

UNIVERSITE DE YAOUNDE I

UNIVERSITY OF YAOUNDE I

\*\*\*\*\*

\*\*\*\*\*

**ECOLE NATIONALE SUPERIEURE  
POLYTECHNIQUE DE YAOUNDE**

**NATIONAL ADVANCED SCHOOL OF  
ENGINEERING OF YAOUNDE**

\*\*\*\*\*

\*\*\*\*\*

**DEPARTEMENT DES GENIES ELECTRIQUE  
ET DES TELECOMMUNICATIONS**

**DEPARTMENT OF ELECTRICAL AND  
TELECOMMUNICATIONS ENGINEERING**



# RÉALISATION D'UNE PLATEFORME D'AIDE AUX AUDITEURS DE SÉCURITÉ DES SYSTÈMES D'INFORMATION



**Mémoire de Fin d'études**

Présenté et soutenu par :

**BANG NJENJOCK FLORENT  
CHIRON**

En vue de l'obtention du

**DIPLOME D'INGENIEUR DE CONCEPTION DU GENIE  
DES TELECOMMUNICATIONS**

Sous la supervision académique du :

**Dr LELE Chrislin**

Devant le jury composé de :

- ◆ Président : NDZANA Benoît, Maître de Conférences E.N.S.P.Y
  - ◆ Rapporteur : **LELE Chrislin**, Chargé de cours E.N.S.P.Y
  - ◆ Examineur : MELINGUI Achille, Chargé de cours E.N.S.P.Y
- :

Année Académique : **2019-2020**

Date de soutenance : 16 Juillet **2020**

# Dédicace

*À mon frère BRIEUC*

## Remerciements

Je remercie les personnes suivantes pour leur contribution à la réalisation de ce travail:

- **Pr NDZANA Benoît**, Chef du département des Génies Électrique et des Télécommunications pour votre accompagnement et la bonne qualité des enseignements dispensé au sein de votre département.
- **Dr LELE Chrislin**, mon encadreur académique, pour vos bons conseils, votre temps et votre volonté à vouloir me pousser au maximum de mes capacités.
- **Dr MELINGUI Achille**, pour avoir accepté d'examiner ce travail.
- **Pr Remy Magloire ETOUA**, Directeur de l' ENSPY, ainsi qu'à tous mes enseignants pour les connaissances qu'ils m'ont donné.
- **Ing. MOUBITANG Yannick** pour son aide en particulier pour avoir fourni la documentation et des conseils qui ont permis la réalisation de ce travail.
- **M. BANG Louis-David** et **Mme BANG Christiane-Solange** pour leur amour et leur soutien moral et financier permanent.
- Mon frère et mes sœurs **BANG Bolie**, **BANG Anaël** et **BANG Claire** pour leur soutien permanent.
- Ma famille pour ses conseils et sa présence dans les bons moments comme dans les moments difficiles.
- Mes amis **AZOMBO Lucien Ludovic** et **TAKAM Richel Flamina** pour leur soutien moral constant dans les épreuves difficiles.
- Mes camarades des Génies Électrique et des Télécommunications et en particulier **ABOUBAKAR Issiakou**, **AMAWISSA Zacharie**, **CHUISSEU Larry**, **MADI François**, **NGNADOU Léticia**, **OTTOU Abed**, **SEPPE Constant** et **YONKEU Clémence** avec qui j'ai passé trois années enrichissantes dans une bonne ambiance.

- Mes amis depuis le lycée de Mballa 2 en particulier **KENETHA Benjamin, ASSE AWONO, SITEDJEYA Youyou, NGUETSA Arnold, GUIANOU Téclaire, ANONG Raïssa et GUIMBANG Blanche.**
- Toute personne ayant contribué de loin comme de près à l'aboutissement de ce travail.

## Liste des abréviations

---

### A

ANSSI: Agence Nationale de la Sécurité Evaluation des Systèmes  
d'Information

API: Application Program Interface

---

### C

CAMTEL: Cameroon Telecommunications

COBIT: Control Objectives for Information and Related Technology

CSRF: Cross Site Request Forgery

CSS: Cascading Style Sheets

---

### D

DCSSI: Direction Centrale de la Sécurité des Systèmes d'Information

DOM: Document Object Model

---

### E

EBIOS: Expression des Besoins et Identification des Objectifs  
de Sécurité

---

### F

FAT: Fiber Access Terminal

---

## G

GPS: Global Positioning System

---

## H

HTML: Hypertext Markup Language

---

## I

ISACA: Information Systems Audit and Control Association

ISO: International Organization for Standardization

ITIL: Information Technology Infrastructure Library

---

## J

JSON: JavaScript Object Notation

---

## L

LGPL: Lesser General Public License

---

## M

MEHARI: Méthode Harmonisée d'Analyse de Risques

MVT: Modèle Vue Template

---

## O

OCTAVE: Operationally Critical Threat, Asset and Vulnerability  
Evaluation

---

## S

SI: Système d'Information

SQL: Structured Query Language

---

## T

TAAO: Techniques d'Audit Assisté par Ordinateur

---

## U

UML: Unified Modeling Language

---

## X

XSS: cross-site scripting

## Résumé

Le développement des technologies de l'information a permis l'évolution des activités au sein des entreprises et des organismes. Ceci a amené divers risques internes et externes liés à la sécurité dans la gouvernance du système d'information dans ces structures. Ainsi il est primordial d'effectuer des audits de sécurité afin de connaître le niveau global de sécurité des systèmes d'information des organismes et de s'assurer de l'intégrité de leurs données et de leur capital informationnel. L'audit de sécurité se pose donc comme une tâche importante qui doit être faite de mains expertes et qui nécessite beaucoup d'analyse de la part de l'auditeur devant évaluer la sécurité du système d'information sous différents aspects notamment organisationnel, physique et opérationnel. C'est un long processus qui nécessite de naviguer à travers différents documents faisant état des politiques de sécurité, des configurations réseau et des systèmes de surveillances implémentés au sein de l'entreprise; ainsi qu'à travers des documents de normes et de lois définissant les directives et les réglementations à respecter pour une organisation afin d'atteindre un niveau de sécurité qui permet de garantir la confidentialité, l'intégrité et la disponibilité de l'information. Ainsi, bien que technique, l'audit de sécurité revêt également un aspect organisationnel nécessitant de nombreuses analyses et faisant intervenir beaucoup de documents de travail. C'est pourquoi nous avons développé une plateforme permettant l'utilisation de documents numériques qui seront stockés dans une base de données à laquelle aura accès les membres de l'équipe d'auditeurs; mettant également à leur disposition entre autres des outils de recherche et d'édition de documents ainsi qu'un forum de discussion sécurisé donnant la possibilité d'échanger leur différentes analyses en temps réel lors de la conduite de l'audit. Pour cela, nous nous sommes appuyés sur le langage de modélisation UML(Unified Modeling Language) pour modéliser notre solution et sur l'architecture MVT (Modèle Vue Template) afin de répondre aux différentes exigences.

**Mots clés:** Technologies de l'information, Système d'information, Audit de sécurité, Outil d'aide, Application web



## Abstract

The development of information technology has enabled the evolution of activities within companies and organizations. This has led to various internal and external security risks in the governance of the information system in these structures. It is therefore essential to conduct security audits to determine the overall level of security of organizations' information systems and to ensure the integrity of their data and information capital. The security audit is therefore an important task that must be carried out by expert hands and requires a lot of analysis by the auditor who must evaluate the security of the information system under different aspects including organizational, physical and operational. It is a long process that requires navigating through various documents that describe the security policies, network configurations and monitoring systems implemented within the company, as well as through documents of standards and laws defining the directives and regulations to be respected by an organization in order to achieve a level of security that guarantees the confidentiality, integrity and availability of information. Thus, although technical, the security audit is also an organizational aspect requiring a lot of analysis and involving a lot of working documents. This is why we have developed a platform allowing the use of digital documents that will be stored in a database to which the members of the audit team will have access; also providing them with tools for searching and editing these documents as well as a secure discussion forum giving them the possibility to exchange their different analyses in real time during the audit. To do this, we used the Unified Modeling Language (UML) to model our solution and the MVT (Model View Template) architecture in order to meet the different requirements.

**Keywords:** Information Technology, Information System, Security Audit, Help Tool, Web Application

# Liste des tableaux

2.1	Acteur intervenant dans le système . . . . .	34
2.2	Les différents cas d'utilisation . . . . .	35
2.3	Description textuelle du cas d'utilisation « S'authentifier » . . . . .	37
2.4	Description textuelle du cas d'utilisation « Créer compte » . . . . .	37
2.5	Description textuelle du cas d'utilisation « Modifier compte » . . . . .	38
2.6	Description textuelle du cas d'utilisation « Supprimer compte » . . . . .	38
2.7	Description textuelle du cas d'utilisation « Créer audit » . . . . .	39
2.8	Description textuelle du cas d'utilisation « Ajouter document » . . . . .	39
2.9	Description textuelle du cas d'utilisation « Modifier document » . . . . .	39
2.10	Description textuelle du cas d'utilisation « Télécharger document » . . . . .	40
2.11	Description textuelle du cas d'utilisation « Supprimer document » . . . . .	40
2.12	Description textuelle du cas d'utilisation « Créer questionnaire » . . . . .	41
2.13	Description textuelle du cas d'utilisation « Supprimer questionnaire » . . . . .	41
2.14	Description textuelle du cas d'utilisation « Créer section » . . . . .	42
2.15	Description textuelle du cas d'utilisation « Modifier section » . . . . .	42
2.16	Description textuelle du cas d'utilisation « Supprimer section » . . . . .	43
2.17	Description textuelle du cas d'utilisation « Créer rapport » . . . . .	43
2.18	Description textuelle du cas d'utilisation « Modifier rapport » . . . . .	44
2.19	Description textuelle du cas d'utilisation « Supprimer rapport » . . . . .	44
2.20	Description textuelle du cas d'utilisation « Télécharger rapport » . . . . .	45
2.21	Description textuelle du cas d'utilisation « Créer discussion » . . . . .	45
2.22	Description textuelle du cas d'utilisation « Supprimer discussion » . . . . .	46
2.23	Description textuelle du cas d'utilisation « Faire des recherches » . . . . .	46

# Liste des figures

1.1	Processus de réalisation d'un programme d'audit [3]	23
2.1	Méthode de développement en cascade	32
2.2	Diagramme des cas d'utilisation de la plateforme d'audit	36
2.3	Diagramme de classe d'analyse de la plateforme	48
2.4	Page d'accueil	49
2.5	Création d'un audit	50
2.6	Architecture physique de la solution	51
2.7	Architecture MVT	52
3.1	Diagramme de déploiement	56
3.2	Page de connexion de l'application	57
3.3	Page d'accueil de l'application	58
3.4	Ajout d'un document	59
3.5	Recherche, téléchargement, suppression d'un document	59
3.6	Modification d'un document	60
3.7	Création d'un questionnaire de contrôle	61
3.8	Création, recherche, suppression de sections	61
3.9	Modification d'une section	62
3.10	Création du rapport final d'audit	63
3.11	Création d'une discussion de groupe	64
3.12	Discussion (côté Danik)	64
3.13	Discussion (côté Ondoua)	65
A.1	Page de création du compte	70
A.2	Page de connexion	71
A.3	Page de gestion des documents	71
A.4	Page de gestion des questionnaires	72
A.5	Page de gestion du rapport d'audit	72
A.6	Page de création de discussions	73
A.7	Page de modification de compte	73

# Sommaire

<b>Dédicace</b>	<b>1</b>
<b>Remerciements</b>	<b>2</b>
<b>Liste des abréviations</b>	<b>4</b>
<b>Résumé</b>	<b>7</b>
<b>Abstract</b>	<b>8</b>
<b>Liste des tableaux</b>	<b>9</b>
<b>Liste des figures</b>	<b>10</b>
<b>Sommaire</b>	<b>11</b>
<b>Introduction générale</b>	<b>13</b>
<b>1 Contexte et problématique</b>	<b>15</b>
1.1 Généralités sur l’audit de sécurité des systèmes d’information . . . . .	16
1.1.1 Présentation . . . . .	16
1.1.2 Quelques standards . . . . .	20
1.1.3 Processus d’audit de sécurité des SI . . . . .	21
1.2 Contexte . . . . .	25
1.3 État de l’art des outils informatiques d’aide . . . . .	27
1.3.1 Les outils de productivité d’audit . . . . .	27
1.3.2 Quelques logiciels de productivité d’audit . . . . .	29
1.4 Problématique . . . . .	30
<b>2 Méthodologie</b>	<b>31</b>
2.1 Méthodologie de développement et langage de conception . . . . .	32

# RÉALISATION D'UNE PLATEFORME D'AIDE AUX AUDITEURS DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

---

2.1.1	Méthode de développement . . . . .	32
2.1.2	Langage de conception . . . . .	32
2.2	Analyse . . . . .	33
2.2.1	Exigences fonctionnelles . . . . .	33
2.2.2	Exigences non-fonctionnelles . . . . .	33
2.2.3	Les cas d'utilisation . . . . .	34
2.2.4	Modèle d'analyse du domaine . . . . .	46
2.3	Conception . . . . .	49
2.3.1	Conception des interfaces . . . . .	49
2.3.2	Architecture de la solution . . . . .	50
2.3.3	Sécurité . . . . .	52
2.4	Choix des outils d'implémentation . . . . .	53
2.4.1	Outils de développement . . . . .	53
2.4.2	Langages de programmation . . . . .	53
2.4.3	Frameworks et bibliothèques utilisés . . . . .	53
<b>3</b>	<b>Résultats et discussions</b>	<b>55</b>
3.1	Déploiement . . . . .	56
3.2	Résultats . . . . .	57
3.2.1	Connexion . . . . .	57
3.2.2	Page d'accueil . . . . .	58
3.2.3	Gestion des documents . . . . .	58
3.2.4	Gestion des questionnaires de contrôle . . . . .	60
3.2.5	Gestion du rapport d'audit . . . . .	62
3.2.6	Gestion des discussions . . . . .	63
3.3	Apport de la solution . . . . .	65
<b>A</b>	<b>Annexe: Interfaces de la maquette de l'application</b>	<b>70</b>

# Introduction générale

L'audit de sécurité consiste fondamentalement à l'analyse des points forts et des points faibles d'un système d'information et dégager ainsi les recommandations d'amélioration [6]. La qualité d'un audit de sécurité réside dans la profondeur et la minutie du travail d'analyse effectué par l'auditeur en se servant des différentes ressources à sa disposition notamment les divers documents de l'organisme audité présentant l'état de sécurité en son sein, et les rapports d'analyse faits lors de la phase de réalisation de l'audit. En effet, le travail d'analyse constituant le nœud de l'audit de sécurité il est essentiel de fournir à l'auditeur un environnement de travail limitant les désagréments liés à la recherche d'une information spécifique dans l'un des nombreux documents à sa disposition. Ces désagréments sont également liés à la non-disponibilité des documents à jour et aux difficultés de communication en temps réel avec ses collègues auditeurs lors de la phase de réalisation de l'audit de sécurité.

Au vu des problèmes sus-cités et au regard de l'évolution de l'Internet et des technologies de l'information nous avons la possibilité de créer des outils simples, adaptés à un contexte précis et abordables financièrement permettant de résoudre ce problème ce qui améliorera grandement l'efficacité de l'équipe d'audit lors de sa mission.

C'est dans le cadre de ce besoin que s'inscrit ce projet de fin de formation. Spécifiquement, le travail consiste à la « réalisation d'une plateforme d'aide aux auditeurs de sécurité des systèmes d'information »

Notre analyse sera structurée en trois parties:

- **Chapitre 1: Contexte et problématique**, où nous commencerons par clarifier les notions clés liées à l'audit de sécurité ainsi que son déroulement, puis nous entrerons dans le vif du sujet en présentant le contexte de notre travail puis l'état de l'art en matière d'outils d'aide à l'audit de sécurité, enfin nous parlerons du problème que nous cherchons à résoudre.
- **Chapitre 2: Méthodologie**, dans ce chapitre, nous présenterons toutes les méthodes utilisées pour le développement, l'analyse, la conception de notre solution et nous terminerons par les outils utilisés pour l'implémentation.

- **Chapitre 3: Résultats et Discussions**, dans ce chapitre nous présenterons la solution réalisée en décrivant son fonctionnement suivi de l'apport de celle-ci.
- Nous terminerons par une conclusion et des perspectives à mettre en œuvre afin d'améliorer notre travail.

# Chapitre 1

## Contexte et problématique

Dans ce chapitre il sera question de présenter les conditions conduisant à réaliser le présent travail. Le chapitre sera articulé en quatre parties:

- Les généralités sur l'audit de sécurité
- Le contexte du projet
- Un bref état de l'art des outils d'aide à l'audit
- La problématique à laquelle nous avons été confrontée



## 1.1 Généralités sur l'audit de sécurité des systèmes d'information

Dans cette partie il est question de définir les contours d'un audit de sécurité en expliquant ce que c'est, puis quels sont les acteurs concernés et enfin comment il se planifie, se déroule et se conclut.

### 1.1.1 Présentation

#### Définitions

Avant de définir ce qu'est un audit de sécurité il convient d'abord de clarifier la notion de système d'information. **Un système d'information (SI)** est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information [1], en général grâce à un réseau d'ordinateurs . Ces ressources incluent le personnel, des procédures, des équipements, des logiciels.

**Un audit** est d'après la norme ISO (International Organization for Standardization) 19011: 2011, un processus systématique, indépendant et documenté permettant d'obtenir des preuves d'audit et de les évaluer objectivement pour déterminer la mesure dans laquelle les critères d'audit sont remplis [3]. On peut ainsi dire qu'un audit de sécurité d'un SI est un audit focalisé sur la sécurité du système d'information.

**Critère d'audit:** Ensemble de polices, de procédures ou d'exigences utilisées comme référence auxquelles les preuves d'audit sont comparées [3].

**Preuve d'audit:** Enregistrements, déclarations de faits ou toute autre information pertinente et vérifiable pour les critères d'audit [3].

#### Objectifs de l'audit de sécurité des SI

Un audit de sécurité est spécifique à chaque entreprise ou institution auditée et est donc réalisé suivant le besoin particulier de cette dernière notamment:

- Évaluer le niveau de maturité du SI en terme de sécurité suite à la demande d'un commanditaire d'audit;
- Vérifier l'efficacité de la politique de sécurité du SI mise en place;
- Tester l'installation d'un nouvel élément dans le SI;
- Analyser et réagir suite à une attaque;
- Tester la résistance du SI par la simulation d'attaques dans des conditions réelles;
- Se certifier (par exemple ISO 27001) etc.

Une mission d'audit de sécurité permet de trouver les vulnérabilités du SI puis de proposer des actions correctives à travers des contrôles. À la fin de l'audit, est délivré par l'auditeur, un rapport détaillé faisant la lumière sur les écarts détectés. Ce rapport comprend aussi un plan détaillé des mesures à appliquer par ordre de priorité, mesures ayant été validées par l'organisme audité. Les audits sont généralement classés en trois catégories qui seront présentées dans le paragraphe suivant.

### Classification des audits

Les audits sont généralement regroupés en trois catégories bien distinctes:

1. **Les audits internes:** Ils sont réalisés pour des organismes souhaitant que leur système d'information soit examiné par rapport à des exigences de sécurité. Ces audits sont établis par des auditeurs internes ou externes à l'organisme.
2. **Les audits externes:** Ici le commanditaire est une entité externe à l'organisme audité, entité qui collabore avec l'organisme audité. L'équipe d'audit intervenant ici est externe à la structure auditée.
3. **Les audits de certification:** Ici le commanditaire est l'organisme audité qui veut prouver que son SI répond aux standards internationaux par exemple l'ISO 27001. L'auditeur ici est un organisme externe accrédité.

La classification des audits ayant été faite, l'on peut à présent entrer en profondeur en présentant les différents domaines d'audit de la sécurité.

### Les domaines d'audit de la sécurité

Il est à souligner que l'audit de sécurité ne se limite pas à des tests de vulnérabilités mais qu'il revêt un aspect plus large et global. Ainsi il couvre différents domaines à savoir l'audit organisationnel et Physique et l'audit technique de sécurité.

#### A. Audit Organisationnel et Physique

L'audit organisationnel et physique permet de déterminer l'état de sécurité complet du SI, d'identifier les zones de défaillances et les risques en découlant. Il permet de mettre en lumière également les manquements liés au processus de management de la sécurité. Dans cette phase les outils de prédilection utilisés sont les questionnaires adaptés au contexte de l'organisme audité, les interviews de certains membres du personnel, ainsi que l'analyse de tout document utile et pertinent pour cette étape. [2] Les éléments potentiellement abordés lors du déroulement de cet audit sont:

- **Politiques de sécurité de l'information:** Il s'agit ici de la nécessité de la mise sur pied et de la mise à jour régulière d'une politique de sécurité de l'information par l'audité.
- **Sécurité des ressources humaines:** Cette section a trait aux recommandations liées à la formation et la sensibilisation des utilisateurs sur les menaces pouvant compromettre la sécurité de l'information ainsi que sur les pratiques qu'ils doivent adopter pour protéger l'information.
- **Contrôle d'accès:** Ici, l'on définit les bonnes pratiques à adopter pour bien gérer et contrôler l'accès à l'information assurant ainsi la protection des systèmes en réseau.
- **Cryptographie:** Les mesures visant à assurer la confidentialité et l'intégrité de l'information par des algorithmes de cryptographie.
- **Sécurité environnementale:** Cette section clarifie les mesures à adopter afin de protéger les locaux contre les accès non autorisés, pour assurer la sécurité du matériel contre le vol ou le sabotage, pour réduire les dégâts en cas de désastre naturel. On a notamment l'adoption de la validation d'entrée à l'aide de carte magnétique. La disposition de gardes au niveau de locaux de stockage des équipements du réseau d'entreprise.
- **Sécurité des communications:** Cette section définit les mesures pour assurer la protection des informations sur le réseau ainsi que la sécurité des informations échangées avec des organismes extérieurs.
- **Gestion des incidents:** Ici, on traite des mesures nécessaires pour détecter des incidents notamment des systèmes de détection d'intrusion, puis les traiter.
- **Sécurité de l'information dans la gestion de la continuité de l'activité:** Dans cette section, sont décrites les mesures à adopter pour réduire l'impact d'événements tels que les catastrophes naturelles ou les pannes matérielles pour pouvoir assurer la poursuite des activités de l'entreprise. On note par exemple la sauvegarde hebdomadaire des données de l'entreprise dans des datacenters.
- **Conformité du SI:** Dans cette section on traite du respect des standards requis par la politique de sécurité adoptée et par les normes de sécurité.

## B. Audit Technique de sécurité

L'audit technique consiste en une analyse plus profonde du SI (équipements réseau, l'infrastructure réseau, applications) en vue de détecter ses vulnérabilités.

- **Audit des vulnérabilités système**

Dans ce type d'audit il est question de réaliser différents tests permettant de mettre en exergue les failles sur les équipements réseau, sur les applications; afin de mettre au pied des mesures correctives: L'audit de vulnérabilités se déroule en deux phases:

- **Phase de découverte des vulnérabilités:** Dans cette phase il s'agit d'utiliser des outils qui s'appuient sur un ensemble de failles connues pour effectuer des scanners de vulnérabilités des applications web, des équipements réseau etc ...
- **Phase d'analyse des vulnérabilités:** Ici on fait une analyse des vulnérabilités découvertes pour dégager un ensemble de mesures (en accord avec la politique de l'entreprise) pour y remédier.

- **Audit d'architecture réseau**

Ici il est question d'analyser l'architecture du réseau pour déterminer les zones susceptibles de compromettre la sécurité. On étudie la topologie (logique et physique) du réseau à l'aide de la documentation et des outils de découverte du réseau, pour s'assurer du respect des bonnes pratiques quant à l'emplacement des équipements réseau (routeur, switch, pare-feu etc ...).

- **Audit de configuration**

Dans l'audit de configuration, il est question d'une évaluation technique des configurations des éléments informatiques (équipements réseaux, applications, bases de données, systèmes d'exploitation, etc...) qui entrent dans la constitution du SI afin de s'assurer de leur conformité avec les mesures de sécurité adoptées.

- **Tests d'intrusion**

L'objectif est de mettre à l'épreuve la résistance du SI face aux attaques (internes ou externes au réseau de l'audité) en simulant des scénarios d'attaques préparés à l'avance, dans lesquels il est question d'exploiter les failles découvertes lors de la phase de détection des vulnérabilités. Les tests d'intrusion sont conduits suivant trois approches:

- **Approche en boîte noire:** Le testeur ne dispose d'aucune information sur l'environnement avant l'attaque
- **Approche en boîte grise:** Le testeur dispose de connaissances partielles
- **Approche en boîte blanche:** Le testeur dispose de toutes les informations lui permettant d'examiner en profondeur l'environnement d'attaque.

- **Audit applicatif**

Ici, il est question d'évaluer le niveau de sécurité des différentes applications utilisées (application de gestion des stocks, application de messagerie etc ...) au sein de l'organisme audité, qui font partie intégrante de son SI. La méthode employée est très souvent l'audit de code (pour les applications auxquelles on y a accès) source qui demande l'intervention d'un auditeur expert du langage de programmation utilisé pour développer cette application.

Comme toute discipline l'audit de sécurité doit respecter un certain nombre de standards.

### 1.1.2 Quelques standards

Il existe différents standards permettant la conduite d'un audit de sécurité. Certains doivent être respectés en vue d'obtenir une certification (ISO 27001, 27006 par exemple) et d'autres servent juste de guides facilitant la tâche d'audit. Certains de ces standards sont présentés ci-dessous:

- **L' ISO 27001:** Elle s'intitule « Systèmes de gestion de sécurité de l'information - Exigences »; Elle fournit des exigences pour un système de gestion de la sécurité de l'information [12]. Les organisations qui satisfont aux exigences peuvent être certifiées par un organisme de certification accrédité après la réussite d'un audit.
- **L'ISO 27006 :** Elle spécifie les exigences à respecter pour les organismes qui procèdent à l'audit en vue d'une certification des SMSI;
- **CobiT (Control Objectives for Information and Related Technology) :** C'est un référentiel développé par l' ISACA ( Information Systems Audit and Control Association). Il définit un ensemble de processus génériques pour la gestion des technologies de l'information, chaque processus étant défini avec des entrées et des sorties de processus, des activités de processus clés, des objectifs de processus, des mesures de performance et un modèle de maturité élémentaire [7];
- **ITIL (Information Technology Infrastructure Library) :** est une bibliothèque qui définit la structure organisationnelle et les compétences requises d'une organisation de technologie de l'information et un ensemble de procédures et de pratiques de gestion opérationnelle standard pour permettre à l'organisation de gérer une opération informatique et l'infrastructure associée[8];
- **EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) :** C'est une méthode d'évaluation des risques en informatique, développée en 1995 par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) et maintenue par l'Agence Nationale de la Sécurité des Systèmes d'Information

(ANSSI) qui lui a succédé en 2009. Elle a connu une évolution en 2010 puis a été renommée en EBIOS Risk Manager [9];

- **MEHARI (Méthode Harmonisée d'Analyse de Risques)** : C'est une méthode d'évaluation (libre et open source) de gestion des risques de l'information, à l'usage des professionnels de la sécurité de l'information [10];
- **OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)**: Elle a été créée par l'Institut d'ingénierie logiciel de l'université américaine Carnegie Mellon en 1999. Elle permet d'identifier et de gérer les risques de sécurité de l'information. Elle définit une méthode d'évaluation complète qui permet à une organisation d'identifier les actifs d'information qui sont importants pour la mission de l'organisation, les menaces qui pèsent sur ces actifs et les vulnérabilités qui peuvent exposer ces actifs aux menaces [11].

### 1.1.3 Processus d'audit de sécurité des SI

Un audit de sécurité se déroule suivant un processus précis et se décline en trois grandes parties à savoir:

1. La phase de préparation de l'audit
2. La phase de conduite de l'audit
3. La phase de clôture

Pour décrire de façon claire ces différentes phases nous allons nous servir du document de référence la norme [3] ISO 19011:2011 intitulée « Lignes directrices pour l'audit des systèmes de management »; elle spécifie entre autres les principes de l'audit, le management d'un programme d'audit et la réalisation d'audits des systèmes de management de la sécurité de l'information .

#### La phase de préparation de l'audit

Une mission d'audit de sécurité d'un SI a lieu sous demande d'un commanditaire (Ce commanditaire peut être l'organisme audité ou tout autre organisme qui a un intérêt à la réalisation de cet audit). Ainsi une lettre de mission est rédigée et signée par le commanditaire puis envoyée au prestataire d'audit qui désignera un responsable. Le responsable de l'audit devra entrer en contact (contact formel ou informel) avec l'audité afin de définir entre autres les objectifs de l'audit, ses critères, de discuter des canaux de communication des ressources nécessaires à la préparation et à la conduite de l'audit. L'organisme audité devra fournir au prestataire toute la documentation nécessaire pour conduire cet audit.

Puis un programme d'audit sera établie par le prestataire en accord avec les objectifs de l'audit. Puis ce programme d'audit devra être validé par le commanditaire et enfin signé par les deux parties prenantes. Il contient entre autres les éléments suivants:

- **Les objectifs du programme d'audit et des audits individuels**
- **Les modalités de l'audit (étendue, nombre, types, durée, date de l'audit)**
- **Les procédures d'audit**
- **Les critères d'audit**
- **La composition des équipes d'audit**
- **Les ressources nécessaires (dispositions logistiques, ressources matérielles, ressources humaines, etc.)**
- **Les processus de gestion de la confidentialité, de la sécurité de l'information et d'autres questions similaires.**

Le programme d'audit est réalisé en suivant un certain nombre d'étapes présentées à la figure 1.1 inspirée de la norme ISO 19001:

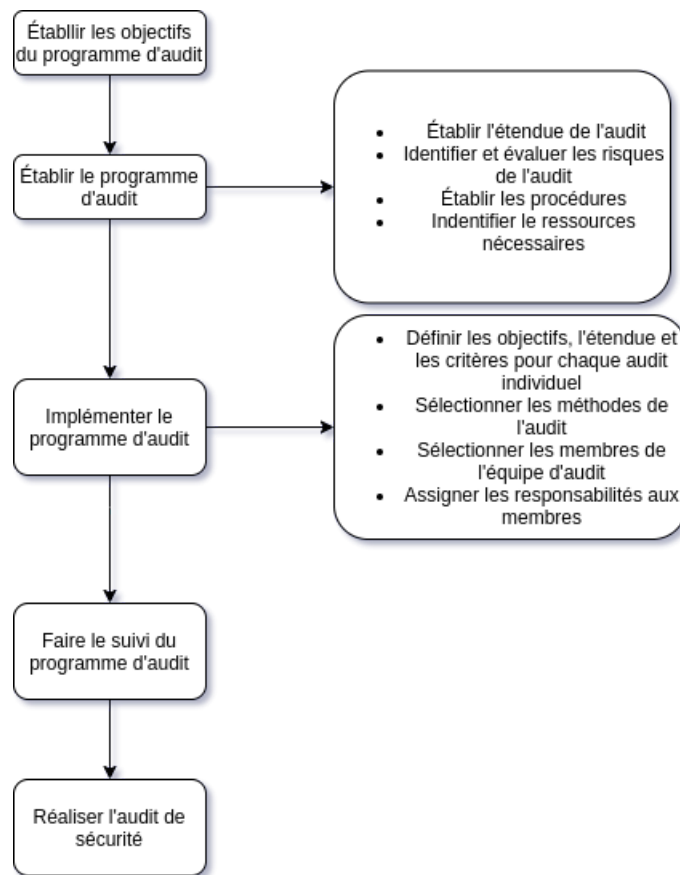


Figure 1.1: Processus de réalisation d'un programme d'audit [3]

Une fois le programme d'audit réalisé, les membres de l'équipe d'audit entament la rédaction des documents nécessaires à la conduite de l'audit incluant :

- **Les questionnaires et checklists:** Ils peuvent se baser sur les questionnaires techniques usuels mais adaptés aux objectifs et critères établis dans le programme d'audit;
- **Les questionnaires d'interview;**
- **Les scénarios de tests techniques;**
- **Revue documentaire etc.**

### La phase de conduite de l'audit

La phase de conduite de l'audit se déroule en plusieurs étapes également et débute par la réunion d'ouverture puis se poursuit par la phase d'exécution, ensuite l'enregistrement de la phase d'exécution et enfin la réunion de clôture.



## 1. La réunion d'ouverture

Elle se tient dans les locaux de l'organisme audité et regroupe l'équipe d'auditeurs, l'audité et le commanditaire de l'audit. Son objectif est de confirmer l'adhérence de toutes les parties au programme d'audit, de présenter l'équipe d'auditeurs, de s'assurer que toutes les activités prévues par l'audit peuvent être conduites, et de clarifier toute ambiguïté. À la fin de cette réunion un compte rendu doit être rédigé.

## 2. La phase d'exécution

Elle consiste à conduire toutes les activités prévues dans le plan d'audit à savoir:

- Les interviews avec certains responsables dans l'entreprise sont effectuées et également des immersions qui consiste pour l'auditeur à observer certaines activités critiques. Toutes les informations recueillies figureront dans un compte rendu qui sera soumis et validé par l'audité et le commanditaire d'audit.
- L'analyse d'écart entre les preuves fournies et les différents critères d'audit dans le but de générer des constats qui sont soit une conformité soit une non-conformité aux critères. Et ces constats seront documentés.

Le prestataire d'audit doit régulièrement communiquer avec le commanditaire et l'audité afin de leur communiquer l'état d'avancement de l'audit et les entraves rencontrées.

## 3. La phase d'enregistrement

C'est dans cette phase qu'il faut être méticuleux car tous les documents qui résultent de la phase d'exécution doivent être soigneusement archivés. Ces documents sont entre autres:

- Les comptes rendus d'interview et d'immersion
- Les fiches d'écarts
- Les relevés techniques contenant les résultats des scans de sécurité, le rapport d'analyse des vulnérabilités, quelques échantillons du trafic réseau, la liste des anomalies de configuration des équipements réseau.

## 4. La réunion de clôture

Le but de la réunion de clôture est de présenter les constats d'audit et les conclusions. Cette réunion réunit l'équipe d'auditeurs, l'organisme audité et lorsque nécessaire, les responsables des fonctions auditées. C'est également pendant la réunion de clôture que l'auditeur en chef informe, le cas échéant, de toute situation qui ferait diminuer le niveau de confiance des constats et conclusions.

### La phase de clôture de l'audit

Dans la phase de clôture il s'agit essentiellement de la rédaction et de la distribution du rapport final d'audit. Le rapport d'audit doit être cohérent avec le programme d'audit défini dès le départ. Il contient notamment:

- Les objectifs de l'audit
- L'étendue de l'audit c'est-à-dire les différentes fonctions ou les différents contrôles audités
- Les commanditaires de l'audit
- Les noms des différents auditeurs impliqués ainsi que des participants du côté des audités
- Les dates et la localisation des activités d'audit conduites
- Les critères d'audit
- Les preuves et constats d'audit
- Les recommandations
- Des informations permettant de savoir jusqu'à quel niveau les critères d'audit ont été remplis.

## 1.2 Contexte

Notre travail a été réalisé dans le cadre de l'obtention du diplôme d'ingénieur du génie des télécommunications à l'École Nationale Supérieure Polytechnique. Et notre stage a été effectué au sein d'Evolving Consulting, entreprise qui fournit des services dans le domaine des TICs notamment la fourniture de matériel informatique et Télécoms, des études de faisabilité et d'opportunités, les audits de sécurité des systèmes d'information etc ...

Dans les entreprises, les organisations et les institutions, l'on a besoin d'assurer la bonne circulation de l'information, son stockage et son traitement en vue de fournir un service de qualité au personnel, aux usagers et aux clients. C'est pourquoi ces organismes mettent sur pied en leur sein, un système d'information. Prenons par exemple le cas de la CAMTEL qui est l'opérateur historique au Cameroun. Elle a mis au point un système qui permet de disposer de la localisation GPS<sup>1</sup> des FATs<sup>2</sup> installés

---

<sup>1</sup>Global Positioning System

<sup>2</sup>Fiber Access Terminal

dans la ville de Yaoundé, localisation qui sera entrée dans la plateforme prévue à cet effet [13]. Ce système d'information (constitué de la plateforme, des techniciens qui installent les FATs et fournissent leur localisation et des bases de données etc...) permet le suivi des équipements et une intervention rapide en cas de pannes de la fibre chez des abonnés dans une zone précise d'où l'importance d'un SI dans la conduite des activités d'une entreprise.

De plus les informations gérées par un SI peuvent être sensibles et privées d'où la vulnérabilité d'un pare-feu peu entraîner l'infiltration d'un hacker qui dérobera des données de conversations téléphoniques; d'où il est nécessaire de s'assurer du bon état de sécurité du SI. C'est pourquoi des audits de sécurité sont effectués, dans le but de vérifier que le SI respecte les standards de sécurité et ne sont pas sujets à des vulnérabilités pouvant engendrer des conséquences catastrophiques. Ainsi, un audit de sécurité est un processus au cours duquel une équipe composée d'auditeurs (ayant des compétences variées) va collecter de nombreux documents sur la structure à auditer (la politique de sécurité du SI, les rapports d'audits précédents etc ... ), les étudier en vue de préparer l'audit, va ensuite préparer des documents (questionnaires d'interview, questionnaires de contrôle, checklists etc ... ) en vue d'effectuer l'audit de différentes fonctions de la structure (fonction marketing, fonction vente etc ... ) sur des aspects organisationnel (évaluations des politiques de sécurité définies ... ), physique (sécurité des locaux contenant les serveurs ...), technique (sécurité des routeurs, des switches, des postes de travail, des applications etc ... ) et enfin devra réunir tous les documents y découlant, les analyser en vue de faire des recommandations pour améliorer la sécurité.

Également lors de la conduite de l'audit ou de la phase d'analyse des constats d'audits, l'équipe d'auditeur a besoin de communiquer et d'avoir éventuellement accès à différents documents ainsi il leur faudrait à chacun avoir des exemplaires et s'ils sont situés à des localisations différentes le partage de ces ressources peut introduire des lenteurs dans le travail (par exemple il faut numériser le document, l'envoyer par mail puis le destinataire devra l'imprimer pour mieux travailler avec etc ...) ce qui pourrait apporter d'autres complications. Il en découle donc qu'il y a une masse importante de documents qui devront être regroupés, classés, analysés manuellement ce qui peut poser des problèmes d'efficacité. D'autres problèmes rencontrés seront aussi la perte de documents, le suivi des versions des documents lorsque plusieurs membres de l'équipe travaillent sur le même document, la collaboration pour le partage des commentaires, des analyses, des documents, les alertes pour notifier en cas de problèmes lors d'une analyse.

L'avènement des outils informatiques et surtout de nouvelles technologies de traitement d'image nous donne la perspective de solutions simples et innovantes pour résoudre des problèmes rencontrés dans différents secteurs d'activités notamment celui de l'audit de sécurité (dans le cas présent).

Après avoir précisé le contexte de notre travail, nous présenterons dans la section suivante un bref état de l'art permettant de positionner notre solution.

## 1.3 État de l'art des outils informatiques d'aide

[4] La technologie informatique est devenue partie intégrante de la plupart des fonctions organisationnelles. Il est probable que de nombreux clients d'audit ont éliminé ou élimineront une partie substantielle de leurs documents papier et les remplaceront par des documents électroniques déposés uniquement sous forme informatique. Un auditeur qui n'est pas en mesure d'utiliser efficacement les outils et techniques d'audit informatisés sera désavantagé. L'auditeur d'aujourd'hui doit être doté d'une compréhension des outils et techniques alternatifs pour tester le fonctionnement des systèmes informatiques et recueillir et analyser les données contenues dans les fichiers informatisés. Les auditeurs peuvent tirer parti de ces outils et techniques pour être plus efficaces et efficaces lorsqu'ils effectuent des travaux d'audit. Les outils et techniques utilisés dans les audits informatiques comprennent:

- **Outils de productivité d'audit:** logiciel qui aide les auditeurs à réduire le temps passé sur tâches administratives en automatisant la fonction d'audit et en intégrant les informations recueillies dans le cadre du processus d'audit.
- **Techniques de documentation du système:** méthodes, telles que l'organigramme, le diagramme de flux de données et les diagrammes de processus métier appliqués aux documents et aux systèmes d'application de test, aux processus informatiques et à leur intégration dans l'environnement informatique.
- **Techniques d'audit assisté par ordinateur (TAAO) :** logiciel qui aide les auditeurs à évaluer les contrôles des applications et à sélectionner et analyser les données informatisées pour les tests d'audit de fond.

Dans la suite , nous nous centrerons sur les outils de productivité d'audit et comment ils aident dans le processus d'audit.

### 1.3.1 Les outils de productivité d'audit

Dans la phase de réalisation d'audit, l'essentiel consiste très souvent à faire une évaluation des contrôles internes mis en place par l'organisme audité afin de déterminer s'ils sont efficaces ou s'ils nécessitent des améliorations. [4] Cependant, de nombreuses tâches associées à la réalisation d'un audit, telles que la planification, les tests et la documentation des résultats, bien que nécessaires, prennent du temps pour effectuer les contrôles des travaux d'évaluation. C'est là que les outils de productivité des auditeurs entrent en jeu. Les outils de productivité des auditeurs aident les auditeurs à automatiser les fonctions d'audit nécessaires et à intégrer les informations recueillies dans le cadre du processus d'audit. Les différentes fonctions automatisées via ces outils sont par exemple:

- Planification et suivi des audits
- Documentation et présentations
- La communication
- Gestion des données, documents de travail électroniques

### **Planification et suivi des audits**

Dans les tâches de planification d'audit il est nécessaire d'établir un calendrier d'audit, un budget prévisionnel afin de suivre les progrès de l'audit. Les feuilles de calcul, les logiciels de base de données, de gestion de projet peuvent être utilisés pour la documentation et la planification des audits.

### **Documentation et présentations**

Des outils, tels que la suite Microsoft Office, fournissent des fonctionnalités pour faciliter la création et la présentation de documents. D'autres outils incluent la vidéo-conférence et / ou les logiciels de capture vidéo pour fournir des présentations aux collaborateurs du monde entier et pour documenter les preuves d'audit, respectivement.

### **La communication**

L'audit de sécurité est un processus réalisé en équipe d'où la nécessité d'un partage rapide et efficace des données ainsi que de communiquer entre membres du groupe. Accéder aux données à jour, échanger des commentaires et analyses permet au personnel d'audit d'effectuer l'audit dans des conditions optimales.

### **Gestion des données, documents de travail électroniques**

L'établissement d'une connectivité électronique offre au personnel d'audit la possibilité d'accéder aux données et de les saisir dans une base de connaissances par exemple une base de données, ce qui leur permet un accès peu importe leur localisation physique. Ainsi les applications de base de données peuvent être développées permettant la saisie électronique des données.

### 1.3.2 Quelques logiciels de productivité d'audit

#### NiftyISO

NiftyISO<sup>3</sup> est une application web permettant de planifier, publier et de gérer les activités d'audit. Elle figure parmi les solutions les plus abordables financièrement mais toutefois relativement cher dans un contexte camerounais pour de jeunes entreprises d'audit car propose des plans de 75 US \$ (soit 43.800 FCFA environ). Elle dispose de fonctionnalités de création d'audit, de questionnaire de contrôle et de rapport d'audit. Il est à noter que NiftyISO ne dispose pas d'application de chat permettant l'échange entre les membres de l'équipe d'audit ni d'une option d'ajout et d'édition de documents ce qui constitue des limitations.

#### Smart Audit

Smart Audit<sup>4</sup> est une application web permettant de réaliser des audits et disposant de nombreuses fonctionnalités de planification d'audit, de gestion du contrôle d'accès aux fichiers par des utilisateurs autorisés, de création de listes de contrôles et bien d'autres. Smart Audit propose des prix également à la hauteur des nombreuses fonctionnalités proposées soit 239 US \$ (soit 139.600 FCFA environ) par mois pour 10 utilisateurs ce qui semble également peu adapté au contexte de jeunes entreprises camerounaises.

Tout ceci permet de situer notre solution dans les outils de productivité d'audit qui permettra de résoudre les problèmes de centralisation de documents numériques dans les bases de données et de communication évoqués plus haut et tout ceci en se servant d'outils libres et gratuits.

---

<sup>3</sup>[www.niftysol.com](http://www.niftysol.com)

<sup>4</sup>[www.smartaudit.co](http://www.smartaudit.co)

## 1.4 Problématique

Dans le domaine d'ingénierie il est question de fournir des solutions simples et innovantes dans l'optique de résoudre des problèmes rencontrés dans divers milieux. C'est pourquoi dans la tentative d'apporter une solution fonctionnelle au problème de management des ressources et des communications dans l'équipe d'auditeurs, nous allons nous servir d'approches simples et efficaces pour réaliser une plateforme qui accompagnera ces derniers dans la conduite de l'audit qui permettra:

- **La centralisation de tous les documents dans une base de données;**
- **D'effectuer des recherches sur le contenu des documents et donnant aussi la possibilité d'utiliser des documents scannés qui seront transcrits grâce à la technologie de Reconnaissance Optique des Caractères;**
- **L'édition de documents et la rédaction du rapport d'audit à travers des outils de traitement de texte;**
- **Enfin la communication entre les membres de l'équipe d'audit pour discuter des différentes analyses ou problèmes rencontrés, cela grâce à un forum de discussion sécurisé.**

C'est tout ceci qui constituera notre challenge tout au long de notre travail.

## Chapitre 2

# Méthodologie

*La méthodologie regroupe l'ensemble des méthodes scientifiques utilisées pour élaborer et proposer une solution à un problème donné. Ce chapitre débutera par une analyse qui précisera les besoins auxquels doivent répondre notre solution, puis se poursuivra sur la conception où sera présentée l'approche utilisée et enfin débouchera sur les outils choisis pour l'implémentation de notre solution.*



## 2.1 Méthodologie de développement et langage de conception

La méthode de développement décrit la suite d'activités d'ingénierie nécessaires pour transformer les besoins formulés en un produit.

### 2.1.1 Méthode de développement

Pour mener à terme notre projet nous avons adopté la méthode de développement en cascade. Nous avons choisi cette méthode car elle est simple d'utilisation et intuitive. Son principe est illustré à la figure 2.1

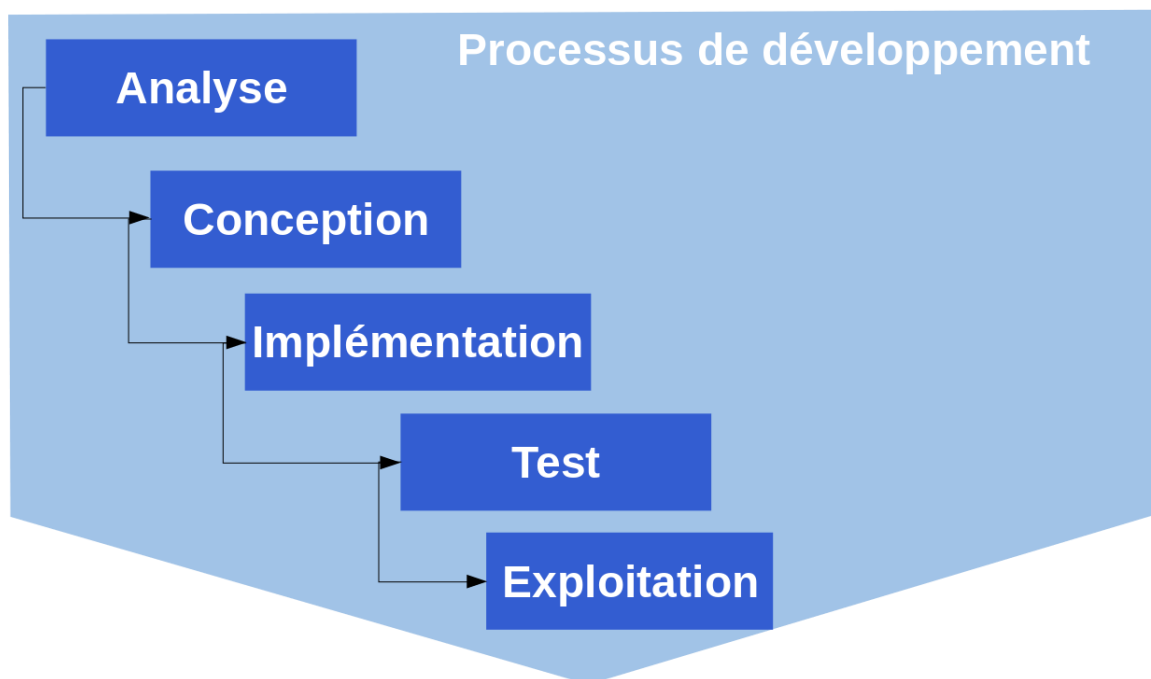


Figure 2.1: Méthode de développement en cascade

### 2.1.2 Langage de conception

Une fois la méthode de développement déterminée, nous devons choisir un langage de modélisation et nous nous sommes tourné vers l' Unified Modeling Language (UML). UML est un langage de modélisation graphique à base de pictogrammes conçu pour fournir une méthode normalisée pour visualiser la conception d'un système [5]. Les

modélisations de notre système ont été effectuées à l'aide de l'outil gratuit Draw.io <sup>1</sup> qui permet de créer des diagrammes de processus, de classes, des organigrammes, des diagrammes UML.

## 2.2 Analyse

L'analyse est un procédé dont l'objectif est de nous permettre de formaliser les étapes préliminaires du développement de notre solution qui répondent aux attentes du client. Cette phase permet d'énumérer les résultats attendus, en termes de fonctionnalités, de performance, de robustesse, de maintenance, de sécurité, d'extensibilité.

### 2.2.1 Exigences fonctionnelles

Les fonctions utiles à réaliser par le système final sont exprimées par les exigences fonctionnelles. Le système doit fournir les fonctionnalités qui suivent:

- Créer, modifier, supprimer un compte
- Créer un audit
- Importer/créer des documents texte
- Faire des recherches sur les documents
- Créer un Questionnaire de contrôle
- Créer une discussion
- Créer/exporter un rapport d'audit

### 2.2.2 Exigences non-fonctionnelles

En plus des exigences fonctionnelles listées plus haut, le système devra également bénéficier des contraintes suivantes:

- **Interface utilisateur simple et intuitive:** L'application devra présenter une interface graphique simple et qui permet une prise en main rapide pour tout nouvel utilisateur.
- **Rapidité des traitements:** Les différentes recherches effectuées devront se faire en un temps minimal ne causant aucune gêne pour l'utilisateur.

---

<sup>1</sup>[www.draw.io](http://www.draw.io)

- **Sécurité des communications:** Le Chat disponible dans l'application devra permettre un échange sécurisé entre les utilisateurs.
- **Utilisation des outils libres:** La solution devra être conçue et développée à l'aide d'outils libres de droit permettant la modification du code source.

### 2.2.3 Les cas d'utilisation

Les cas d'utilisation permettent de décrire les différents scénarios qui entrent en jeu lors de l'interaction de l'utilisateur avec le système. Pour définir les cas d'utilisation, nous commencerons par définir les acteurs intervenants et ensuite des cas d'utilisation par acteur.

#### Identification des acteurs

Le système étant conçu pour être utilisé uniquement par des auditeurs dans leur tâche d'audit de sécurité nous pouvons dès lors dire que l'acteur principal est l'auditeur de sécurité. Dans le tableau suivant figure la description des différents rôles de l'auditeur.

Table 2.1: Acteur intervenant dans le système

Acteur	Description des rôles
Auditeur	Il s'agit d'un membre de l'équipe d'auditeurs qui est capable de créer un compte pour pouvoir se connecter, importer des documents, créer un Questionnaire de Contrôle Interne qui l'aidera à réaliser sa tâche d'audit, créer un rapport d'audit final dans lequel figureront tous les commentaires et toutes les recommandations. Il est aussi capable de créer une discussion sur un sujet précis lorsqu'il rencontre un problème quelconque (lors de l'analyse des documents, ou de la rédaction du rapport etc ... ) pour pouvoir échanger avec ses différents collègues.

#### Identification des cas d'utilisation

Un cas d'utilisation représente un ensemble de séquences d'actions qui sont réalisées par le système et qui produisent un résultat observable pour un acteur. Nous récapitulons dans le tableau suivant les cas d'utilisation en fonction de l'acteur principal : l'auditeur

Table 2.2: Les différents cas d'utilisation

Acteur	Cas d'utilisation
Auditeur	<ul style="list-style-type: none"><li>• Ajouter, supprimer, modifier un compte</li><li>• Créer un audit</li><li>• Ajouter, modifier, supprimer, télécharger un document</li><li>• Créer, supprimer un questionnaire de contrôle</li><li>• Créer, supprimer une section d'un questionnaire</li><li>• Créer, modifier, supprimer, télécharger un rapport d'audit</li><li>• Créer, supprimer une discussion</li></ul>

### Diagramme des cas d'utilisation

Les diagrammes des cas d'utilisation sont des diagrammes UML utilisés pour donner une vue globale du comportement fonctionnel d'un système. À la figure 2.2 nous présentons les diagrammes des cas d'utilisation de notre système:

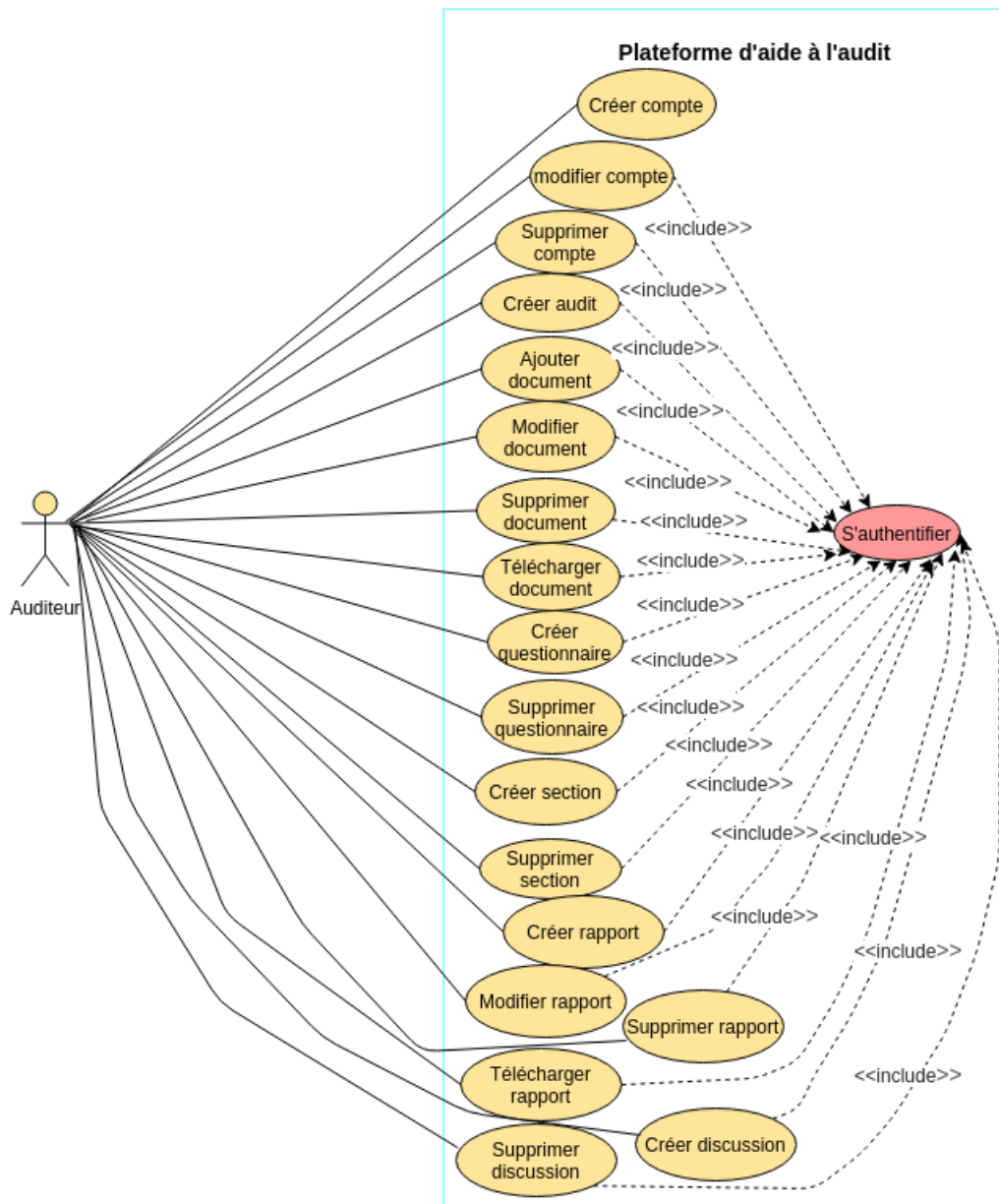


Figure 2.2: Diagramme des cas d'utilisation de la plateforme d'audit

### Description textuelle des cas d'utilisation

À présent, après avoir listé les cas d'utilisation rencontrés, nous pouvons décrire avec clarté en quoi consiste chacun de ces cas qui seront présentés dans les tableaux 2.3 à 2.23.

Table 2.3: Description textuelle du cas d'utilisation « S'authentifier »

<b>Cas d'utilisation</b>	<b>« S'authentifier »</b>
<b>Objectif</b>	Permettre à l'auditeur d'accéder à la plateforme grâce à un nom d'utilisateur et un mot de passe.
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur doit disposer d'un compte préalablement créé.
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur saisit ses informations d'authentification (nom d'utilisateur et mot de passe) et valide</li><li>2. La plateforme autorise l'accès de l'utilisateur à son compte</li></ol>

Table 2.4: Description textuelle du cas d'utilisation «Créer compte »

<b>Cas d'utilisation</b>	<b>« Créer compte »</b>
<b>Objectif</b>	Permettre à l'auditeur de créer un nouveau compte
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	–
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur crée un compte en fournissant ses informations: nom, prénom, email, nom d'utilisateur et mot de passe</li><li>2. La plateforme enregistre les informations saisies</li></ol>

Table 2.5: Description textuelle du cas d'utilisation « Modifier compte »

<b>Cas d'utilisation</b>	<b>« Modifier compte »</b>
<b>Objectif</b>	Permettre à l'auditeur de modifier son mot de passe et/ou son nom d'utilisateur
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié correctement et est connecté à la plateforme
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur saisit l'ancien mot de passe et le nouveau, ainsi que le nouveau nom d'utilisateur le cas échéant et valide</li><li>2. La plateforme enregistre les informations saisies</li></ol>

Table 2.6: Description textuelle du cas d'utilisation « Supprimer compte »

<b>Cas d'utilisation</b>	<b>« Supprimer compte »</b>
<b>Objectif</b>	Permettre à l'auditeur de supprimer son compte
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et est connecté à la plateforme
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur appuie sur le bouton de suppression du compte</li><li>2. La plateforme affiche un message lui demandant de saisir le mot de passe pour permettre la suppression</li><li>3. L'auditeur saisit son mot de passe et valide</li><li>4. La plateforme le déconnecte et supprime le compte</li></ol>

Table 2.7: Description textuelle du cas d'utilisation « Créer audit »

<b>Cas d'utilisation</b>	<b>« Créer audit »</b>
<b>Objectif</b>	Permettre à l'auditeur de créer un audit
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et est connecté à la plateforme
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur saisit les informations requises puis valide</li><li>2. La plateforme enregistre les informations</li></ol>

Table 2.8: Description textuelle du cas d'utilisation « Ajouter document »

<b>Cas d'utilisation</b>	<b>« Ajouter document »</b>
<b>Objectif</b>	Permettre à l'auditeur d'importer ou de créer un document
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et est connecté
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur saisit les informations relatives au document et valide</li><li>2. La plateforme importe/crée le fichier et l'enregistre</li></ol>

Table 2.9: Description textuelle du cas d'utilisation « Modifier document »

<b>Cas d'utilisation</b>	<b>« Modifier document »</b>
<b>Objectif</b>	Permettre à l'auditeur d'éditer le contenu d'un document
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et est connecté à la plateforme et le document doit avoir été créé préalablement
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur sélectionner le document à modifier et l'ouvre dans l'éditeur</li><li>2. Il le modifier et sauvegarde les modifications</li><li>3. La plateforme met à jour le fichier dans la base de données</li></ol>



Table 2.10: Description textuelle du cas d'utilisation « Télécharger document »

<b>Cas d'utilisation</b>	<b>« Télécharger document »</b>
<b>Objectif</b>	Permettre à l'auditeur de télécharger un document de la plateforme vers son disque de stockage local
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et le document a été préalablement créé
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur sélectionne le document à télécharger et clique sur le bouton de téléchargement</li><li>2. La plateforme enclenche le téléchargement du fichier</li></ol>

Table 2.11: Description textuelle du cas d'utilisation « Supprimer document »

<b>Cas d'utilisation</b>	<b>« Supprimer document »</b>
<b>Objectif</b>	Permettre à l'auditeur de supprimer un document
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et le document à supprimer a été préalablement créé
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur sélectionne le document à supprimer et appuie sur le bouton de suppression</li><li>2. La plateforme affiche un message de confirmation de suppression</li><li>3. L'auditeur confirme la suppression</li><li>4. La plateforme supprime le document</li></ol>

Table 2.12: Description textuelle du cas d'utilisation « Créer questionnaire »

<b>Cas d'utilisation</b>	<b>« Créer questionnaire »</b>
<b>Objectif</b>	Permettre à l'auditeur de créer un questionnaire de contrôle
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et est connecté
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur saisit les informations nécessaires à la création et valide</li><li>2. Le système enregistre les informations en créant le questionnaire</li></ol>

Table 2.13: Description textuelle du cas d'utilisation « Supprimer questionnaire »

<b>Cas d'utilisation</b>	<b>« Supprimer questionnaire »</b>
<b>Objectif</b>	Permettre à l'auditeur de supprimer un questionnaire de contrôle
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et le questionnaire en question a préalablement été créé
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur sélectionne le questionnaire à supprimer</li><li>2. La plateforme affiche un message de confirmation de suppression</li><li>3. L'auditeur confirme la suppression du questionnaire</li><li>4. La plateforme supprime le questionnaire</li></ol>

Table 2.14: Description textuelle du cas d'utilisation « Créer section »

<b>Cas d'utilisation</b>	<b>« Créer section »</b>
<b>Objectif</b>	Permettre à l'auditeur d'ajouter une section dans un questionnaire de contrôle
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et le questionnaire a été préalablement créé
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur sélectionne le questionnaire auquel il souhaite ajouter une section</li><li>2. Il appuie sur le bouton d'ajout et saisit les informations de la section et valide</li><li>3. La plateforme enregistre les informations en créant le questionnaire</li></ol>

Table 2.15: Description textuelle du cas d'utilisation « Modifier section »

<b>Cas d'utilisation</b>	<b>« Modifier section »</b>
<b>Objectif</b>	Permettre à l'auditeur de modifier le contenu de la section d'un questionnaire de contrôle
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et la section a préalablement été créée
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur sélectionne la section à éditer et clique sur le bouton d'édition</li><li>2. Il effectue toutes les modifications nécessaires et sauvegarde</li><li>3. La plateforme enregistre les modifications effectuées</li></ol>

Table 2.16: Description textuelle du cas d'utilisation « Supprimer section »

<b>Cas d'utilisation</b>	<b>« Supprimer section »</b>
<b>Objectif</b>	Permettre à l'auditeur de supprimer une section d'un questionnaire
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et la section à supprimer a préalablement été créée
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur accède au questionnaire en question</li><li>2. Il sélectionne la section et clique sur le bouton de suppression</li><li>3. La plateforme affiche un message de demande de confirmation de suppression</li><li>4. L'auditeur confirme la suppression</li><li>5. La plateforme effectue la suppression</li></ol>

Table 2.17: Description textuelle du cas d'utilisation « Créer rapport »

<b>Cas d'utilisation</b>	<b>« Créer rapport »</b>
<b>Objectif</b>	Permettre à l'auditeur de créer le rapport d'audit
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et est connecté à la plateforme
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur saisit les informations dans le formulaire de création de rapport et valide</li><li>2. La plateforme enregistre les informations et crée le rapport</li></ol>

Table 2.18: Description textuelle du cas d'utilisation « Modifier rapport »

<b>Cas d'utilisation</b>	<b>« Modifier rapport »</b>
<b>Objectif</b>	Permettre à l'auditeur d'éditer le rapport final d'audit
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et a préalablement créé le rapport
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur clique sur le bouton d'édition du rapport</li><li>2. Il effectue toutes les modifications et sauvegarde</li><li>3. La plateforme enregistre les modifications effectuées</li></ol>

Table 2.19: Description textuelle du cas d'utilisation « Supprimer rapport »

<b>Cas d'utilisation</b>	<b>« Supprimer rapport »</b>
<b>Objectif</b>	Permettre à l'auditeur de supprimer un rapport d'audit
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et a préalablement créé le rapport
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur clique sur le bouton de suppression</li><li>2. La plateforme affiche un message de demande de confirmation de suppression</li><li>3. L'auditeur confirme la suppression</li><li>4. La plateforme effectue la suppression du rapport</li></ol>

Table 2.20: Description textuelle du cas d'utilisation « Télécharger rapport »

<b>Cas d'utilisation</b>	<b>« Télécharger rapport »</b>
<b>Objectif</b>	Permettre à l'auditeur de télécharger le rapport d'audit sur son disque de stockage local
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et a préalablement créé le rapport d'audit
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur clique sur le bouton de téléchargement du rapport</li><li>2. La plateforme enclenche le téléchargement du rapport</li></ol>

Table 2.21: Description textuelle du cas d'utilisation « Créer discussion »

<b>Cas d'utilisation</b>	<b>« Créer discussion »</b>
<b>Objectif</b>	Permettre à un auditeur de créer une discussion de groupe sur un sujet précis
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et est connecté à la plateforme
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur saisit les informations (nom et description de la discussion) nécessaires à la création de la discussion et valide</li><li>2. La plateforme enregistre les informations</li></ol>

Table 2.22: Description textuelle du cas d'utilisation « Supprimer discussion »

<b>Cas d'utilisation</b>	<b>« Supprimer discussion »</b>
<b>Objectif</b>	Permettre à l'auditeur de supprimer une discussion
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié et la discussion a préalablement été créée
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur sélectionne la discussion à supprimer et clique sur le bouton de suppression</li><li>2. La plateforme affiche un message de confirmation de suppression</li><li>3. L'auditeur confirme la suppression</li><li>4. La plateforme supprime la discussion</li></ol>

Table 2.23: Description textuelle du cas d'utilisation « Faire des recherches »

<b>Cas d'utilisation</b>	<b>« Faire des recherches »</b>
<b>Objectif</b>	Permettre à l'auditeur de faire des recherches par nom, contenu sur les documents, questionnaires
<b>Acteur concerné</b>	Auditeur
<b>Précondition</b>	L'auditeur s'est authentifié
<b>Scénario nominal</b>	<ol style="list-style-type: none"><li>1. L'auditeur saisit le mot clé dans la barre de recherche</li><li>2. L'auditeur sélectionne l'option de recherche par nom ou contenu et valide</li><li>3. La plateforme effectue une recherche et affiche la liste des documents/questionnaires/sections correspondant(e)s</li></ol>

## 2.2.4 Modèle d'analyse du domaine

Le modèle d'analyse du domaine permet l'élaboration du diagramme de classes. Il permet de définir les classes qui modélisent les entités ou concepts présents dans le

domaine de l'application. On le dégage à partir des exigences fonctionnelles et des cas d'utilisation. Le diagramme de classes est le suivant :



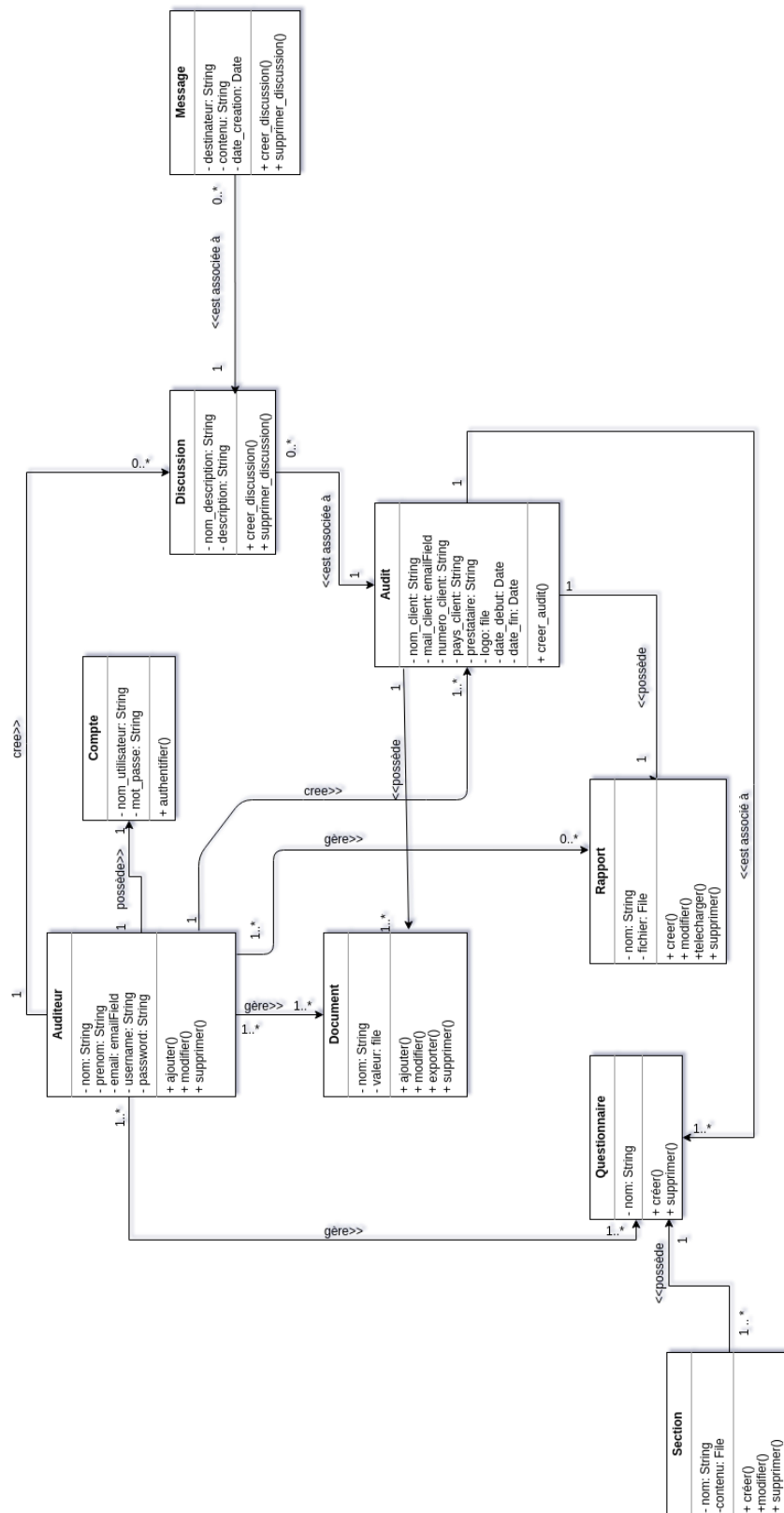


Figure 2.3: Diagramme de classe d'analyse de la plateforme

## 2.3 Conception

Dans cette section nous présenterons la conception des interfaces utilisateur de notre application ensuite l'architecture de notre solution et enfin l'aspect sécurité de la plateforme

### 2.3.1 Conception des interfaces

Afin de faciliter la phase d'implémentation nous avons choisi de concevoir les interfaces de notre application et leur logique (lien entre les pages) grâce à l'outil gratuit et open source Pencil<sup>2</sup> qui permet de créer des maquettes de site web sur des plateformes de bureau populaires.

Nous présenterons quelques pages (les autres pages sont présentées en annexe) permettant de mettre en relief l'aspect graphique général désiré. Nous avons par exemple la page d'accueil à la figure 2.4 qui permet de voir le choix effectué quant à la présence d'un menu à gauche qui permet un accès rapide à toutes les fonctionnalités.

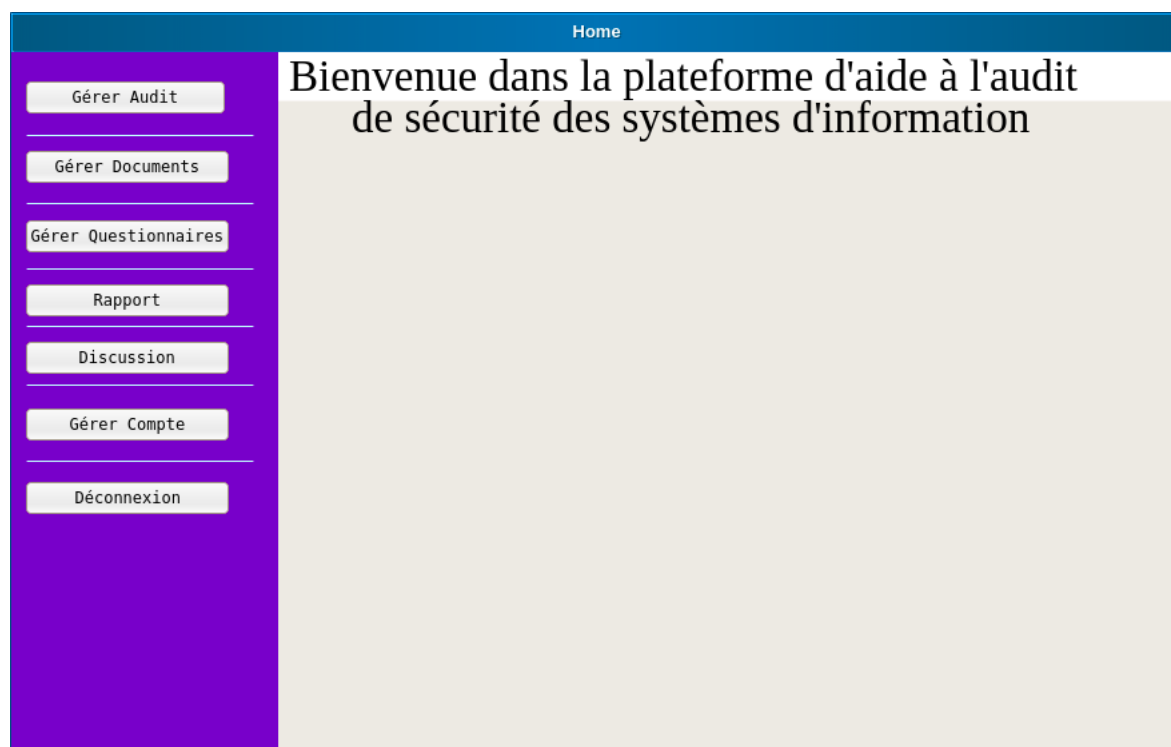


Figure 2.4: Page d'accueil

Ensuite nous avons la page qui permet la création d'un audit (figure 2.5)

---

<sup>2</sup>pencil.evolus.vn

The screenshot shows a web application interface for creating an audit. It features a blue header bar with the text 'Home'. On the left, there is a purple sidebar containing several buttons: 'Gérer Audit', 'Gérer Documents', 'Gérer Questionnaires', 'Rapport', 'Discussion', 'Gérer Compte', and 'Déconnexion'. The main content area is divided into two columns. The left column is titled 'Créer Audit' and contains a form with the following fields: 'Nom du client:', 'Mail du client:', 'Numéro de téléphone du client:', 'Pays du client:', 'Prestataire', 'Logo entreprise:', 'Date de début:', and 'Date de fin:'. Each field has a corresponding text input box. At the bottom of this column is a 'Créer' button. The right column is titled 'Gérer Audit' and contains the heading 'Informations relatives à l'audit' followed by the same set of labels as the left column, but without input boxes.

Figure 2.5: Création d'un audit

Tout ceci nous guidera donc dans la phase d'implémentation.

## 2.3.2 Architecture de la solution

### Architecture physique

Pour notre solution nous avons fait le choix d'une architecture Client-Serveur qui permettra une utilisation simple et aisée. L'architecture physique est présentée à la figure 2.6

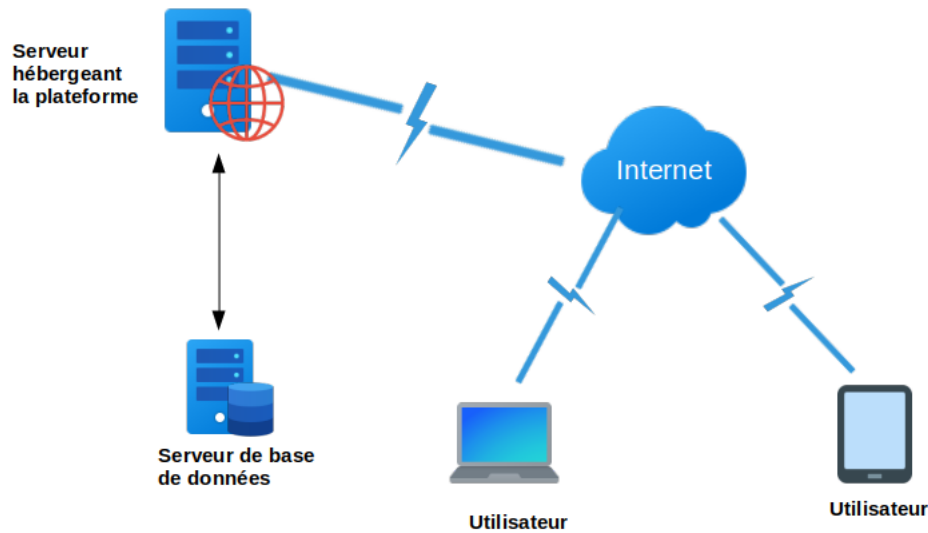


Figure 2.6: Architecture physique de la solution

Une fois l'architecture physique définie nous pouvons passer à l'architecture logicielle.

### Architecture MVT

L'architecture MVT (Modèle Vue Template) est un modèle de conception logicielle utilisé pour développer des applications web. Cette architecture se compose des parties suivantes:

- **Le modèle:** Il représente la structure de l'objet dans la base de donnée.
- **La vue:** C'est l'interface utilisateur c'est-à-dire ce que l'on voit dans le navigateur lorsque le site web est affiché.
- **Les templates:** Ce sont des fichiers HTML qui peuvent recevoir des objets du langage de programmation utilisé (objets python par exemple) et qui sont liés à des vues.

Elle est illustré à la figure 2.7



Figure 2.7: Architecture MVT

### 2.3.3 Sécurité

La solution doit être sécurisée étant donné la nature de l'activité pour laquelle elle est utilisée notamment l'audit de sécurité qui met un point d'honneur sur la confidentialité des données du client. Les mesures de sécurité adoptées seront:

- **L'utilisation du protocole https :** Il permettra le transfert sécurisé des informations chiffrées.
- **Le chiffrement des mots de passe dans la base de donnée:** Les mots de passe des utilisateurs ne doivent pas apparaître en clair dans la base de données.
- **La protection contre la faille XSS (cross-site scripting):** Ceci préviendra contre l'injection de code HTML contenant des scripts Javascript malveillants qui peuvent être exécutés par des utilisateurs dans leur navigateur.
- **La protection contre les attaques CSRF (Cross Site Request Forgery):** Cette protection préviendra contre la possibilité pour un utilisateur malveillant d'exécuter des actions en utilisant les informations d'identification d'un autre utilisateur à son insu ou sans son consentement.
- **La protection contre les injections SQL (Structured Query Language) :** Cette protection permettra d'éviter à un utilisateur malveillant d'exécuter du code SQL arbitraire sur une base de données pouvant entraîner par exemple la suppression d'enregistrements ou une fuite de données.

## 2.4 Choix des outils d'implémentation

### 2.4.1 Outils de développement

Les codes sources de notre application ont été produits grâce au logiciel Sublime Text qui est un éditeur de texte générique codé en C++ et Python, disponible sur Windows, Mac et Linux.

### 2.4.2 Langages de programmation

#### Langages utilisés Côté client

L'interface utilisateur a été réalisée grâce à des langages populaires et bénéficiant d'une grande communauté de développeurs qui participent à leur maintenance et leur évolution ce qui donne accès à une bonne documentation. Nous avons notamment:

- **HTML5 (HyperText Markup Language 5):** il s'agit en fait d'un langage de description développé pour représenter et structurer les pages et les documents sur le Web. Il fournit la structure de base des sites, qui est améliorée et modifiée par d'autres technologies comme CSS et JavaScript.
- **CSS3 (feuilles de style en cascade):** utilisé pour contrôler la présentation, le formatage et la mise en page des pages Web. Si HTML est la cloison sèche, CSS est la peinture.
- **JavaScript:** langage de script, principalement utilisé pour rendre les pages web dynamiques. En bref, JavaScript est un langage de programmation qui permet aux développeurs web de concevoir des sites interactifs.

#### Langage utilisé Côté serveur

- **Python:** C'est un langage de programmation interprété, de haut niveau et à usage général. Créé par Guido van Rossum et publiée pour la première fois en 1991, la philosophie de conception de Python met l'accent sur la lisibilité du code.

### 2.4.3 Frameworks et bibliothèques utilisés

L'utilisation de frameworks et de bibliothèques présente de nombreux avantages comme un temps de développement plus court, un code homogène et maintenable. Cela facilite la réutilisation du code. Nous avons utilisé les frameworks et bibliothèques suivants pour notre travail

### Bibliothèques Côté client

- **jQuery:** C'est une bibliothèque JavaScript open source qui simplifie la création d'applications Web. Plus précisément, jQuery simplifie la manipulation du DOM (Document Object Model) HTML, JavaScript et la gestion des événements.
- **Bootstrap :** C'est un framework CSS gratuit et open-source réactif destiné au développement Web côté client. Il contient des modèles de conception basés sur CSS et JavaScript pour la typographie, les formulaires, les boutons, la navigation et d'autres composants d'interface.
- **TinyMCE:** C'est un éditeur de texte rtf (rich-text format) en ligne publié sous forme de logiciel open source sous license LGPL (Lesser General Public License). Il a la capacité de convertir des champs HTML textarea ou d'autres éléments HTML en instances d'éditeur. Il fournit différentes options d'éditations telles que présentes dans des éditeurs de documents à l'instar de Microsoft Word.

### Frameworks Côté serveur

- **Django:** Django est un framework Web Python de haut niveau qui permet un développement rapide. Conçu par des développeurs expérimentés, il prend en charge une grande partie des tracas du développement Web, on peut donc se concentrer sur l'écriture de l'application sans avoir à implémenter certaines fonctionnalités importantes. C'est un framework gratuit et open source; il est réputé pour permettre le développement d'application sécurisée car il intègre différentes fonctionnalités de sécurité permettant d'éviter les attaques XSS, l'injection SQL, les attaques CSRF et bien d'autres.
- **OCR Space:** Ce n'est pas un framework mais une API qui fournit une façon simple d'effectuer la reconnaissance optique de caractères dans plusieurs langues à partir d'images ou de documents PDF. Et le texte extrait est renvoyé sous au format JSON.

## Chapitre 3

### Résultats et discussions

*Dans ce chapitre nous présenterons comment nous déploierons notre solution en situation réelle puis les résultats obtenus sous forme de capture d'écran et enfin commenterons notre solution.*



## 3.1 Déploiement

À présent que nous avons effectué la conception et l'implémentation de notre solution, nous pouvons passer à son déploiement pour permettre son utilisation. Notre application Web est destinée à fonctionner dans un environnement client-serveur. La figure 3.1 montre comment les composants du système sont liés entre eux. L'application Web est empaquetée dans un conteneur docker afin de garantir l'évolutivité. La base de données est également configurée sur le serveur pour stocker les documents, messages et autres informations nécessaires.

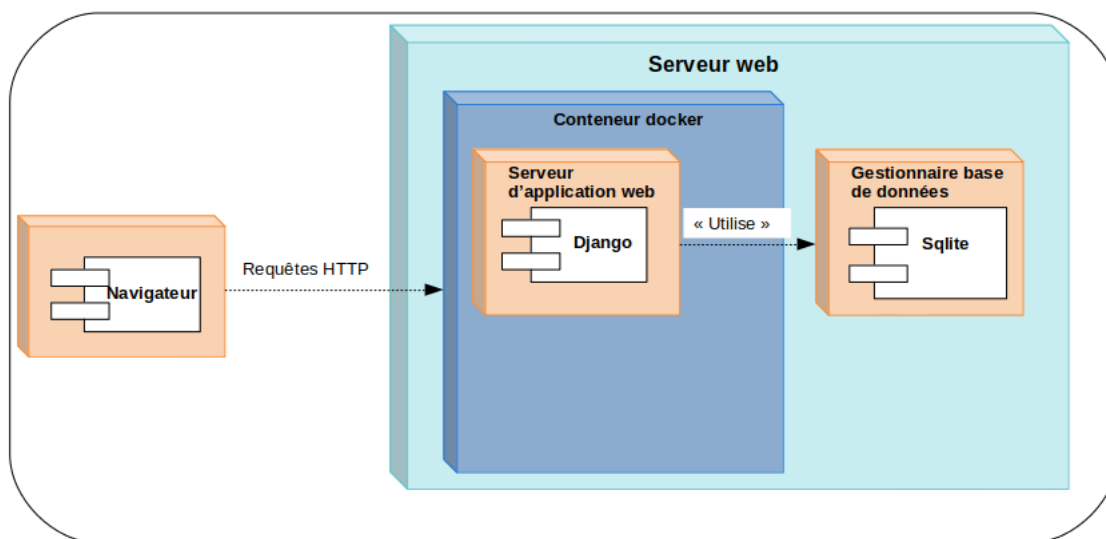


Figure 3.1: Diagramme de déploiement

## 3.2 Résultats

### 3.2.1 Connexion

La figure 3.2 présente l'interface de connexion permettant d'accéder à l'application. L'auditeur doit juste saisir ses identifiants de connexion et valider.

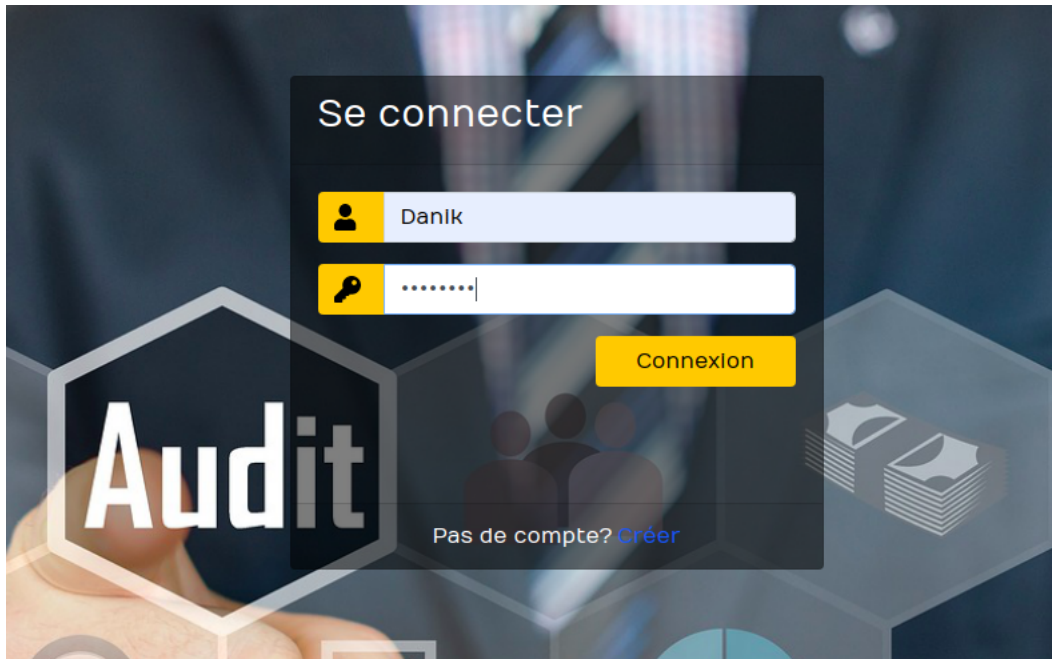


Figure 3.2: Page de connexion de l'application

### 3.2.2 Page d'accueil

L'auditeur dispose d'une page d'accueil lui présentant l'application ce qui permettra une prise en main plus rapide comme on peut le voir à la figure 3.3



Figure 3.3: Page d'accueil de l'application

### 3.2.3 Gestion des documents

Puis nous avons les différentes pages qui permettent de créer ou importer un document (figure 3.4), de faire des recherches suivant divers filtres sur les documents, d'effectuer d'autres actions telles que le téléchargement et la suppression (figure 3.5) et enfin de modifier le document que l'on désire (figure 3.6)

Ajouter un document

Sélectionner l'audit Client: High-Tech Center Polytechnique Période: June 26, 2020

Nom du document

Document : Choose file No file chosen

Enregistrer

Figure 3.4: Ajout d'un document

Recherche de documents

Sélectionner l'audit Client: High-Tech Center Polytechnique Période: June 26, 2020

Filtre : Nom

Liste des documents

Show 10 entries Search:

Nom	Action	Action	Action
Configurations réseau	Ouvrir	Télécharger	Supprimer
Politique de Sécurité du Système d'Information	Ouvrir	Télécharger	Supprimer
Procédures de contrôle	Ouvrir	Télécharger	Supprimer

Figure 3.5: Recherche, téléchargement, suppression d'un document

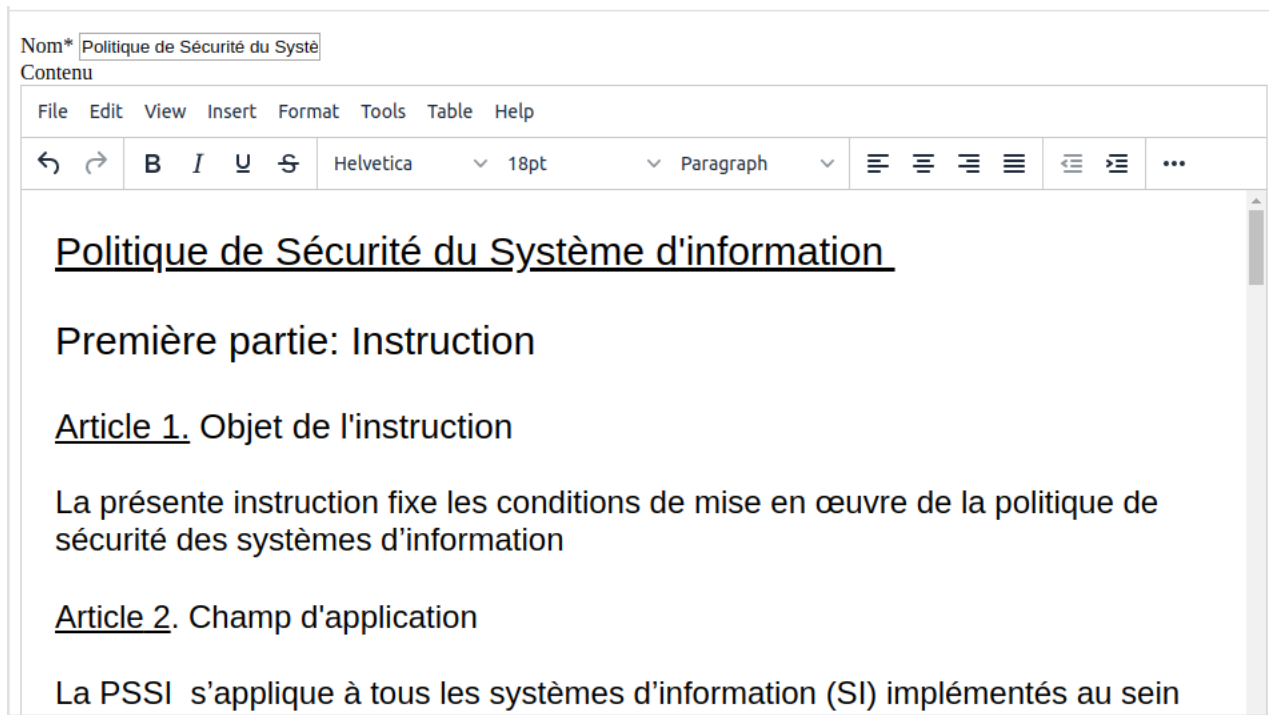


Figure 3.6: Modification d'un document

### 3.2.4 Gestion des questionnaires de contrôle

L'auditeur dispose d'une interface pour créer un questionnaire (figure 3.7), créer des sections dans ce questionnaire, faire des recherches (figure 3.8) et éditer ces sections (figure 3.9)

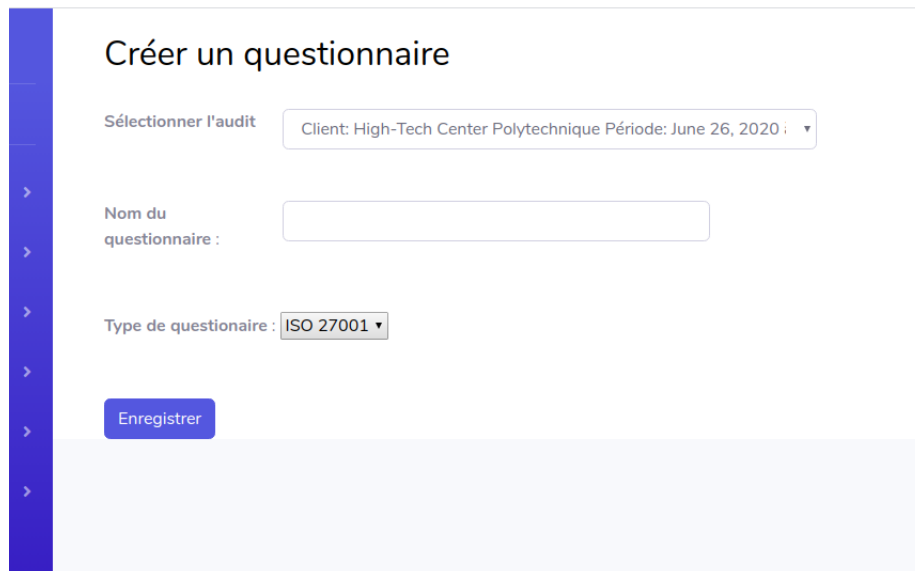


Figure 3.7: Création d'un questionnaire de contrôle

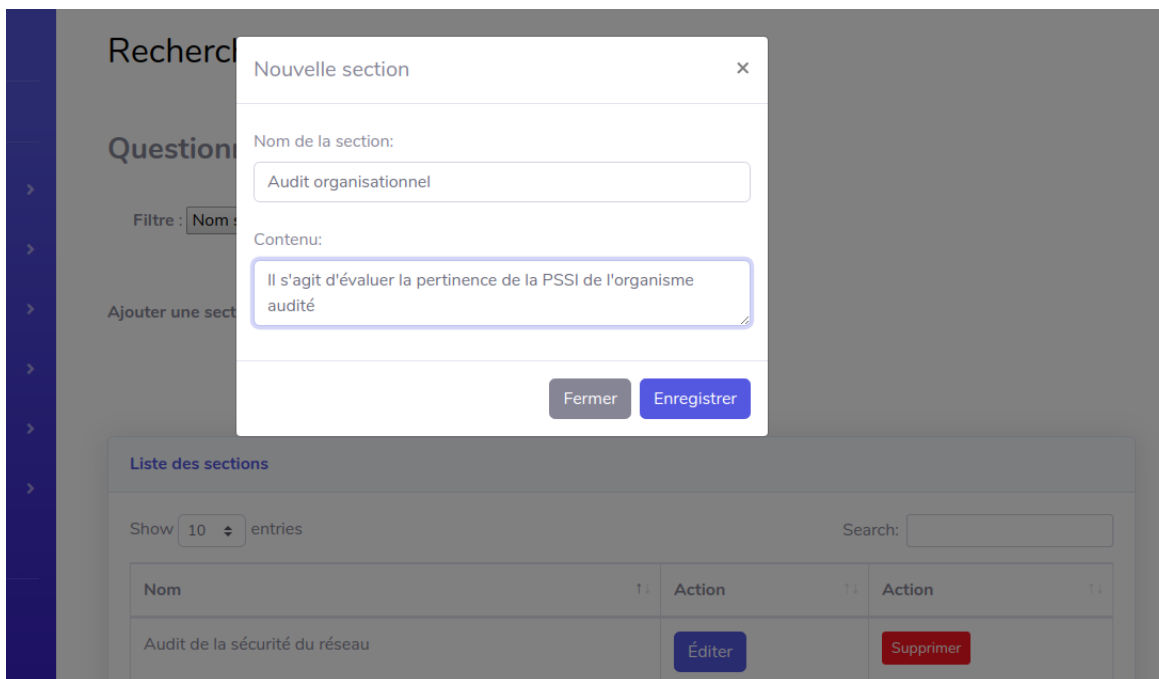


Figure 3.8: Création, recherche, suppression de sections

# RÉALISATION D'UNE PLATEFORME D'AIDE AUX AUDITEURS DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Nom de la section\*

Contenu

File Edit View Insert Format Tools Table Help

↶ ↷

**B** *I* U ~~S~~

Helvetica ▾ 14px ▾ Paragraph ▾

≡ ≡ ≡ ≡

≡ ≡

...

Questions	Réponses et remarques
Existe-t-il des pare-feu sur toutes les connexions Internet ou Extranet ?	
Les pare-feu sont-ils utilisés en interne pour séparer l'accès aux réseaux ayant des niveaux de sécurité différents?	
L'utilisation de NAT ou PAT est-elle implémentée dans votre environnement pour masquer le réseau interne d'Internet?	
Votre pare-feu et votre routeur sont-ils configurés pour se conformer aux normes de sécurité documentées?	

Figure 3.9: Modification d'une section

## 3.2.5 Gestion du rapport d'audit

Également, l'auditeur peut créer un rapport d'audit (figure 3.10) et en modifie son contenu grâce à un outil d'édition riche (TinyMCE, que nous avons intégré à notre logiciel et présenté dans la section Frameworks et bibliothèques utilisées) proposant de nombreuses fonctionnalités tout comme pour la modification du contenu des documents et des sections.

Figure 3.10: Création du rapport final d'audit

### 3.2.6 Gestion des discussions

Enfin nous avons une application de chat permettant aux membres de l'équipe d'audit de partager leurs différentes remarques et de discuter sur des problèmes éventuels. La figure 3.11 présente l'interface de création de la discussion, la figure 3.12 présente le chat du côté de l'utilisateur nommé *Danik* et la figure 3.13 du côté de l'utilisateur nommé *Ondoua*.



Créer une discussion de groupe

Sélectionner l'audit Client: High-Tech Center Polytechnique Période: June 26, 2020

Nom de la discussion Architecture réseau

Description Les documents d'architecture du réseau sont incomplets

Créer

Figure 3.11: Création d'une discussion de groupe



Figure 3.12: Discussion (côté Danik)

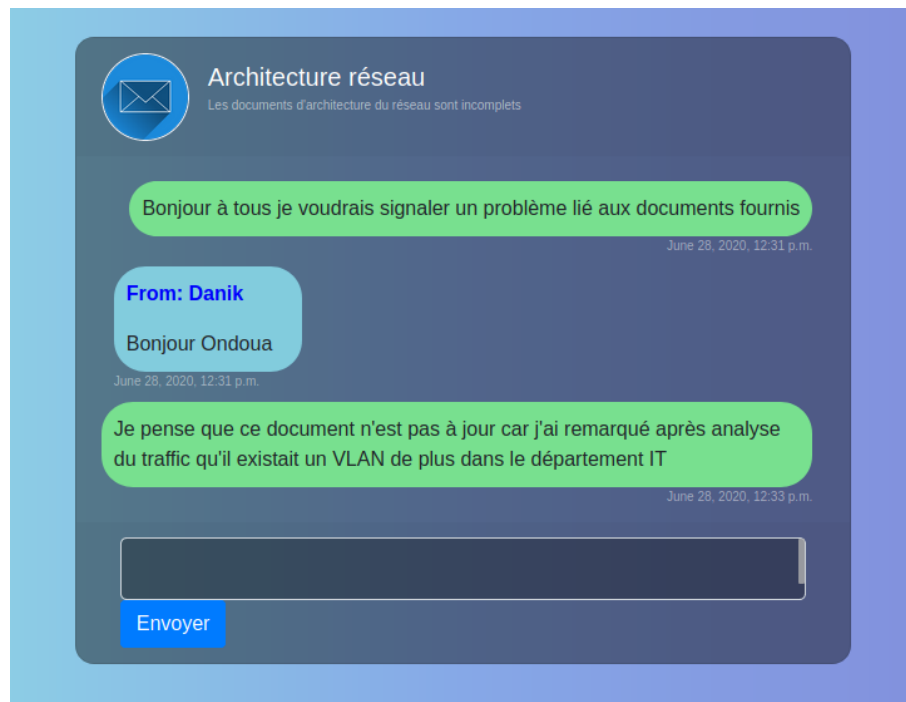


Figure 3.13: Discussion (côté Ondoua)

### 3.3 Apport de la solution

Notre solution apporte un gain significatif en terme d'efficacité car les différents membres de l'équipe d'audit ont accès en tout lieu (grâce à un ordinateur, une tablette ou un smartphone) aux différents documents leur permettant de mener à bien la phase de réalisation de l'audit sous la simple condition de disposer d'une connexion à Internet. De plus la possibilité de faire des recherches pour retrouver rapidement un questionnaire (et même la section qui les intéresse) et y noter directement les réponses et les observations faites lors de la conduite de l'audit. De plus les différents membres de l'équipe d'audit ont la possibilité de signaler directement un problème et d'en discuter (à travers une application de chat sécurisé) leur permet d'avancer rapidement dans leur tâche d'audit.

# Conclusion générale et perspectives

## Conclusion générale

Afin d'accompagner l'auditeur de la planification à la rédaction du rapport final d'audit, nous avons conçu et réalisé une plateforme mettant à sa disposition divers outils facilitant son travail d'analyse des documents et garantissant l'accessibilité à ces documents en plus de permettre les communications entre membres de l'équipe d'auditeurs. Spécifiquement, la solution proposée:

- permet la centralisation des différentes données et documents nécessaires à la planification, la conduite et la clôture de l'audit permettant un accès en tout lieu sous la simple condition de disposer d'un accès à Internet;
- permet la mise à disposition d'outils de recherches bénéficiant de différentes options ce qui permet à l'auditeur de récupérer le document qu'il désire;
- intègre un outil disposant de nombreuses fonctionnalités permettant de modifier les documents directement sur la plateforme;
- dispose d'un forum de discussion permettant aux membres de l'équipe d'audit de partager leurs différentes analyses et de faire part d'éventuels problèmes rencontrés lors de la conduite d'audit.

## Perspectives

Aucune solution n'étant parfaite, la nôtre présente certains manquements:

- Les documents créés ou importés ne sont que des documents textes et images (contenant du texte) or l'on pourrait disposer d'enregistrements audio;
- Les questionnaires et rapports d'audit présentant en général une structure assez répétitives d'un document à l'autre doivent être rédigés intégralement par l'auditeur;

- La plateforme présente quelques limites pour les utilisateurs de tablettes ou de smartphones car il leur est contraignant de passer le navigateur pour se connecter et se déconnecter.

Au regard des différentes insuffisances sus-citées les perspectives suivantes sont envisageables:

- L'intégration d'un module de transcription vocale permettant d'intégrer l'utilisation de fichiers audio qui seront transcrits texte pour être édités éventuellement;
- L'intégration d'un module permettant de dessiner des diagrammes et des organigrammes;
- L'intégration de différents templates contenant la structure générale d'un questionnaire de contrôle ou d'un rapport d'audit;
- Le développement d'une application mobile Android ou iOS pour rendre plus agréable l'utilisation de la plateforme sur smartphones et tablettes.

## Références Bibliographiques

- [1] De Courcy R.(1992), Les systèmes d'information en réadaptation, Québec, Réseau international CIDIH et facteurs environnementaux, no 5 vol. 1-2 p. 7-10.
- [2] Administration de la défense nationale du Maroc, «Guide d'Audit de la Sécurité des Systèmes d'Information» [en ligne]. Available: [https://www.dgssi.gov.ma/sites/default/files/attached\\_files/guide\\_audit\\_v30-12-2015.pdf](https://www.dgssi.gov.ma/sites/default/files/attached_files/guide_audit_v30-12-2015.pdf). [Accès le 23 avril 2020, 13h02].
- [3] Bristish Standard Institution, «Guidelines for auditing management systems (ISO 19011:2011),» [En ligne]. Available: [https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030257143&awc=3911\\_1593790110\\_c0ec4bc1be36721df3988e71a9647d09](https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030257143&awc=3911_1593790110_c0ec4bc1be36721df3988e71a9647d09). [Accès le 01 avril 2020, 13h20].
- [4] Angel R. Otero(2019) . Tools and Techniques Used in auditing IT. Dans : *Information Technology Control and Audit* Angel R. Otero. Taylor & Francis Group publications, 6000 Broken Sound Parkway NW, Suite 300. Chap. 4, pp. 97-101.
- [5] Wikipedia, «Définition de UML,» [En ligne]. Available: [https://fr.wikipedia.org/wiki/UML\\_\(informatique\)](https://fr.wikipedia.org/wiki/UML_(informatique)). [Accès le 27 Juin 2020, 12h05].
- [6] YENDE RAPHAEL Grevisse, «SUPPORT DE COURS DE L'AUDIT DES SYSTÈMES D'INFORMATION» [en ligne]. Available: <https://hal.archives-ouvertes.fr/cel-01964389/document>. [Accès le 01 Mai 2020, 12h30].
- [7] Haes, S.D.; Grembergen, W.V. (2015). COBIT as a Framework for Enterprise Governance of IT. Dans : *Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5 (2nd ed.)*. Springer. Chap. 5, pp. 103–128.
- [8] ITIL, «ITIL,» [En ligne]. Available: <https://www.itlibrary.org/>. [Accès le 04 Juillet 2020, 12h10].
- [9] ANSSI(2010), EBIOS, Expression des Besoins et Identification des Objectifs de Sécurité, Paris, ANSSI.

- [10] Wikipedia, «MEHARI,» [En ligne]. Available: <https://en.wikipedia.org/wiki/MEHARI>. [Accès le 04 Juillet 2020, 12h25].
- [11] Cio-wiki, «OCTAVE,» [En ligne]. Available: [https://cio-wiki.org/wiki/OCTAVE\\_\(Operationally\\_Critical\\_Threat\\_Asset\\_and\\_Vulnerability\\_Evaluation\)](https://cio-wiki.org/wiki/OCTAVE_(Operationally_Critical_Threat_Asset_and_Vulnerability_Evaluation)). [Accès le 04 Juillet 2020, 12h20].
- [12] ISO, «ISO / IEC 27001,» [En ligne]. Available: <https://www.iso.org/isoiec-27001-information-security.html>. [Accès le 04 Juillet 2020, 12h07].
- [13] Francelle CHISSEU, *Rapport de stage: Service de réseau d'accès filaire.*, Stage d'imprégnation, Juin-Août 2018.

## Annexe A

### Annexe: Interfaces de la maquette de l'application

Cette partie regroupe les interfaces (de la maquette de la plateforme) dessinées lors de la phase de conception.

La maquette de la page de création de compte (Sign Up) est présentée. Elle est encadrée par une barre de navigation bleue en haut à gauche avec le lien "Log In". Le formulaire principal est centré sur un fond gris clair. Le titre "Sign Up" est en bleu. Les champs de saisie sont : "First Name", "Last Name", "email", "Position", "Speciality", "Username" (précedé d'une icône d'utilisateur) et "Password" (précedé d'une icône de cadenas). Un bouton "create" est situé en bas à droite du formulaire. En bas à gauche, il y a le lien "Already have an account ?" suivi du lien "Sign in" en bleu.

Figure A.1: Page de création du compte

La page de création de compte permet de créer ses accès en renseignant les champs Nom, Prénom etc. Ce sont les noms d'utilisateur et le mot de passe qui constituent les identifiants de connexion.

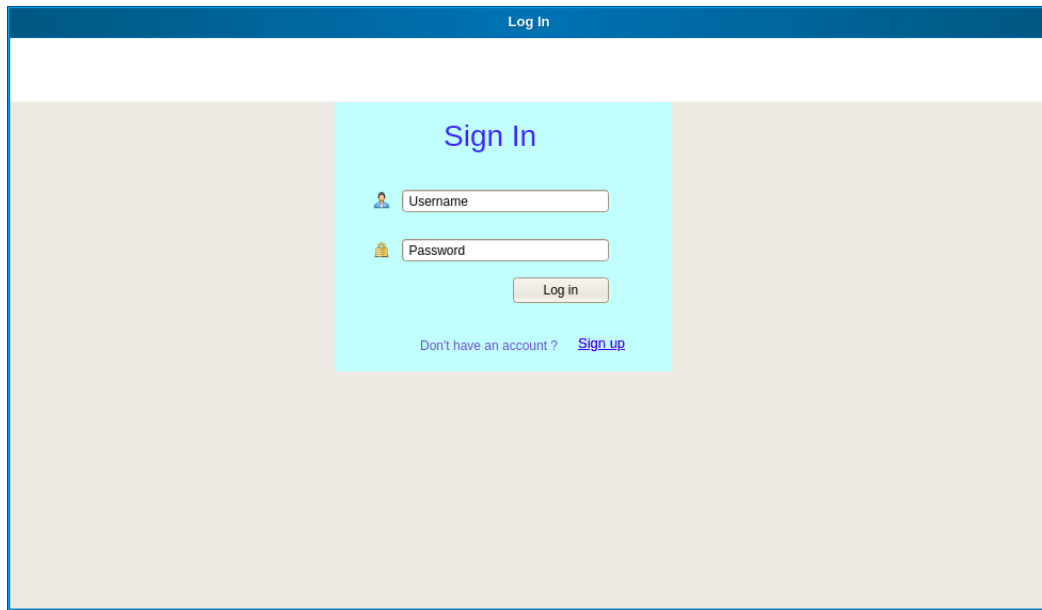


Figure A.2: Page de connexion

Ici nous avons la page de connexion où il suffit de saisir ses identifiants pour accéder à la plateforme.

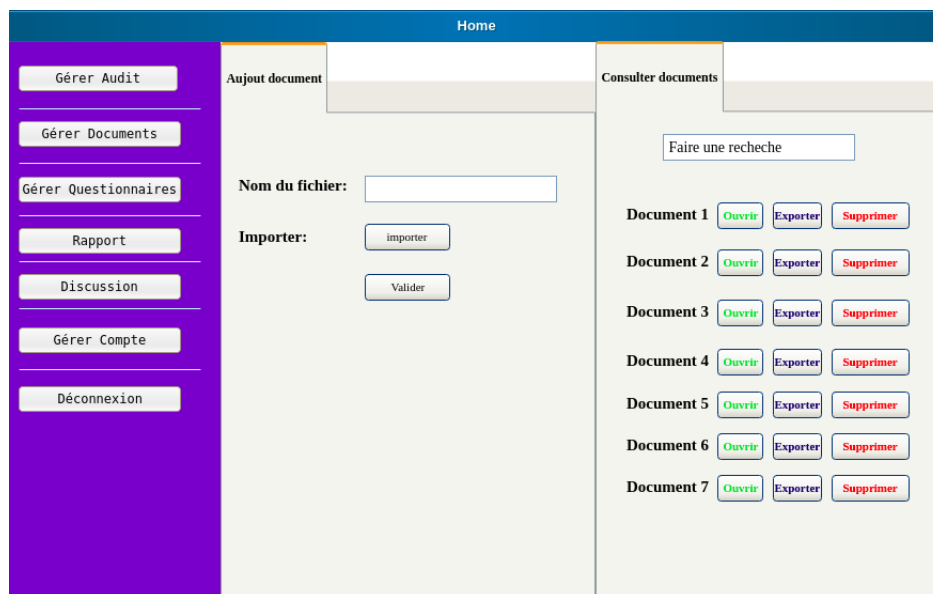


Figure A.3: Page de gestion des documents

Nous avons à présent la page qui nous permet de créer un document, de l'ouvrir, de le télécharger ou de le supprimer.



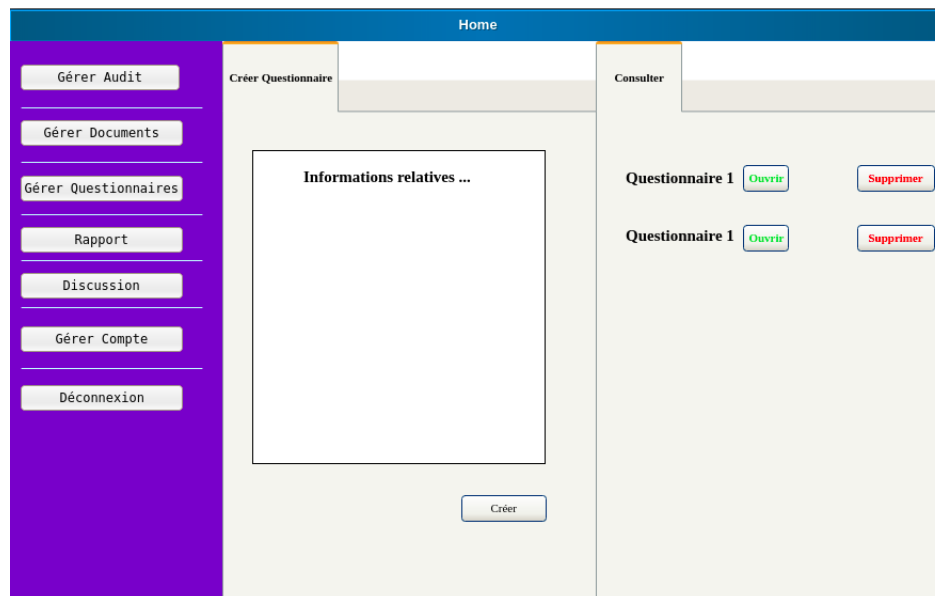


Figure A.4: Page de gestion des questionnaires

Ici l'on crée des questionnaires de contrôle (en saisissant son nom) et on a également la possibilité d'en supprimer.

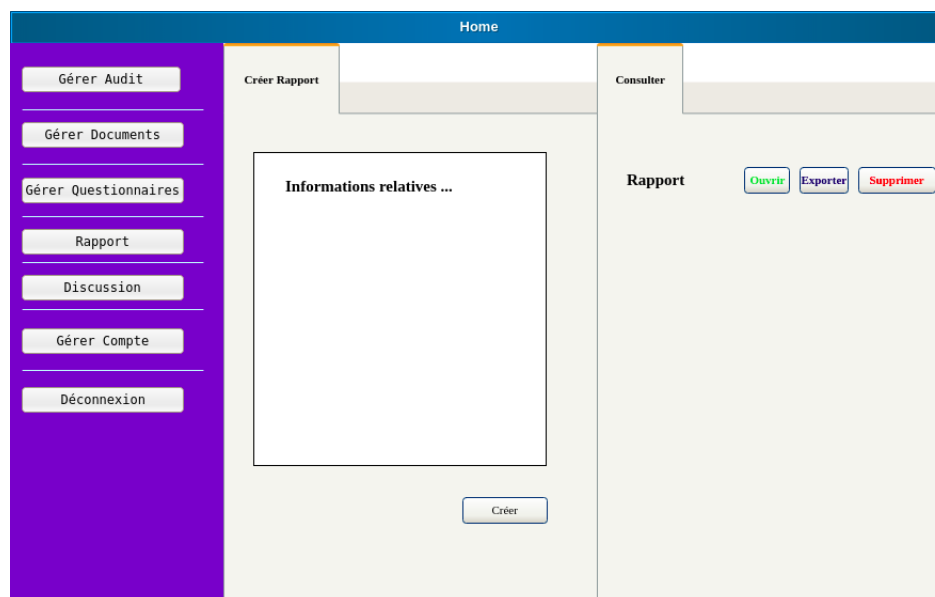


Figure A.5: Page de gestion du rapport d'audit

Ici est présenté la page de gestion du rapport audit où l'on ne peut créer qu'un seul rapport (en saisissant son nom), l'éditer et le supprimer.

The screenshot shows a web application interface with a blue header bar labeled 'Home'. On the left is a purple sidebar with buttons: 'Gérer Audit', 'Gérer Documents', 'Gérer Questionnaires', 'Rapport', 'Discussion', 'Gérer Compte', and 'Déconnexion'. The main content area is divided into two panels. The left panel, titled 'Créer discussion', contains two text input fields labeled 'Nom de la discussion' and 'Description de la discussion', followed by a 'Créer' button. The right panel, titled 'Consulter discussions', displays a list of two discussions. 'Discussion 1' and 'Discussion 2' each have two buttons: a green 'Ouvrir' button and a red 'Supprimer' button.

Figure A.6: Page de création de discussions

Il suffit de saisir le nom de la discussion et sa description puis elle apparaîtra dans la liste et l'utilisateur pourra y accéder.

The screenshot shows the 'Modifier' page of the application. The layout is consistent with the previous page, featuring the same blue header and purple sidebar. The main content area has two panels. The left panel, titled 'Modifier', contains several text input fields for user information: 'First Name', 'Last Name', 'email', 'Position', 'Speciality', 'Username' (preceded by a user icon), 'Previous Password' (preceded by a key icon), and 'New Password' (preceded by a key icon). Below these fields is an 'Enregistrer' button. The right panel, titled 'Consulter compte', contains a large rectangular box labeled 'Informations relatives ...' and a red 'Supprimer compte' button at the bottom.

Figure A.7: Page de modification de compte

On donne la possibilité à l'utilisateur de modifier ses identifiants de connexion et de supprimer son compte.