Tableau 3:référentiel stratégique d'AL SALAM BANK- ALGERIA

Mission	Vision	Valeur
S'engager à faire face aux défis bancaires à venir des marchés locaux, régionaux et mondiaux, tout en s'appuyant sur les plus hauts standards de qualité et de performance pour répondre au mieux aux attentes de sa clientèle et de ses investisseurs.	Etre les leaders de la finance bancaire universelle basée sur les préceptes de la sharia en proposant des produits et services bancaires innovants, certifiés conformes par le conseil sharia de la banque.	**L'Excellence:** C'est le facteur qui nous permet d'atteindre nos objectifs. Chez Al Salam Bank-Algeria nous faisons de l'excellence une culture générale et individuelle, nous la transmettons à nos clients à travers des services de haute qualité et à la pointe de la technologie. **L'Engagement:** Chez Al Salam Bank-Algeria faire preuve d'engagement, c'est avoir le sens de la responsabilité et se dévouer totalement aux attentes de ses clients et collaborateurs. **La Communication:** Nous faisons de la communication interne/externe une priorité, car nous restons conscients qu'elle est notre meilleure alliée pour mieux servir notre clientèle.

Source : à partir des documents interne de l'entreprise

2. Les produits et les services offerts par AL SALAM BANK ALGERIA :

Pour répondre au mieux aux besoins et attentes de sa clientèle, Al Salam Bank-Algeria propose des produits et services bancaires innovants tout en veillant au respect de ses valeurs. Nous citons :

2.1 Les opérations de Financement :

Al Salam Bank - Algeria finance aussi bien vos projets d'investissements, que vos besoins en exploitation et consommation et vous propose des contrats de :

- Moucharaka ;
- Moudharaba ;
- Ijara ;
- Mourabaha ;
- Istisnaâ ;
- Salem ;
- Bai Bi Taksit ;
- Bai Al Ajal ; etc...

2.2 Les opérations de Commerce Extérieur :

Al Salam Bank-Algeria s'engage à exécuter vos opérations de commerce extérieur avec célérité, en vous proposant des solutions efficientes, conçues et adaptées à vos besoins telles que :

- Les moyens de paiement à l'international : Les crédits et remises documentaires ;
- Les garanties bancaires.

2.3 Les placements et Investissements :

Désireux de rentabiliser les excédents de trésorerie de votre entreprise ?

Al Salam Bank-Algeria vous propose des solutions de placement attractives et sûres.

Faites fructifier vos capitaux ou bien vos excédents de trésorerie aux meilleures conditions du marché, en :

- Souscrivant des bons d'investissement ;
- Ouvrant un livret d'épargne « Oumniyati » ;
- Ouvrant un compte d'investissement.

2.4 Les services :

Al Salam Bank-Algeria met à votre disposition des services bancaires innovants, rapides et modernes tels que :

- Les services de transfert d'argent par le biais d'instruments de paiement automatisés ;
- La banque à distance « Al Salam Moubachir » ;
- Le service mail swift « Swifti » ;
- La carte de paiement électronique « Amina » ;
- Le paiement en ligne « E-Amina » ;
- La carte de paiement internationale « Al Salam Visa » ;
- Le Mobile Banking ;• Les coffres forts « Aman » ;
- Les terminaux de paiement électronique « TPE » ;• Les guichets Automatiques de Banque « GAB » ; etc.

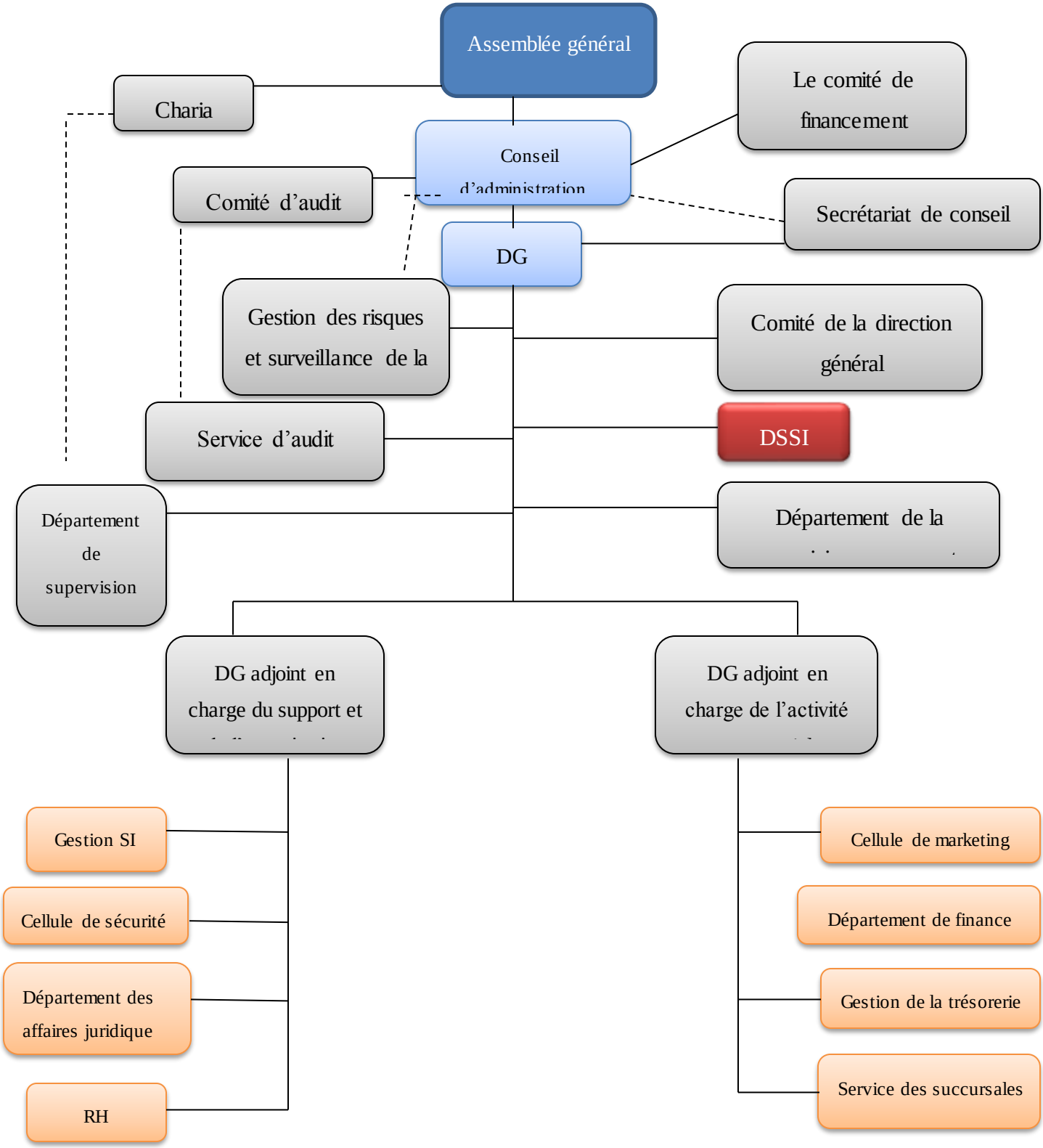
Tableau 4:fiche signalétique de la banque Fiche signalétique

Fiche signalétique	
Nom de l'entreprise	AL SALAM BANK ALGERIA
Logo	
Siège social	233 Rue Ahmad Ouaked Dely Ibrahim
Objet social	Activités bancaires
Date de création	2006
Statut juridique	SPA
Site web	https://www.alsalamalgeria.com
Téléphone	+213 21372717

Source : élaborer par nous même à partir des documents interne de l'entreprise

L'organigramme qui suit permet de donner une vue d'ensemble sur la structure générale de l'entreprise

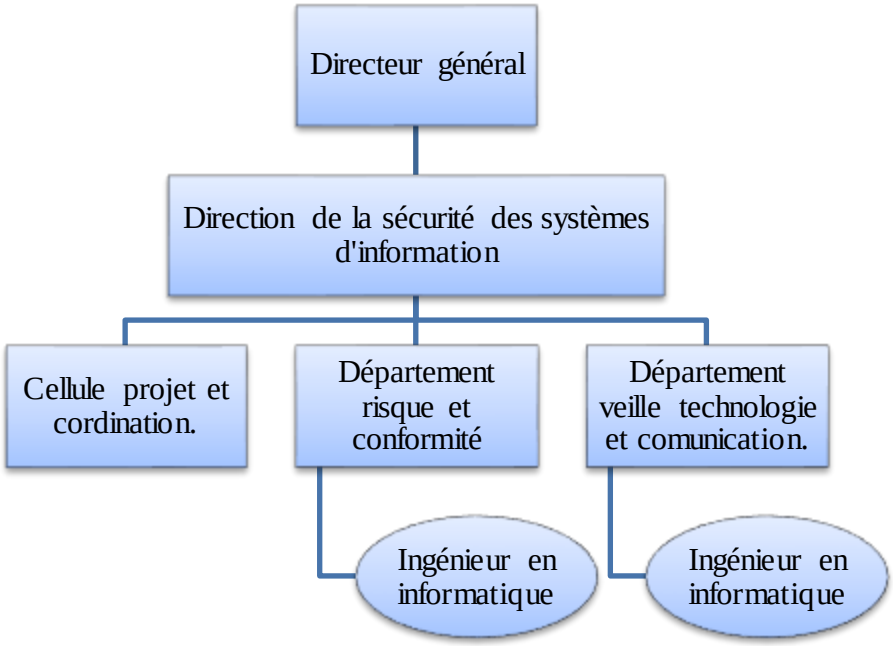
Figure8 : organigramme D'AL SALAM BANQUE



Source : élaboré par nous même à partir des documentations interne de l'entreprise

Nous avons effectué notre stage au sein de la direction de sécurité des systèmes d'information, présentée dans l'organigramme ci-dessous, plus précisément au niveau du département risque et conformité.

Figure 9:Organigramme de la direction de sécurité des systèmes d'information



Source : élaboré par nous même à partir des documentations interne de l'entrepris

La Direction de la Sécurité des Systèmes d'information est chargée de couvrir l'ensemble des besoins et exigences de la Banque en matière de sécurité et conformité du système d'information par rapport à la réglementation de la Banque d'Algérie d'une part et aux Normes et Standards Internationaux (IFRS, CSCF SWIFT, IS027001, 27005, 27015, PCI-DSS, Accord BALE III, SOX, COBIT & COSO), d'autre part.

3. DEPARTEMENT RISQUES ET CONFORMITE :

3.1 Attributions du Chef de Département Risques et Conformité :

Le Chef de Département a pour attributions de :

-Assurer la conformité des systèmes d'information de la Banque avec les obligations légales en vigueur ;

-Diriger et coordonner les activités du Département en vue de réaliser les objectifs arrêtés par la Direction ;

-Veiller à la mise en œuvre de la Politique de Sécurité du Système d'information définie par la Banque

-Assurer la réalisation des missions relevant la compétence de son Département ;

-Etablir des référentiels d'audit (recueils de règles, procédures, politiques..... etc) qui permettent de renforcer la fiabilité et la pertinence des recommandations effectuées par la Direction dans te cadre de l'audit des systèmes d'information ;

-Rendre compte, régulièrement, des activités du Département au Directeur de la structure ;

-Etablir, périodiquement, le rapport d'activité du Département et le transmettre à la hiérarchie.

3.2 Missions du Département Risques et Conformité :

Le Département Risques et Conformité a pour missions de :

-Procéder à l'identification, l'implémentation et la revue des contrôles de risques de sécurité ;

-Contribuer à l'élaboration et la mise en place de la charte de sécurité en matière de risques et conformité ;

-Réaliser les missions d'audit interne des systèmes d'information de la Banque ;

- Apprécier les domaines des applications informatiques en production (Jira, Taysir, application des Avis, Portail Predont.....etc), en particulier les données opérationnelles, les données de base, les paramètres, les interfaces entre l'application et le système, la gestion des droits d'accès à l'application ;

-Evaluer l'efficacité et la performance des systèmes d'information au regard des objectifs stratégiques de la Banque ;

-Evaluer les risques des systèmes d'information nécessaires au fonctionnement des applications (Sécurité physique, sécurité des réseaux, plan de secours, ...etc) ;

- Assurer et apprécier, dans le cadre d'un audit d'une application, ta sécurité de l'infrastructure informatique nécessaire au bon fonctionnement des applications du système d'information de la Banque ;

-Participer, en étroite collaboration avec la Cellule Gestion des Risques, à la consolidation des risques métiers (opérationnels) et risques informationnels ;

-Participer, en collaboration avec la Direction des Systèmes d'information, la Cellule de

-Développement des Projets des Systèmes d'information, la Cellule Gestion des Risques et la Direction de l'Audit Interne, aux travaux d'identification et de classification des activités critiques de la Banque dans le cadre de la mise en place d'un plan de continuité d'activité ;

-Assurer la surveillance des accès quant aux habilitations des utilisateurs de la Banque en conformité avec la Politique de sécurité adoptée par la Banque ;

-Veiller à la bonne utilisation des droits d'accès autorisés aux utilisateurs de la Banque ;

-S'assurer de la mise en place des protections nécessaires du système d'information et vérifier leur efficacité (tests de reprise, tests d'attaque malveillante, ...etc).

4. Le positionnement épistémologique :

Le concept de l'épistémologie est apparu dans les débuts du 20 -ème siècle, elle représente une branche de philosophie des sciences et elle se focalise sur l'étude des théories et des fondements de la connaissance, Selon Piaget (1967), « l'épistémologie est l'étude de la construction valables ».

Le questionnement épistémologique permet aux chercheurs d'élaborer un paradigme épistémologique et d'acquérir les connaissances nécessaires pour soutenir et justifier leurs travaux de recherche qui seront élaborées ; Il ne se restreint pas à une réflexion méthodologique. (Marie-Laure Gavard-Perret, 2012)

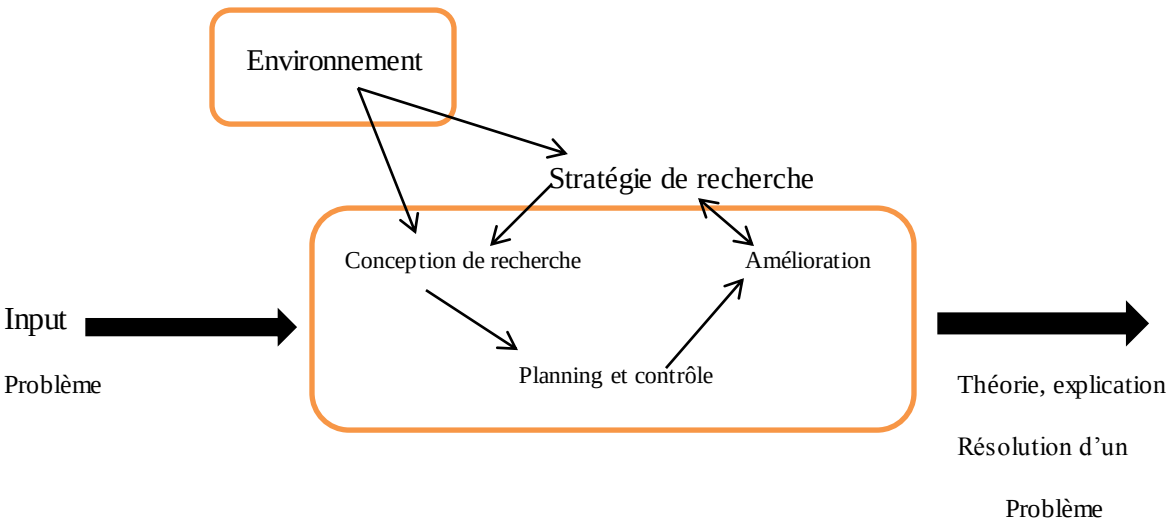
L'enjeu d'un positionnement épistémologique selon (Kuhn, 1962) est définit par « *[…] une constellation de croyance, valeurs, techniques, etc. partagées par une communauté donnée*» (cité par Avenler & Gavard-Perret, 2012). En outre cette définition désigne les conséquences de ce positionnement sur la démarche de recherche à adapter, les méthodes à mobiliser et la nature de la connaissance à produire

De ce fait on conclut que notre travail de recherche s'inscrire dans un cadre épistémologique. En effet ce cadre aura une liaison sur les orientations méthodologiques.

Selon (AVENIER, 2008) (Girod- seveille et peret, 2003) dans la science de gestion seuls les paradigmes positiviste, constructiviste et interprétativiste sont adapté pour ce domaine. Selon F. Wacheux (1996, p.265) le positivisme courant classique de la recherche, il s'intéresse à la vérification d'une réalité préétablie en recherchant des liens de causalités entre des faits. Tandis que la phénoménologie (contient l'interprétativisme et le constructivisme) oriente le chercheur vers la construction sociale d'une réalité inexistante. L'objectif est donc, de construire une réalité ou une connaissance qui se comprend comme étant la présentation de l'expérience cognitive des individus. Le paradigme constructiviste a une attitude ouverte de recherche, plutôt qu'avec un paradigme définitif (positiviste). Autrement dit, il existe plusieurs attitudes constructivistes la seule chose commune comme le précise F.Wacheux (1996, p.43), D'où notre choix se focalisera entre ces deux approches.

Partant de constat, on inscrit notre recherche dans une position épistémologique constructiviste car nous allons développer notre intelligence en construisant des connaissances en action et en situation et par la réflexion, ces connaissances mène vers des nouvelles résultats, En outre notre projet de recherche commence par l'identification des acteurs principaux et leurs rôles dans le processus de contrôle puis définir les risques associer au contrôle afin de définir le processus optimiser et d'obtenir des résultats qui impliques des axes d'amélioration

Figure 10:modèle de la recherche (Coughlan & Brady)



Source : Hazem Ben Aissa, (2001), (Quelle méthodologie de recherche appropriée pour une construction de la recherche gestion, www.strategie-aims.com)

5. L'approche de recherche :

Comme nous avons vu dans la partie cadre conceptuel, la gestion des risque SI et la sécurité de système d'information recouvre un ensemble diversifie des approches et des sources , notre projet de recherche et basé sur le Framework CSP SWIFT qui définit un ensemble de contrôle nécessaire pour assurer la sécurité SI, nous on s'intéresse au contrôle numéro 4 du programme SWIFT(prévenir le vols d'identifiants), commençant d'abord par l'identification des différents acteurs et leurs rôles dans le processus de contrôle on utilisant la matrice RACI, notant également que nous allons proposer un processus optimiser pour le contrôle 4, Dans ce contexte nous avons opté pour la recherche-action l'une des approches liées au paradigme épistémologique constructiviste.

Selon (Hugon et seibel, 1989) la recherche-action est l'existence d'une action de transformation d'un fait réel, ayant un double objectif qui sont la transformation d'un fait réel et produire des connaissances

Dans le même contexte Lewin (1951) a définit la recherche-action comme une action qui commence par une vision de changement de la recherche en ayant une corrélation entre la théorie et la pratique, lors de cette recherche, le chercheur s'inscrit comme un acteur actif dans le management et la résolution des problèmes posés, il utilise son expertise, expérience et son cadre de référence pour arriver à faire une démonstration valable et justifier de la recherche.

6. Méthode de recherche :

Dans le processus de recherche, plusieurs concepts et paradigmes peuvent être impliqués ensemble et peuvent être complémentaires, Selon (Benaissa, 2001) dans le choix de la conception de la recherche, nous restons dans des débats épistémologiques de conflits entre paradigmes. Cependant, Il existe des questions où il est préférable d'utiliser une approche quantitative et pour d'autres une approche qualitative.

Dans le cadre de l'élaboration de notre travail de recherche, nous avons opté pour une méthodologie qualitative, (Taylor et Bodgen, 1984) définit l'approche qualitative comme «*la recherche qui produits et analyser des données descriptives telle que les paroles écrite et dite et les comportements observatoire des personnes »*

Selon Piaget (1967) l'utilisation d'une méthode de recherche est souvent la conséquence d'un choix méthodologique et épistémologique. , et c'est à cet égard que nous avons choisi la méthode de recherche qualitative

L'argument principale de notre choix et comme nous l'avons déjà précisé c'est l'étude et l'évaluation de la conformité des contrôles de sécurité de la banque vis-à-vis le CSP SWIFT et extraire les métriques associer aux contrôles par des entretiens et faire aussi une cartographie pour les scenarios des risques qui peuvent impacter le niveau de sécurité d'ASBA, et à la fin modéliser les contrôles de sécurité, pour cela on doit forcément s'appuie sur des méthodes et moyens qualitatif pour collecter les données et présenter un modèle de conformité et la modélisation des contrôles comme des résultats, cette démarche a été confirmer par les travaux de (Crozier et friedberg ,1977) qui ont justifier le choix de la démarche qualitative dans les recherche de gestion par l'importance de la connaissance du contexte afin de pouvoir faire une évaluation , pour eux le chercheur tentera dans ces entretiens de trouver la logique interne du système ainsi que la stratégie global

7. Collecte de données :

Pour l'élaboration de notre projet de recherche nous avons exploité des techniques et des outils de collecte de données qui sont principalement dans notre cas de nature qualitative.

Selon (MILES et HUBERMAN, 1991), une donnée qualitative se présente sous forme de mots plutôt que de chiffres. Il ajoute (F.Wacheux 1996, p.192) que la collecte s'organise en fonction des possibilités du terrain et des exigences de la problématique. C'est au chercheur à organiser le recueil de sa matière première.

Les méthodes de collectes de données sont très variées et nombreuse (Macnee, Maccabe, 2008) de son coté à proposer plusieurs moyens de collecte de données telle que l'entrevue individuelle ou en groupe, en face à face ou à distance, le journal, l'observation participante ou non participante, les méthodes artistiques, et la combinaison de différentes méthodes de collecte de données

Dans notre cas d'étude nous avons opté pour l'entretien et l'analyse documentaire et l'observation, Ces derniers, nous ont apparus les plus adéquats et les plus adaptés aux exigences de notre problématique. Comme l'affirme (F.Wacheux, 1996, p.192) l'entretien et la documentation sont des deux sources incontournables et indispensables lorsque l'on s'intéresse aux acteurs, à l'organisation et aux comportements des acteurs dans l'organisation. Pour (Crozier et Friedberg, 1977, p.458) les entretiens sont l'occasion pour

le chercheur de réunir aussi rapidement que possible le maximum d'informations concrètes sur le vécu quotidien des acteurs, sur ce qui est implicite dans le champ considéré.

7.1 Recherche documentaire :

Selon (N'DA Paule, 2015) la recherche documentaire permet de collecter une littérature importante sur des questions pour obtenir les informations les plus pertinentes dans un domaine d'objet à traiter. Il s'agit notamment d'enchainement de recherche, d'identification et d'acquisition des documents liés à des sujets clairement définis, ainsi construire des stratégies de recherche qui nécessitent des méthodes efficaces

Selon (Dinet et Passerault, 2004) *« la recherche documentaire vise à identifier et localiser des ressources informationnelles déjà traitées, soit par individus soit par des machines. La recherche documentaire s'accompagne du qualitatif « informatisée » lorsque cette activité implique l'interaction entre deux systèmes, l'un humain (i.e., l'usager, l'utilisateur) et l'autre informatique (i.e., une base de données) via un logiciel et une interface.* »

Pour l'élaboration de notre recherche, nous avons consulté des ressources documentaires qui passent en revue le concept de la gestion de la sécurité des risques des systèmes d'information et l'ensemble des pratiques (Normes, Méthodes, Framework) utiliser dans le domaine de la sécurité des systèmes d'information et décortiquer l'outil utiliser qui est le CSP SWIFT, Pour ce faire nous avons exploité des sources de données documentaires informatisés et non informatisés, accessibles et gratuites, y compris : les ressources de la bibliothèque de l'ENSM, des ouvrages, des articles, des thèses et les différents moteurs de recherches mais également des documents internes à l'entreprise en rapport avec la gestion et la sécurité des système d'information et l'audit de sécurité aussi. Cette étape nous a été essentielle pour l'enrichissement de nos bases théoriques, permettant ainsi une bonne constitution de notre recherche qui correspond à notre cas pratique, ainsi qu'à la rédaction du cadre théorique.

7.2 L'observation :

L'observation est une technique déployer par nous-même lors de notre stage au sein de L'ASBA, elle était très utile pour faire un constat réel sur la culture de l'entreprise en particulier la culture et la politique de sécurité, la sensibilisation et la culture de contrôle ainsi que l'utilisation des référentiels de bonne pratique dans la gestion des risques et la sécurité des SI

7.3 L'entretien semi directif :

L'entretien est un mode privilégié de collecte d'informations dont le but est d'aider les chercheurs à obtenir des faits et des explications aux participants dans des situations variées comme le souligne (F. Wacheux,1996) *« en science de gestion, particulièrement, la plupart des recherches qualitatif s'alimente « au mots des acteurs » pour comprendre les pratiques organisationnelle et les représentation des expérience »*

Nous avons opté pour la technique d'entretien semi directif parmi les quatre autres modèles d'entretien car, cette technique est dotée d'un guide d'entretien facile à appliquer et elle nous permet de collecter un grand nombre de données en une seuls rencontre en couvrant toutes les questions souhaiter, ainsi qu'elle offre la possibilité d'aborder plusieurs sous-titres en un seul thème. Comme le précis (F. waheux ,1996) *« l'acteur s'exprime librement mais sur des questionnement bien précis, sous le contrôle de chercheur, l'implication est partagée ».*

Tableau 5:les entretiens avec les différents responsables

Responsable intervenant à l'interview	Sujet de l'entretien	Date
Directeur de sécurité des systèmes d'information	-Présentation de la direction de sécurité des systèmes d'information de l'ASBA -politique de sécurité de la banque	26/06/2021
Responsable de département risque et conformité	-les contrôles de sécurité de CSP SWIFT -Les acteurs et leurs roles -le niveu de respect des bonnes pratiques de csp swift	27/06/2021

Source : élaboré par nous-mêmes à partir des documents interne de l'entreprise

Tableau 6:guide d'entretien semi directif

Guide d'entretien semi-directif
La collecte d'information sur les contrôles de sécurité étudiés pour faire l'évaluation de conformité(les questions étaient posées aux responsables cités dans le tableau précèdent) Q1 : Quels sont les acteurs qui participent dans les contrôles et ainsi leurs responsabilités ?

Q2 : Qui définit la politique de mots de passe ainsi la politique d'AML de l'entreprise ?
Q3 : Avez-vous une cartographie des risques ? si oui ? est-elle mise à jour ?
Q4 : Comment peut-on extraire les métrique associées aux contrôles (les bonnes pratiques du programme SWIFT) pour évaluer le niveau de conformité de la sécurité SI ?
Q5 : Disposez-vous d'un bilan sur l'état de sécurité de SI actuel ? comment vous l'évaluer ?
Q6 : Comment procéder le département risque et conformité pour identifier les besoins de sécurité SI ?
Q7 : Comment vous évaluez les risques des systèmes d'information nécessaires au fonctionnement des applications (Sécurité physique, sécurité des réseaux, plan de secours, ...etc)
Q8 : -Assurez-vous la surveillance des accès quant aux habilitations des utilisateurs de la Banque en conformité avec la Politique de sécurité adoptée par la Banque ?
Q9 :
Q10 : Développez-vous un plant pour faire faces aux risques ? quelles sont les grandes lignes de ce plan
Q11 : Est-ce-que vous avez déjà Fait un audit interne des systèmes d'information de la banque ?
Q12 : Comment vous évaluer le degré de vigilance de vos collaborateurs en matière de la sécurité informatique ?

Source : élaboré par nous-mêmes à partir des documents interne de l'entreprise

CHAPITRE Ⅲ : ÉVALUATION DE LA CONFORMITÉ ET MODÉLISATION DES CONTOLES DE SECURITÉ

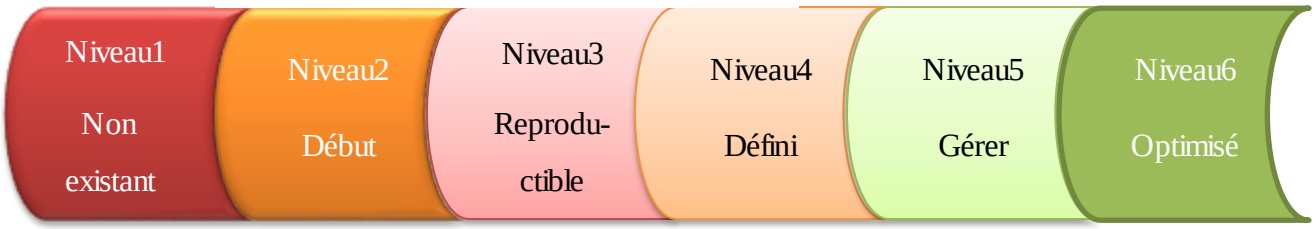
Section 1 : Évaluation de la conformité de la mesure numéro 4 du programme Swift (prévenir les vols d'identifiants) :

La mesure 4 du programme Swift se décompose en deux contrôles obligatoires à respecter, le premier consiste à la politique de mots de passe(CO 4.1) qui vise à assurer que les mots de passe sont suffisamment robustes pour résister aux attaques courantes, en mettant en place et en appliquant une politique efficace en matière de mots de passe. Le deuxième contrôle consiste à l'utilisation de l'authentification à facteurs multiples (CO 4.2) qui sert à empêcher que la violation d'un facteur d'authentification unique permette d'accéder aux systèmes ou applications SWIFT, en mettant en place une authentification à facteurs multiples. Nous allons essayer de déterminer pour chaque contrôle les acteurs qui participent dans le processus et les responsabilités de chaque un, puis extraire les métriques associées au contrôle, afin d'évaluer la conformité de la banque vis à vise la mesure 4 du programme SWIFT et de proposer un processus optimiser pour chaque contrôle

1.1 Présentation des résultats de l'évaluation des contrôles :

Nous avons évalué la conformité de la sécurité SI d'ASBA vis-à-vis le programme SWIFT, les affirmations générer lors des entretiens mener avec le DSSI, responsable de département risque et conformité et les acteurs qui participent dans le contrôle et nos observations collecter toute au long de notre stage, nous allons justifier dans quelle mesure on était d'accord avec les affirmation selon les métriques de contrôle de la mesure qui sont prédéfinie par le Framework CSP SWIFT pour arriver à la fin à classer les dans un échelle a 6 niveaux :

Figure 11: échelle d'évaluation des mesures



Source : élaborée par-nous même

Nous avons défini une échelle d'évaluation sur un poids de (5) :

• Pas du tout respect = 0

•Respecter un petit peu = 1.66

• Respecter à un certaine degré = 3.33

• Complètement respecter = 5

1.2.Contexte et description de contrôle CO4.1-Politique en matière de mots de passe

La mise en place d'une politique en matière de mots de passe qui protège contre les attaques courantes visant les mots de passe (par exemple, cassage, attaque par force brute) permet de protéger efficacement contre le piratage de comptes. Les cyber-pirates utilisent souvent les privilèges d'un compte piraté pour se déplacer latéralement au sein d'un environnement et étendre leur attaque. Un autre risque est le piratage des clés d'authentification locale visant à violer l'intégrité des transactions. Il faut toutefois garder à l'esprit que les mots de passe seuls ne sont généralement pas suffisants pour parer aux cyber-attaques actuelles. Les utilisateurs doivent donc appréhender cette mesure en étroite relation avec l'authentification multifactorielle requise

1.2.1 Identification des acteurs :

Lors de notre identification des rôles et des responsabilités des acteurs qui participent dans le contrôle nous avons constaté l'absence de l'utilisation de la matrice RACI, partant de cette observation nous avons signalé cette insuffisance au chef département risque et conformité et nous avons adopté une démarche pour réaliser les matrices RACI pour les deux contrôles étudier dans notre cas, vu l'importance de cette outil dans la définition des rôles et des responsabilité assigne pour chaque acteur dans le processus de contrôle

Tableau 7:matrice RACI pour CO 4.1

Acteur / Responsabilité	Contrôleur DSSI	Administrateur PAM	Administrateur système	Administrateur base de donnée	Administrateur réseau
Définir la politique de mots de passe	R/A	I/C	I/C	I/C	I/C
Demander la mise à jour de l'inventaire	R	I	I	I	I
Signaler l'ajout ou l'achat d'un nouveau équipement (logiciel ou un serveur ou d'une base de donnée)	I	R	R	R	R
Revoir et réviser la politique de mots de passe de la banque	R/A	C	C	C	C
Vérifier la conformité de la politique de MP par rapport au standard SWIFT	R	I	I	I	I
Rédiger le rapport de contrôle et dégager les recommandations	R	I	I	I	I

Source : élaboré par-nous même à partir des documents interne de l'entreprise

1.2.2 Evaluation de contrôle CO 4.1 :

Nous avons pu retirer les indicateurs clés pour évaluer la conformité de CO 4.1, ces indicateurs représentent des métriques associées au contrôle qu'elles doivent être respectées par la politique de sécurité de la banque, pour être conforme vis-à-vis le standard CSP SWIFT

Contrôle

CO 4.1 : politique en matière de mots de

Pas du tout respecter | Respecter un petit peu | Respecter à un certain degré | Complètement respecter•

Type de contrôle : Obligatoire

Tableau 8:tableau d'évaluation CO 4.1

N	Les métriques associées aux CO 4.1	Poids	Le degré du respect des métriques				Résultat
1	La redéfinition de la politique de mots de passe	5			X		3.33
2	Mise à jour de l'inventaire des équipements	5		X			1.66
3	Evaluation de l'efficacité de la politique de mots de passe	5	X				0
4	Gestion et stockage des mots de passe conforme à la bonne pratique international	5			X		3.66
5	Longueur, composition et complexité de mots de passe	5				X	5
6	La non réutilisation de mots de passe, expiration de mots de passe	5				X	5

Source : élaborer par nous-même à partir du CSP SWIFT

1.2.3 Cartographie les scenarios de menace de contrôle CO 4.1 :

Dans cette partie nous avons détecté et identifier les différents scenarios de menace et les risques qui peuvent impacter la politique de mots de passe de l'ASBA, les critères impactés (Disponibilité, Intégrité, Confidentialité, Traçabilité) et la criticités de chaque scénario peuvent varier en fonction des variables de l'environnement de l'utilisateur

Tableau 9:cartographie des scenarios de menaces de CO4.1

Scenario de menace	Nature	Critères impactées				Criticité
		D	I	C	T	
Les comptes des anciens utilisateurs ne sont pas supprimés systématiquement et existent toujours dans l'annuaire	Correctif	√	√		√	Moyenne
Une politique est mise en place pour les mots de passe, mais n'est pas appliquée, ce qui engendre l'utilisation par les opérateurs de mots de passe faibles facilement cassables lors d'une cyber-attaque.	Correctif	√	√	√		Élevé
Un mot de passe d'une longueur insuffisante permet de calculer son empreinte, qu'un cyber-pirate extrait de la mémoire du PC et qui lui permet de retrouver le mot de passe d'origine	Correctif	√	√	√	√	Élevé
Les mêmes mots de passe sont utilisés par un administrateur pour des systèmes situés à l'intérieur et à l'extérieur de la zone sécurisée, ce qui permet à un cyber-pirate de dérober le mot de passe le plus exposé et de le réutiliser pour accéder à la zone sécurisée.	Correctif	√	√	√	√	Élevé
Les comptes administrateurs sont détenus par d'autres personnes que l'administrateur système	Correctif	√	√		√	Faible

Source: élaboré par nous- même

1.3 Contexte et description de contrôle CO 4.2-Authentification à facteur multiples :

L'authentification multifactorielle(AMF) nécessite la fourniture de plusieurs (deux ou plus) des facteurs d'authentification courants suivants:

• Facteur de connaissance (quelque chose que l'opérateur connaît), un mot de passe.

• Facteur de possession (quelque chose que l'opérateur a), généralement: − jetons connectés (par exemple, jetons USB, cartes à puce), − jetons non connectés (par exemple, générateurs de mots de passe à usage unique utilisant le téléphone portable de l'opérateur)

• Facteur d'inhérence (quelque chose que l'opérateur est), généralement un facteur biométrique comme une empreinte digitale ou la reconnaissance vocale.

1.3.1 Identification des acteurs : Tableau 10:matrice RACI pour le contrôle CO 4.2

Acteur / Responsabilité	Contrôleur DSSI	Administrateur PAM	Administrateur système	Administrateur base de données	Administrateur réseau
La définition de la politique l'authentification multifactorielle	R/A	I/C	I/C	I/C	I/C
Demander la mise à jour de l'inventaire	R	I	I	I	I
Signaler l'ajout ou l'achat d'un nouveau équipement (logiciel ou un serveur ou d'une base de donnée) pour appliquer l'AMF	I	R	R	R	R
Réviser et renforcer l'authentification avec d'autre facteur	R	I	I	I	I
Vérifier la conformité de la politique d'AMF par rapport au standard SWIFT	R	I	I	I	I
Rédiger le rapport de contrôle et dégager les recommandations selon le GAP	R	I	I	I	I

Source : élaboré par nous-même à partir des documents interne de l'entreprise

1.3.2 Evaluation de contrôle CO 4.2 : Nous avons pu retirer les métriques associées au contrôle pour évaluer la conformité de CO 4.2

Contrôle

CO 4.2 : Authentification à facteur multiples (AFM)

Type de contrôle : Obligatoire

Tableau 11:tableau d'évaluationCO4.2

N	Les métriques associées aux CO 4.2	Poids	Le degré du respect des métriques				Résultat
			Pas du tout respecter	Respecter un petit peu	Respecter à un certain degré	Complètement respecter•	
1	La combinaison entre au moins deux facteurs d'authentifications (facteur de possession et facteur de connaissance)	5				X	5
2	Le dispositif utilisé pour le facteur de possession doit être différent du dispositif utilisé pour entrer le facteur de connaissance	5				X	5
3	La mise en œuvre de l'AMF au moins à une étape d'authentification lors un administrateur ou un utilisateur final veulent accédée à la zone sécurisé	5				X	5
4	L'AMF est mise en place pour l'accès des administrateurs à distance, en général pour l'authentification VPN.	5			X		3.66
5	Les facteurs d'authentification fournis sont attribués individuellement et associés à une responsabilité individuelle pour l'accès aux services, au système d'exploitation et aux applications.	5				X	5

Source : élaborer par nous-même à partir du CSP SWIFT

1.3.3 Cartographie les scenarios de menace de CO 4.2 :

Dans cette partie nous avons détecté et identifier les différents scenarios de menace et les risques qui peuvent impacter la politique d'AMF de l'ASBA, dans ce cas nous avons pu trouver seulement deux scenarios possible de risque car l'ASBA a établi une forte politique de AMF qui empêche les cyber-attaques et réduire les vulnérabilités, Les scénarios suivants sont des exemples destinés à aider les utilisateurs à comprendre les types de cyber-menaces de la mesure et ne sont pas exhaustifs, les critères impactés (Disponibilité, Intégrité, Confidentialité, Traçabilité) et la criticités(faible, moyenne, élevé) de chaque scénario peuvent varier considérablement en fonction des variables de l'environnement de l'utilisateur

Tableau 12:cartographie des scenarios de menace de CO 4.2

Scenario de menace	Nature	Critères impactés				Criticité
		D	I	C	T	
L'authentification multifactorielle n'est pas mise en place pour l'accès aux applications, ce qui permet à un cyber-pirate d'utiliser un mot de passe volé pour accéder à l'intégralité de l'interface de messagerie SWIFT.	Correctif	√	√	√	√	Élevé
L'authentification multifactorielle n'est pas mise en place pour l'accès au système d'exploitation de l'interface de messagerie, ce qui permet à un cyber-pirate d'utiliser un mot de passe volé pour obtenir un accès administrateur au système.	Correctif	√	√	√	√	Élevé

Source: élaboré par nous- même

1.4 Niveau de conformité des contrôles de la mesure :

Tableau 13:niveau de conformité des contrôles de la mesure

Contrôle	Résultat total(RT)	poids total(PT)	RT/PT	Niveau de conformité estimé
Politique en matière de mots de passe	18.65	30	0.62	Niveau 4
Authentification multifactorielle	23.66	25	0.94	Niveau 5

Source : élaborée par nous-même

Section2 : modélisation des contrôles de la mesure sous la forme d'un processus

Dans cette section nous allons exploiter nos connaissances acquises lors de l'évaluation de la conformité des contrôles SWIFT, et après que nous avons bien détecté les métriques associées aux contrôles à partir de CSP SWIFT et aussi grâce à l'aide des acteurs interne de la banque, nous allons définir un processus de contrôle de conformité optimisé qui regroupe les deux contrôles (politique en matière de mots de passe et authentification à facteur multiple) de la mesure étudier (prévenir les vols d'identifiant)

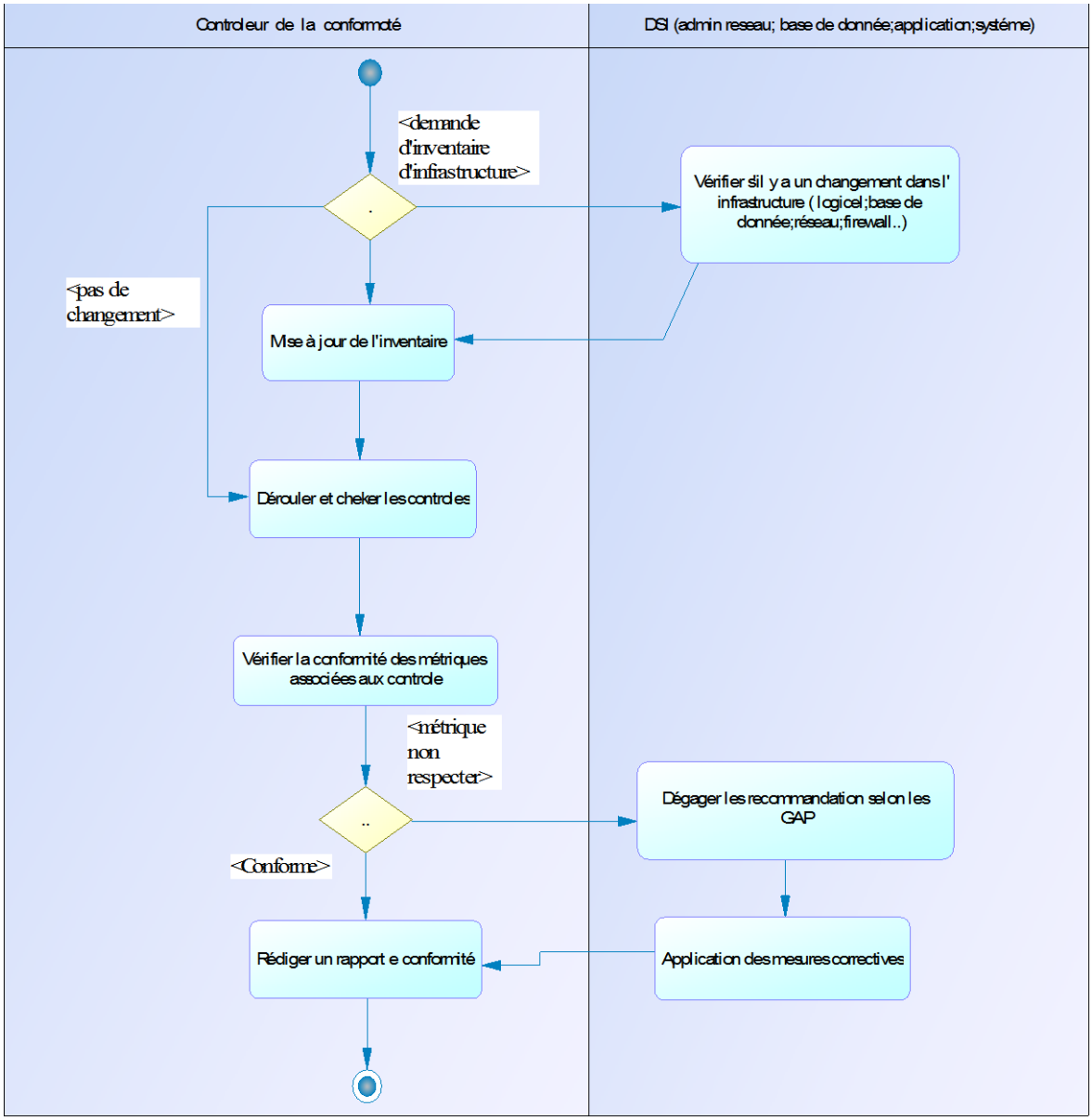
2.1 Objective de la modélisation des contrôles :

Le but de la modélisation des contrôles de sécurité SWIFT est de construire et d'optimiser le processus de contrôle de conformité de la DSI, qui rentre dans le projet de développement d'un workflow qui sert à automatiser ces contrôles et il permet à rationaliser le travail et aussi il permet un gain de temps et de ressource ainsi à minimiser les couts et la quantification de la charge de travail

Pour réaliser ce travail, nous avons utilisé le logiciel Power AMC comme un outil de modélisation des processus vu sa disponibilité (logiciel open source) et sa facilité d'utilisation

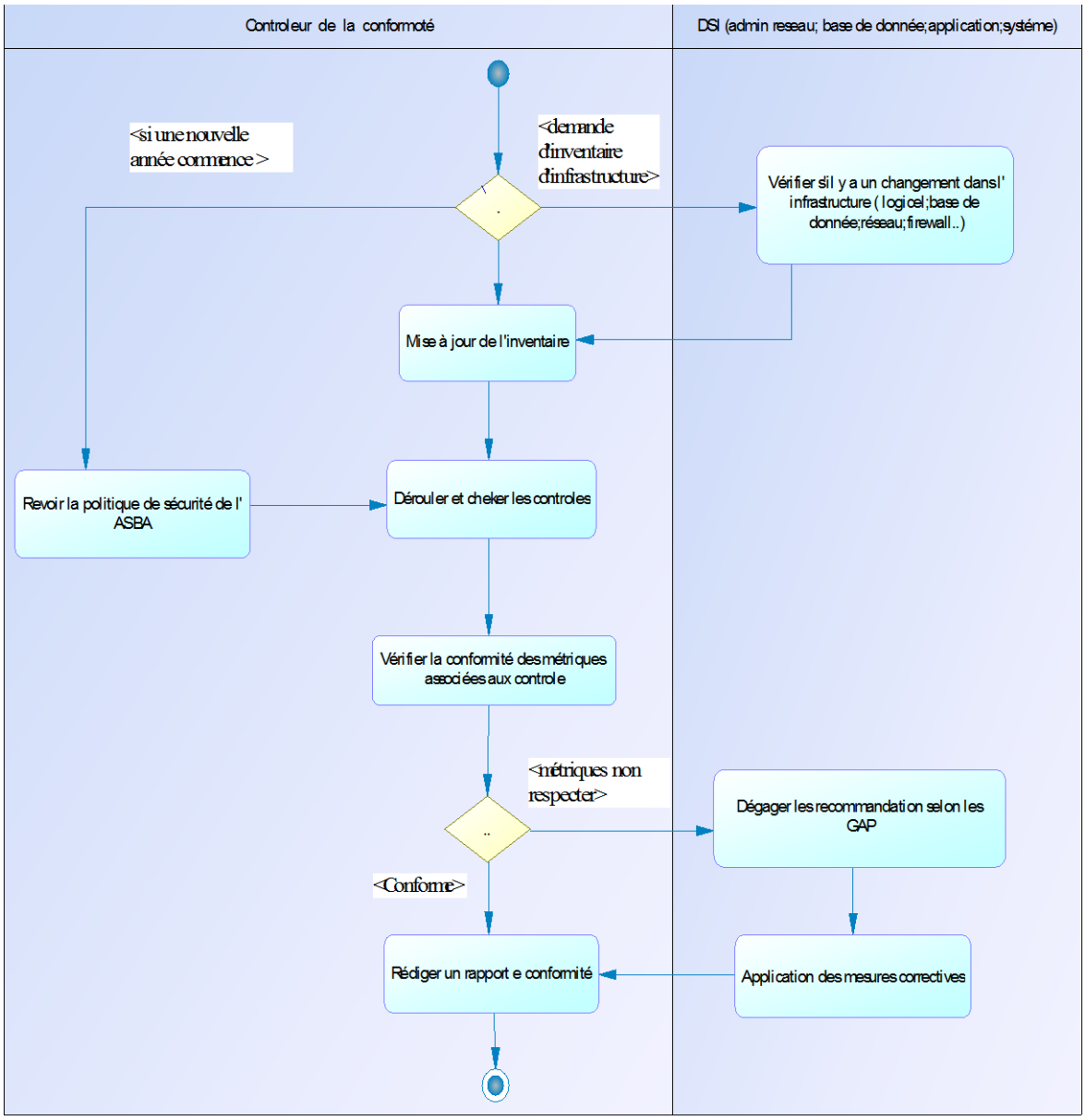
En premier temps nous avons pu développer un processus de contrôle mensuel, puis on a réussi développer un modèle plus optimisé qui rentre dans le projet de workflow

Figure 12:modélisation de processus de contrôle de conformité mensuel



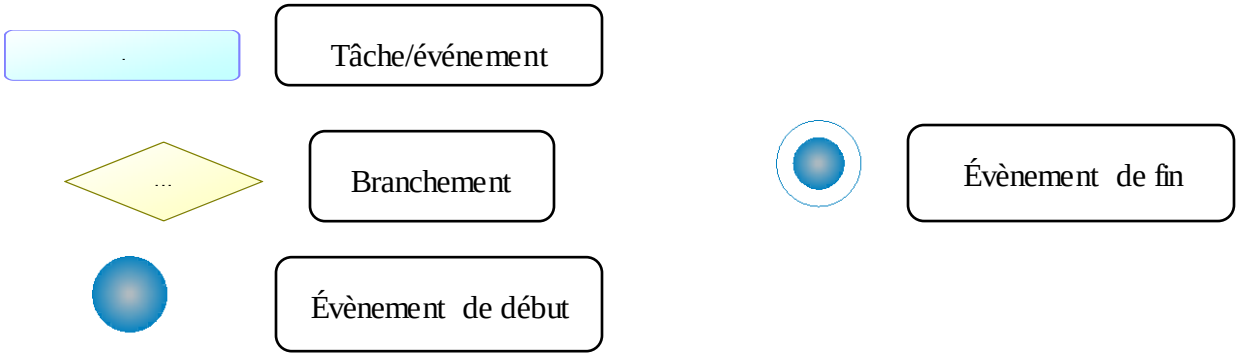
Source : élaboré par nous-mêmes avec logiciel PowerAMC à partir des documents internes de l'entreprise

Figure 13: processus de contrôle optimiser



Source : élaboré par nous-mêmes avec logiciel PowerAMC à partir des documents internes de l'entreprise

-Signification des formes :



2.2 La description du processus optimisé :

Le contrôleur demande aux administrateurs s'il y a un changement dans l'infrastructure ou changement d'équipement (par exemple un achat d'un nouveau serveur, réseau, firewall, base de donnée) car ce dernier implique forcement une modification dans la politique de mots de passe et une modification dans la politique d'authentification, donc le contrôleur reçoit une mise à jour d'inventaire et passe à à la vérification de la conformité des métriques associées aux contrôles qu'on a déjà extraire, il compare la politique de sécurité mise en place par la banque avec celle de CSP SWIFT afin de savoir le niveau de conformité et les scénario de menace et les vulnérabilité afin de dégager des recommandations et appliquer les mesures correctives pour être conforme vis-à-vis le CSP SWIFT

Si une nouvelle année commence, le contrôleur doit revoir la politique de sécurité de la banque et intégrer les bonnes pratiques de CSP SWIFT

CONCLUSION

Opérant dans un domaine d'activité très sensible, AL'SALAM BANQUE ALGERIE doit Établir le meilleur mécanisme possible pour atteindre ces objectifs et Développer des orientations stratégiques à long terme en veillant à la satisfaction de ces clients, la traçabilité des transactions et maîtrise des risques liés à cette activité. Pour cela elle doit assurer un niveau de sécurité élevé de son SI pour que ce dernier soit agile, performant et efficace

La gestion de la sécurité des risques des systèmes d'information fait partie intégrante du management de l'entreprise. C'est l'une des composantes de la gouvernance des SI. De manière globale, la direction générale est la propriétaire du système d'information et doit s'assurer du bon fonctionnement de celui-ci mais aussi de sa pérennité et ce compris de sa bonne évolution et de sa sécurité.

La DSI au sein d'AL SALAM BANQUE est chargée de couvrir l'ensemble des besoins et exigences de la Banque en matière de sécurité et conformité du système d'information par rapport à la réglementation de la Banque d'Algérie d'une part et aux Normes et Standards Internationaux

Nous avons dans le cadre de cette recherche utilisé le standard de sécurité «CSP SWIFT » de la société SWIFT pour évaluer la conformité d'AL SALAM BANQUE vis-à-vis ce standard, il était question d'évaluer en premier temps la conformité des contrôles de sécurités définit par le programme SWIFT, afin de modéliser ces contrôles étudier sous forme d'un processus optimiser de contrôle

En premier lieu, nous avons passé en revue les différentes théories sur la gestion des risques et la sécurité des SI et les différentes méthodes, standards, et norme utilisés dans le domaine, puis d'appréhender l'ensemble des mesures et des contrôles qui composent le standard CSP SWIFT. La revue de la littérature nous a aussi permet de positionner notre étude dans une épistémologie constructiviste et d'adopter une démarche qualitative par des outils de collecte de données (les entretiens et la documentation) pour évaluer la politique de sécurité de la banque existante vis-à-vis le programme SWIFT par l'extraction des bonnes pratiques et des métriques qui sont fournies par le programme SWIFT et aussi d'analyser l'ensemble des documents relatifs à la sécurité et la gestion des risques SI.

Avant de procéder à cette évaluation nous avons défini les acteurs et leurs responsabilités dans chaque contrôle étudier, dans cette étape on a constaté l'absence d'un outil qui définit les rôles et les responsabilités affectées pour chaque contrôle puis on a cartographie les

scenarios de risques qui peuvent arriver, L'évaluation de niveau de conformité des contrôles a été basée sur l'ensemble de nos remarques et sur des entretiens menés avec le DSSI et le responsable de département risque et conformité

Cependant, il ressort de cette évaluation que le contrôle CO4.2«authentification multifactorielle» est de niveau5 (bien gérer et conforme au CSP SWIFT), et le contrôle CO4.1«politique en matière de mots de passe» est de niveau4 (définit mais il ne respecte pas les bonnes pratiques à 100%)

Enfin, nous avons pu réaliser la modélisation des contrôles évaluer sous forme d'un processus optimisé qui rentre dans le projet de la réalisation d'un workflow sur lequel L'ASBA travail, l'objectif de ce processus est d'optimiser les ressources et les moyens et il permet à un gain de temps et ainsi à la quantification de la charge de travail et d'attendre efficience et d'automatiser le travail

En résumer, l'évaluation est faite pour savoir si la politique de sécurité de la banque Applique est conforme vis-à-vis le CSP SWIFT car c'une exigence de partenariat quelle doit être respecter par les clients de SWIFT, et la modélisation des processus de contrôles

Est une solution rational pour le contrôleur de la conformité au lieu de relire à chaque fois le standard pour extraire les bonnes pratiques le contrôleur déroule le processus et à la fin si la banque est conforme il rédige un rapport de conformité sinon il dégage des recommandation pour corriger les anomalies

Cette expérience du projet de fin d'études nous a été très enrichissante, car cela nous a permis d'étoffer nos connaissances acquises tout au long de notre parcours universitaire : licence en ingénierie du logiciel et master en management stratégique et système d'information. De plus, ce projet nous a également permis d'aller directement sur le terrain professionnel, de mettre en pratique les techniques de gestion de projet apprises auparavant.et de contribuer par notre modeste travail à proposer une solution pour le contrôleur de la conformité de standard CSP SWIFT

RÉFÉRENCES BIBLIOGRAPHIQUES

(CLUSIF)Club de la sécurité de l'information français. (2010). «Méthode Harmonisée d'Analyse de Risques (MEHARI) : guide d'analyse et de traitement des risques, paris»

ASNAR, Y., GIORGINI P., (2006). «Modelling Risk and Identifying Countermeasure in Organizations». CRITIS 2006: p55-66.

AVENIER. (2008). Méthodologie de la recherche : inscrire son projet de recherche dans un cadre épistémologique paris. Peason EDUCATION. France.

CHRISTOPHER, A.J., Dorofee, A.J., 2010. « RMF Risk Management Framework ».

CIGREF, (2002) sécurité des systèmes d'information (à paraitre) «quelle politique global de gestion des risques ?» Edition CIGREF, France. (2002).

CROZIER, FRIEDBERG. (1977). L'acteur et le système. EDITION de seuil 1977.

DEYRIEUX André, (2003) «le système d'information nouvel outil de stratégie»

DIAMONDE Moussa(2014) «les fondements de la gouvernance si : maitrise des risques »dans MANSOURI Khalifa, gouvernance des systèmes d'information

DUBOIS, J.-C. (1996). «L'analyse du risque : une approche conceptuelle et systémique, Chenelière-McGrawHill».

HAZEM B A, (2001) « Quelle méthodologie de recherche appropriée pour une construction de la recherche en gestion ? », disponible sur www.strategie-aims.com (page consultée le 23 juin 2021)

Hugon, Seibel,(1990), «Revue française de pédagogie», Edition Recherches impliquées

ISO/CEI 17799, (2005). «Information technology-Security techniques-Code of Practice for Information Security Management», International Organisation for StandardisationGenève.

ISO/CEI 27005, (2011). «Technologies de l'information - Techniques de sécurité - Gestion des risques liés à la sécurité de l'information, International Organisation for Standardisation, Genève».

KUHN. (1979). The signifiance of piaget's : formel Operations stage in EDUCATION. Journal of Éducation. Volume 61. Page[34-50].

LAOUFI Nabil(2017) «processus guidé pour l'identification des exigences de sécurité à partir de l'analyse des risques» thèse pour le doctorat en informatique, conservatoire national des arts et métiers paris

LIANG, L., Ren, W., & Song, J. (2013). The state of the art of risk assessment and management for information systems. 9th International Conference on Information Assurance and Security (IAS).

MAYER Nicolas, HUMBERT Jean-philippe(2006) «la gestion des risques pour les systèmes d'informations» Article paru dans le magasine MISC n°24

MAYER Nicolas, HUMBERT Jean-phillipe(2006).la méthode EBIOS : présentation et perspective d'utilisation pour la certification ISO 27001 [en ligne], https://portail-qualite.public.lu/dam-assets/fr/publications/confiance-numerique/etudes-nationales/Pub-NMA-JPH-MISC27/NMA-JPH-MISC27.pdf (page consultée le 20/06/2021)

MILES et HUBERMAN (1991) « analyses des données qualitatives », De Boeck Supérieur

PIAGET, (1967), « logique et connaissance scientifique encyclopédie de la pléiade ».

Secrétariat Général De la Défense Nationale (2010). EBIOS-Expression des Besoins et Identification des Objectifs de Sécurité : méthode de gestion des risques, Agence nationale de la sécurité des systèmes d'information, paris

SEYMOUR Bosworth (2002) «computer Security Handbook» John wiley and Sons

SIMISTER, T. (2000), «Risk management: the need to set standards», Balance Sheet, Vol. 8 No. 4, page. 9-10.

SWIFT, (2021) «SWIFT Customer Security Controls Framework v2021: Customer Security Programme»

STNEBURNER, G., GOGUEN, A., Feringa, A .(2007). «NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems», United States National Institute of Standards and Technology, Washington, DC, (2007).

THIÉTART et al (2003), « Méthodologie de recherche en management », Edition Dunod.

WACHEUX F, (1996), « Méthodes qualitative et recherche en gestion ». Economica.

WALKE, R; C.TOPKAR; V, MATEKAR. (2011). An approach to risk quantification in construction projects. International Journal of Engineering Science and Technology, 3(9), 6846-6855.

YVES B. DESHARNAIS (2018) «PCI DSS made easy», Edition PCI DSS 3.2.1, Canada, 458 page

ANNEXE:

DOCUMENTS INTERNES DE LA DSI

1. FORMULAIRE ACCÉS T-24

Référence :.....
STRUCTURE : ....

Nom & Prénom :.....
Fonction : .....
Liste des Accès:

Système	Type d'accès

le ..../.../.....Signature & cachet
du Responsable de la Structure

Partie 2 (Partie réservée à la Direction Des Systèmes d'Information)

Système : ..... User ID : .....

Système : ..... User ID : .....

Système : ..... User ID : .....

Le ..../.../..... Signature & cachet
du Responsable de la Structure de la DSI

2. FORMUMAIRE ACCÉS INTERNET

Nom :.....
Prénom :.....
Fonction :.....
Structure :.....

Motif de la demande .....

.....

Type d'accès

Permanent : ( )
Temporaire : ( ) de ..... au .....

Etendue de l'accès

( ) Accès complet
( ) Catégories de sites suivantes **(1)** :.....
( ) Uniquement les sites suivants **(2)**:.....

Signature du Demandeur : Signature et cachet Le :	Autorisation du Responsable de la structure : Signature et cachet Le :
Autorisation du Directeur Général Adjoint : Cachet et signature : Le :	Autorisation du Directeur Réseau **(3)** : Signature et cachet Le :
Direction des systèmes d'Information : Reçu le :..... Exécuté le :.....	Signature :

1- **Ex : finances, droit.....**
2- **Ex : www.alsalamalgeria.com, www.bank-of-algeria.dz**
3- **Signature du Directeur Réseau concerne uniquement les Agences**

3. FICHE D'AFFECTATION« ACCÉS VPN»

Utilisateur :

Nom et Prénom	
Fonction	
Structure & institution	
Motif	

Informations sur la plateforme de connexion distante

- Equipement utilisé pour la connexion (PC, Laptop ou autre) : .....
- Réseau utilisé pour la connexion (Sans fil, LS, Internet,) : .....
- Système utilisé pour la connexion (Windows, Linux, Unix, …etc) : .....
- Le client VPN à utiliser pour la connexion : .....
- Lieu de connexion (adresse et/ou commune et/ou ville et/ou pays) : .....

Paramétrage et Configuration du VPN : (A remplir par l'administrateur)

- Nom du Groupe VPN :.....
- Nombre de tentatives d'accès tolérées (Session) :.....
- Utilisateur (Login) :.....
- Liste des équipements ou zones concernés par l'accès (serveur/ adresse IP):.....
- Validité du compte :
  - Date et Heure début : .....
  - Date et heure fin : .....
  - Jours concernés (D, L, M, M, J, V, S) :.....

Validation de l'affectation de l'accès VPN :

Signature et cachet du Demandeur Le :	Signature et cachet du Responsable de la structure : (uniquement pour le personnel d'ASBA) Le :
Direction de la sécurité du système d'Information : Reçu le : Signature	Direction Générale Reçu le : Signature

Très important

Le compte d'accès VPN est personnel, ne peut être emprunté ni cédé à un collègue ou autre personne quel que soit son rang.