PREPARED BY :
AHMED OLABISI OLAJIDE

ABC TECHNOLOGIES

ISMS SCOPE

1.0 **INTRODUCTION**

The implementation of the ISO/IEC 27001 standard is no small feat. It necessitates the creation of an Information Security Management System (ISMS) designed to comprehensively address information security practices, risks, and vulnerabilities. This Implementation delves into the development of the ISMS at ABC Technologies, with a specific focus on the Software Activity division. It encompasses the definition of the ISMS scope, the identification of assets to be protected, the rationale behind scope size, and the boundaries within which information security practices will be executed.

This scope is a commitment to ensure the confidentiality, integrity, and availability of critical information assets at ABC Technologies. It represents a journey towards not just compliance with information security standards but a proactive approach to securing the future of the organization and its software activity.

1.1 **SCOPE STATEMENT**

“The Information Security Management System (ISMS) of ABC Technologies outlines the guidelines for protecting sensitive information and ensuring the confidentiality, integrity, and availability of data within the Software Activity division. This division encompasses software development, CRM software, and the associated IT infrastructure. The main objective is to safeguard critical assets, customer data, financial information, and intellectual property within this division while adhering to ISO/IEC 27001 standards. This commitment also extends to external entities and databases like SoftProd and maintenance records that are essential for software activities. This is in Accordance with the Latest Version of the Statement of Applicability”.

The scope statement highlights the company's commitment to safeguarding information security. It emphasizes the protection of its highly valuable assets and compliance with industry standards.

1.2 SCOPE BOUNDARIES

It has been determined that the ISMS will only encompass ABC Technologies' software activity. In a meeting with **Sabina Senat** and the individuals responsible for the software activity, an assessment was made regarding the information that needs protection. This includes the product development plan (design, development costs, source code, etc.), marketing plans (company's growth strategy), human resources data, customer database, financial and accounting data, and all contracts (partnerships, employees, contractors).

In this case, the boundaries are established by what falls within the Software Activity division, as detailed by ABC Technologies. This division encompasses software development, CRM software, and related IT infrastructure, along with specific assets and data sets mentioned. Anything outside of this defined area is considered outside the scope and is not covered by the ISMS.

Defining the scope boundaries is a critical step in the development of the ISMS, as it ensures that resources are focused on securing the most critical assets and processes while avoiding unnecessary complexity and resource allocation for areas that are not directly related to the software activities.

1.2.1 ORGANIZATIONAL BOUNDARIES

The organizational scope of ABC Technologies includes the Software Activity division, which consists of various departments, roles, and processes that are directly involved in software development, CRM software, and IT support for these activities. The following elements are included in this scope:

- The President and Vice-President (Paul Evans and Sally McCarty)
- The IT Supervisor (William Clay) and IT team
- The Sales Supervisor and Sales Team
- The Customer Service Supervisor and Customer Service Agents
- The Marketing Supervisor and the Web Designer
- The Support Technician (Billy Davis)

- The Manager of Software Development (Sam Gold) and the Software Activity Team
- The Supervisor Information Security (Alan Brown)
- The Quality Control Analyst (Paul Lee)
- The Programmer (Mick Harris)
- The Network Supervisor (Peter Ly) and Network Technicians
- The Supervisor IT Support (Fred Jones) and Support Technicians
- The HR Manager (Jack Johns)
- The Financial Manager (Maria Garcia)
- The Internal Audit Supervisor (Emily O'Connor)
- The Security and Environment Supervisor (Andrew Hakinen)
- The Legal Advisor and Supervisor for Customer and Supplier Accounts (Thomas Smith)
- The Payroll Supervisor (Jennifer Gordon)
- The Customer Account Assistant (Alexander Fox) and Supplier Account Assistant (Patricia Ducan)
- The Management Controller (Dennis Williams)
- The Security Guard (night) (Pierre Jackson)
- The Administration Team
- The CEO (Sabina Senat)

1.2.2 **INFORMATION SYSTEMS BOUNDARIES**

The information systems boundaries encompass all IT infrastructure, software systems, and databases directly related to the Software Activity division. This includes the following:

- Software development tools and systems
- CRM software and related databases
- IT network infrastructure supporting the software activities
- Information systems involved in product development, marketing, customer data, financial and accounting, and contract management
- External databases, such as SoftProd, containing information relevant to software activities

1.2.3 PHYSICAL BOUNDARIES

The physical scope includes the locations directly associated with the Software Activity division, primarily the head office in Bradford, where most software activities are concentrated, and the sales office in Leeds, which handles sales and services. It also encompasses the physical security measures in place, such as access controls and clear desk policies within these locations.

1.3 RESEARCH AND JUSTIFICATION OF WHAT ASSETS AND BUSINESS PROCESSES ARE INCLUDED AND EXCLUDED FROM THE SCOPE

The protection of a product development plan, especially the source code, is critical and important for several reasons. Source code often contains unique algorithms, functionalities, and features that provide a competitive advantage. Securing it ensures that competitors cannot easily replicate or reverse-engineer these advantages. Making unauthorized changes to the source code can lead to the introduction of vulnerabilities and compromise the software's integrity. To mitigate these risks, it is important to protect the source code from unauthorized modifications .

Maintaining the confidentiality and security of the Customer Database is essential to uphold customer trust. Customers share their personal information with organizations under the assumption that it will be kept safe. Failing to protect this data can result in data breaches and privacy violations, damaging the company's reputation. Customer databases are attractive targets for cybercriminals. Protecting this data is crucial to prevent data breaches, identity theft, and financial losses for both the organization and its customers.

Assets and processes outside the Software Activity division, such as those related to the Printing and 3D Graphics divisions, hardware infrastructure, and hardware maintenance, are excluded from the scope due to the organization's needs and challenges for the ISMS.

Any products or services offered by ABC Technologies outside of the Software Activity division are excluded. The inclusion and exclusion of these assets and business processes are based on their relevance to the Software Activity division, the criticality of their functions, and the need for information security measures to protect them effectively. This ensures that the ISMS focuses on securing the most vital aspects of ABC Technologies' software activities

1.4 RESEARCH AND JUSTIFICATION REGARDING THE SIZE OF SCOPE

The scope of the study is restricted to the Software Activity division only. This means that other divisions like Printing and 3D Graphics, as well as hardware infrastructure and maintenance, are not included which makes it a **Limited Scope** (PECB, 2016). Therefore, the focus is on the core activities related to software development, CRM software, and associated IT infrastructure. While this limitation streamlines the implementation of security measures, it does not address other areas of the organization that may also require information security.