

“Live as if you were to die tomorrow. Learn as if you were to live forever.”

— **Mahatma Gandhi**

General Introduction:

The information system is today an integral part of businesses and public institutions. Responsible for the continuity of the activity of the company, any tort committed can lead to significant risks essentially aimed at paralyzing the company's Information System or altering confidential data.

As a result, a security audit consists in validating the means of protection implemented on the organizational, procedural and technical levels, with regard to the security policy by calling on a trusted third party expert in IT security audit. The security audit leads, beyond the observation, to analyze the operational risks and to propose recommendations and action plans quantified and prioritized to correct the vulnerabilities and reduce the exposure to the risks.

The National Computer Security Agency ANSI, which is responsible for managing the activity of auditors of Information System security, wishes to create a means to supervise the workflow of auditors.

It is in this context that our end-of-studies project is integrated, which aims to set up a solution to automate the process of filing an application for the certificate to exercise the activity of expert auditor in the field of computer security and offer the ANSI team a tool to supervise this process.

This report is a synthesis of the work carried out within ANSI and is organized into four chapters. The first chapter will be devoted to the presentation of the host organization and the state of the art. The second chapter will be reserved for the Specification of needs and the design to analyze the functional and non-functional needs and to detail the architectural design. The third chapter will be dedicated to carrying out the work to present the tools used to accomplish this work and will describe with screenshots the work developed. Finally, we will end with a concluding chapter.

TABLE OF CONTENTS

Contents

DEDICATION.....	2
Acknowledgements.....	3
General Introduction:.....	5
TABLE OF CONTENTS.....	6
Chapter 1 : State OF THE ART.....	8
1. Introduction :.....	9
2. Presentation of ANSI :.....	9
2.1 ANSI Objectives :.....	9
2.2 Organization of ANSI :.....	10
Figure 1 : ANSI organization chart	10
3. State of the art :	11
3.1 Project Presentation :.....	11
Chapter 2 : Requirements Analysis.....	12
1. Introduction :.....	13
2. Study of the existing :.....	13
3. Application Requirements :	13
3.1 Functional Requirements :	13
3.2 Non-Functional Requirements :	13
4. Use case diagram :.....	14
4.1 Global use case	14
4.2 Authentification Use Case	15

Chapter 1 : State OF THE ART

1. Introduction :

In this introductory chapter, first, there is a contextualization of the project, a specification of the framework for its elaboration, and a presentation of the host organization in which the internship related to this project is done. Second, there is a description of the project framework and the development of a comparative study of existing solutions.

Finally, there is a presentation of a new suggested solution and which methodology to follow for this solution.

2. Presentation of ANSI :

The National Computer Security Agency is a public institution which was created in 2004 and operates under the supervision of the Ministry of Communication Technologies and Digital Economy. It ensures the implementation of strategic national guidelines for the security of information systems and networks. The agency provides several national services by offering technical solutions of a directional and indicative nature (specifications, technical advice, awareness-raising ...), emergency services (management of cyber incidents according to security law) as well as participation in the study of large and sensitive projects.

2.1 ANSI Objectives :

As part of the implementation of the national strategic choice in the field of computer security, and to meet the requirements of constant development assisted by the use of modern technologies and the integration of services and public and private institutions, l 'ANSI was created to ensure IT security and to implement a specific national plan.

Its main missions are :

- The implementation of national and public strategic guidelines to ensure the security of information systems and networks.
- Certify natural and legal persons in order to exercise the task of audit expert in the information systems security sector.
- Offer essential solutions and tools to avoid attacks and threats that can prevent the proper functioning of information systems and networks.
- Control the information systems and networks of the various public and private institutions.
- Set standards for the security of information systems and prepare technical guides.

2.2 Organization of ANSI :

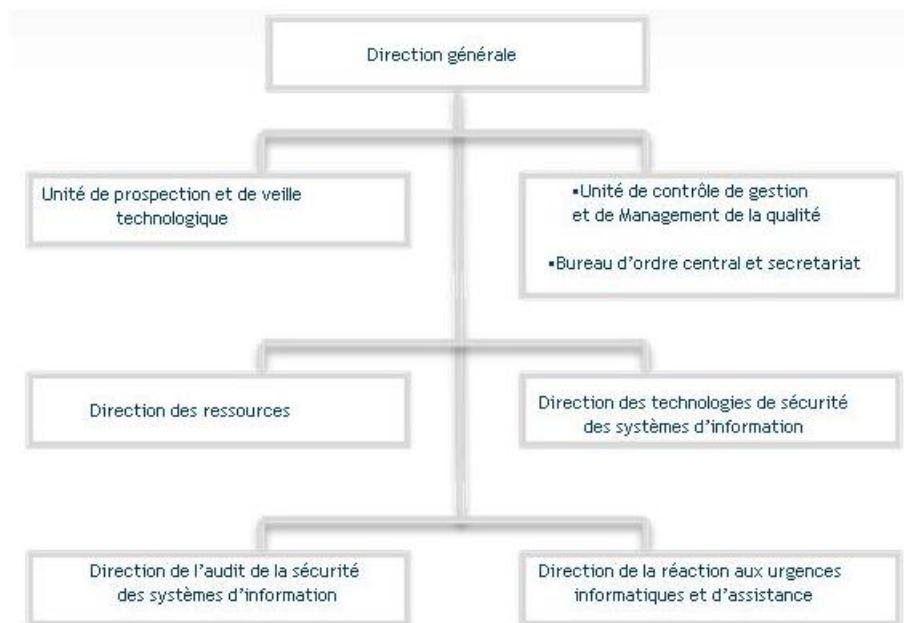


Figure 1 : ANSI organization chart

According to Figure 1, ANSI is made up of 6 units and directorates managed by the director general. The main units and departments are:

- Prospecting and technological watch unit: whose task is to follow scientific developments in the field of IT security and to provide technical mechanisms to attract research and development projects ...
- Management control and quality management unit: which prepares management and quality guides, monitors the preparation of statistics and monitors achievements.
- Information systems security technologies department: which intervenes during an incident or an attack on Tunisian networks and websites and performs technical audit and mock attacks to ensure the security of networks and information systems.
- Information systems security audit department: which analyzes the security situation of information systems and networks subject to the audit operation by putting evaluation indicators.
- Direction of reaction to computer emergencies and assistance: which puts guides and awareness programs intended for the public and specialists in the field, detects dangers and assesses them by directly announcing the attacks which target the national cybernetic space, with the coordination of internet service providers and others.

3. State of the art :

3.1 Project Presentation :

The present project entitled Workflow for the management of the activity of auditors aims to develop a web application for registration, administration of auditors in order to supervise their activities. We will develop an interface for the registration and creation of an account for new auditors on this site, fill out a form and submit their application files for the certificate to exercise the activity of auditor, manage data and personal information of the accounts of registered auditors, an interface to connect to accounts, an interface for administrators to supervise the activities of auditors.

Chapter 2 : Requirements Analysis

1. Introduction :

This Chapter starts specifying users which are administrators of the platform and auditors. These administrators still have problems when it comes to supervising the activities of auditors. The project goal is to give the platform managers the ability to maintain their work in a simpler way.

2. Study of the existing :

Nowadays, for administrators to execute their work, they have to go through a lot of paper work and the audit mission are filled in using excel files.

3. Application Requirements :

3.1 Functional Requirements :

Application requirements do not require much analysis because most are self-evident and some of them emerged during the application development process based on internal tests and comments. These requirements are:

- Authenticating users wanting to access the application and use the services using a login and a password which will be encrypted in the database in order to make the task of password discovery by an attacker complicated.
- Allow user registration to the application.
- Allow users to complete the registration form.
- Convert the completed form to a downloaded PDF file.
- Download the PDF file to the database.
- Allow sending alerts and warnings to ANSI agents and concerned parties.
- Grant the administrator the possibility to manage users.

3.2 Non-Functional Requirements :

After functional requirements are determined, non-functional requirements considered throughout the application development process. Among these requirements, we reference:

- The efficiency of its operations and the speed of responses and their reliability.
- User friendly and ergonomic interfaces: which must be simple and well-structured in terms of information content.
- Scalability and extensibility : the system must be functional and open to new modules and functionalities.
- Portability : the application must imperatively run on windows , Mac and Linux.
- The availability of its services 24 hours / 7 days.

4. Use case diagram :

An UML use case diagram is the primary form of system/software requirements for a new software program under development. Use case specify the expected behavior (what), and not the exact method of making it happen (how).

4.1 Global use case

Every software, project or service, after brainstorming phase demand to collect all the pieces together and frame the idea behind. Figure 1.1 presents connection between all platform components.

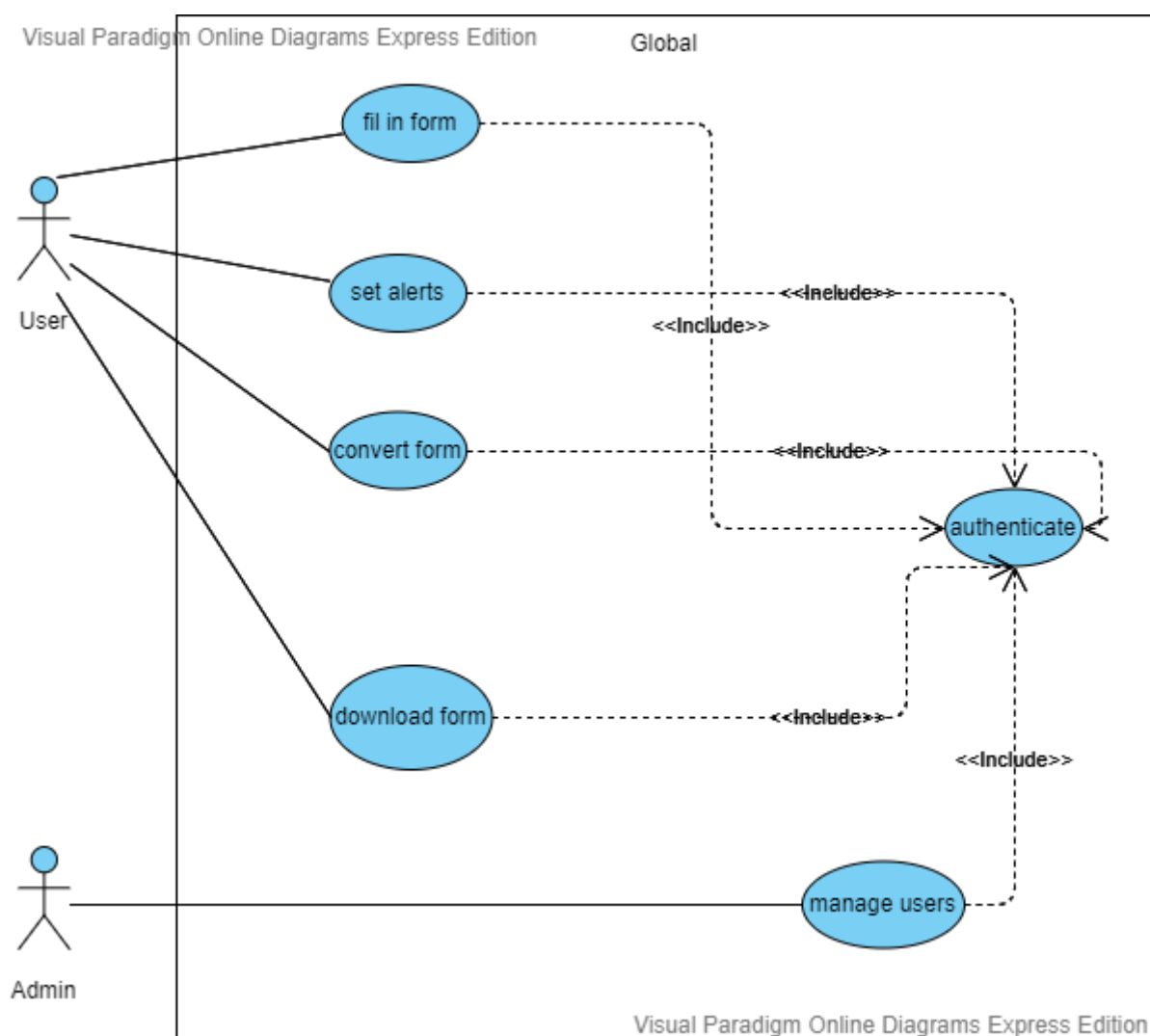


Figure 2.1 : First Case – Global

4.2 Authentification Use Case

