People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
Larbi TEBESSA University - TEBESSA
Faculty of economic commercial and management sciences

Submitted in partial fulfillment of the requirements for the degree of Master

Domain: Accounting and Finance

Field: Accounting sciences

Specialty: Accounting and Finance

Evaluating cyber security measures in protecting accounting information systems: case study of tebessa phosphate company

Topic submitted by:

GUERDI Imen

OUAHAB Ikram

Before the jury:

Dr. Ben Aboude Chadia	University Larbi Tébessi	President
Dr. Jawel Marwa	University Larbi Tébessi	Examiner
Dr. Abid Khadidja	University Larbi Tébessi	Supervisor

Class of 2026

Gratitude and Appreciation

يتقدم الطالبان بخالص عبارات الشكر والتقدير والاحترام إلى الأستاذة المشرفة

"عبيد خديجة"

التي تفضلت بالإشراف على هذه المذكرة، ولم تبخل علينا بتوجيهاتها العلمية القيّمة ونصائحها السديدة طوال مراحل إعداد هذا العمل

كما نتوجه إليها بعظيم الامتنان على صبرها، وتشجيعها المستمر، وملاحظاتها البنّاءة التي كان لها الأثر الكبير في تحسين محتوى هذه الدراسة وإخراجها في صورتها النهائية

لقد كانت متابعتها الدقيقة وحرصها الدائم دافعًا لنا لبذل المزيد من الجهد والاجتهاد، فكان لتوجيهاتها فضل كبير في تجاوز مختلف الصعوبات التي واجهتنا أثناء إنجاز هذه المذكرة.

ونسأل الله تعالى أن يجزيها عنا خير الجزاء، وأن يوفقها في مسيرتها العلمية والمهنية، وأن يجعل ما قدمته لنا في ميزان حسناته.

Dedication

...إلى نفسي

التي تعلّمت أن تقف وحدها،

حين غاب السند،

.وأن تكمل الطريق رغم الغياب

إلى روح والدي" قردي عبد الله" رحمه الله

الغائب عن عيني، الحاضر في قلبي،

أهدي هذا العمل،

لعلّه يصل إليك دعاءً وفخراً لا ينقطع

إلى أمي... صبرك كان دائماً سرّ قوتي

إلى إخوتي... شكراً لكم على دعمكم

Dedication

﴿ فَرِحِينَ بِمَا آتَاهُمُ اللهُ مِنْ فَضْلِهِ ﴾

من قال أنا لها "نالها " وأنا لها إن ابت رغماً عنها أتيتُ بها

لم تكن الرحلة قصيرة ولا ينبغي لها أن تكون لم يكن الحلم قريبا ولا الطريق كان محفوفا بالتسهيلات لكني فعلتها ونلتها

أهدي تخرجي الى النور الذي أضاء دربي الى العزيز الذي حملت اسمه فخراً الى الرجل الذي سعى طوال حياته لأكون الأفضل (أبي الغالي)

الى التي احتضنتني بقلبها قبل يدها التي سهلت لي الطريق بدعائها الى الظل الخفي والقلب الحني الى سر قوتي ونجاحي (امي الغالية)

Abstract:

This study aimed to identify the most important cybersecurity measures for protecting Accounting Information Systems (AIS), through a case study conducted at the Phosphate Company (SOMIPHOS), Tebessa branch, using the descriptive-analytical approach.

The study concluded that SOMIPHOS places great importance on cybersecurity for accounting information systems by adopting a set of security procedures and measures to protect accounting data, particularly through the use of the Sage 100c system. These measures include controlling user access permissions, data encryption, and regular data backups.

The study also revealed several areas that the company should improve, most notably strengthening cybersecurity culture among employees and increasing awareness of the risks of cyberattacks. In addition, the study showed that the field of cybersecurity in Algeria still experiences some delays compared to developed countries, despite the growing interest in it in recent years.

Keywords: cybersecurity, accounting information systems (AIS), Sage 100C system, Cybersecurity measures.

الملخص:

هدفت هذه الدراسة إلى معرفة أهم تدابير الأمن السيبراني في حماية نظم المعلومات المحاسبية، من خلال دراسة حالة بمؤسسة الفوسفات (SOMIPHOS) فرع ولاية تبسة وذلك بالاعتماد على المنهج الوصفي التحليلي .

وقد توصلت الدراسة إلى أن مؤسسة SOMIPHOS تولي أهمية كبيرة للأمن السيبراني لأنظمة المعلومات المحاسبية، من خلال اعتمادها على مجموعة من الإجراءات والتدابير الأمنية لحماية البيانات المحاسبية، خاصة باستعمال نظامSage 100c ، مثل التحكم في صلاحيات المستخدمين، تشفير البيانات، والنسخ الاحتياطي المنتظم.

كما أظهرت الدراسة وجود بعض النقاط التي ينبغي على المؤسسة تحسينها، من أبرزها ضرورة تعزيز الثقافة السيبرانية لدى العاملين، وزيادة الوعي بمخاطر الهجمات الإلكترونية. كذلك بيّنت الدراسة أن مجال الأمن السيبراني في الجزائر لا يزال يشهد بعض التأخر مقارنة بالدول المتقدمة، رغم تزايد الاهتمام به في السنوات الأخيرة .

الكلمات المفتاحية: الامن السيبراني، نظم المعلومات المحاسبية(AIS) ، النظام ,sage 100c تدابير الامن السيبراني.

Contents:

List of tables

List of Figures

Introduction:

In recent years, the world has witnessed a dangerous and rapid development, which indicates that we have entered the age of digitization, especially in the field of information and communication technology. This has led to a cautious shift in the way information is managed in various institutions, and accounting information systems have become a tool. Essential and reliable for processing, storage, and provision, these systems are also characterized by their reliability, which aids in decision-making. However, with this impressive development in the use of these digital systems, challenges and obstacles have emerged that hinder and affect the operations of institutions. This is due to cyberattacks that threaten accounting data, such as breaches, data manipulation, and unauthorized access, making it imperative to have deterrents.

From this perspective, cybersecurity emerged as a fundamental pillar for protecting these accounting systems. Its goal is to ensure protection, maintain the continuity of the institution, and reduce cyber risks. This term is relatively new locally but internationally recognized, and Algeria is still studying and implementing it. Our study aims to evaluate cybersecurity in protecting accounting information systems. This study combines theoretical and applied concepts to understand all aspects, obtain a logical and sound analysis, and identify vulnerabilities.

1- Presenting the main problem:

The research problem lies in evaluating the effectiveness of cybersecurity for accounting information systems, considering that the latter is a deterrent and effective means of protecting accounting information systems and maintaining their integrity. Therefore, based on the above, we can pose the following question:

How effective are cybersecurity measures in protecting accounting information systems within organizations, particularly in the case of Tebessa Phosphate Company?

2- Sub-questions:

- What are the main cybersecurity threats?
- What are the components of accounting information systems?
- How are cybersecurity measures applied in organizations?
- How does the Sage system contribute to data security?

3- Hypotheses:

In order to answer the main research problem and the sub-questions of the study, the research is based on a set of hypotheses that can be formulated as follows:

- Cybersecurity measures are effective in protecting accounting information systems within organizations **(Main Hypothesis)**.
- The use of systems such as Sage improves data security and reliability.
- The application of cybersecurity practices reduces risks and cyber threats.
- The effectiveness of accounting information systems depends on the level of cybersecurity measures adopted by the organization.

4- Objectives:

In light of the accelerating digital transformation and the growing reliance on accounting information systems within organizations, cybersecurity has become a strategic necessity to ensure the protection of financial and accounting data from various cyber threats. Depends on that, this study aims to:

- To analyze the role of cybersecurity in protecting AIS.
- To study the use of the Sage system in the company.
- To evaluate the effectiveness of cybersecurity measures.

5- Importance of the study:

This study addresses a fundamental and important new topic of great significance, namely "Evaluating cyber security measures accounting information systems." This topic is of paramount importance and must be examined. This importance is summarized in the main points addressed in this study, which presented a set of risks that threaten accounting information systems facing institutions of all types. It also presented the measures taken and the components, and we also sought to provide an applied study that brings together all the questions raised. Our goal is to reconcile and link the practical and theoretical aspects of this study. It also sheds light on the seriousness of these cyberattacks and the extent to which they affect the work of institutions. It also highlights how to reduce these cyber risks, support decision-making, and enhance confidence in accounting systems.

6- Justification of the study:

- Integrating specialization with digitalization.
- A new topic locally, especially in the field of accounting and finance.

- Getting to know cybersecurity up close

7- Limitations of the study:

- **Spatial limitation**: The study is offered in two sections: Human Resources and Computer Science, at the phosphate company in Tebessa province.
- **Temporal limitation**: In the theoretical framework, all periods were covered, while in the practical framework, it was studied over 3 months. The study was conducted during this period, despite its length, to ascertain the essential information.
- **Human limitation:** The study focused on those responsible for the accounting information system and the Sage 100c system.

8- Study methodology:

This study adopted a descriptive-analytical approach to understand the concepts related to both cybersecurity and accounting information systems, and to identify and evaluate the measures taken. A case study of the Phosphate Corporation was also used as an applied model to help apply theoretical concepts to practical realities through the study of the Sage system.

9- Research Structure:

This study is divided into two main chapters, preceded by an introduction and followed by a conclusion, as follows: Chapter One: Theoretical Framework of Cybersecurity and Accounting Information Systems.

This chapter addresses the theoretical aspect of the study, discussing the concepts of cybersecurity and its importance, as well as defining the second variable, accounting information systems, and their role in organizations. It also addresses cyber threats that target and threaten the system, and the relationship between the two variables.

Chapter Two: Applied Study: A Case Study of the Phosphate Company in Tebessa

This chapter focuses on the applied field study, introducing the company and the subject of the study, familiarizing oneself with the Sage system, and evaluating the effectiveness of the company's cybersecurity measures in protecting accounting data from risks and breaches.

10- Study challenges:

- We ran into a few challenges while doing our research, such as the following:
- The scarcity of free resources and the abundance of paid resources

- Difficulty in finding an institution that accepts internships
- Access to basic internal data is prohibited.

11- Previous studies:

- **Almomani, S., & et al. (2021). The Efficiency and Effectiveness of the Cyber Security in Maintaining the Cloud Accounting Information. Academy of Strategic Management Journal, 20(2).**

This study examined the efficiency and effectiveness of cybersecurity in maintaining cloud accounting information. The results highlighted that cybersecurity controls significantly enhance data protection, confidentiality, and integrity in cloud-based accounting environments.

However, the study focused mainly on cloud accounting environments without deeply analyzing the effectiveness of specific cybersecurity measures within Accounting Information Systems (AIS).

This study extends this by evaluating concrete cybersecurity measures and their practical role in protecting AIS in organizational settings.

- **Romney, M. B., & Steinbart, P. J. (2020). Accounting Information Systems. Pearson.**

The authors analyzed Accounting Information Systems and emphasized their role in improving financial reporting quality and decision-making. They found that AIS performance strongly depends on internal controls and information reliability.

The study does not explicitly integrate cybersecurity as a core determinant of AIS protection.

This research bridges this gap by linking cybersecurity measures directly to the protection and reliability of AIS.

- **Stallings, W. (2017). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley.**

This work provides a comprehensive overview of cybersecurity principles, standards, and best practices. It highlights how structured security frameworks reduce system vulnerabilities and cyber risks.

While the study offers a theoretical foundation for cybersecurity, it lacks application within accounting environments.

Our study applies these principles specifically to AIS, evaluating their effectiveness in financial information protection.

- **National Institute of Standards and Technology (NIST). (2018). Cybersecurity Framework.**

The NIST framework introduces a structured approach to managing cybersecurity risks through identification, protection, detection, response, and recovery functions.

Although widely applicable, the framework remains general and not tailored specifically to accounting systems.

Our research adapts and evaluates these cybersecurity functions within AIS to assess their practical effectiveness in accounting environments.

- **El Sharif, A. (2019). The Impact of Accounting Information Systems on Financial Reporting Quality in Banking Institutions.**

The study investigated the impact of Accounting Information Systems components on financial information relevance in banking institutions. It concluded that AIS improves accuracy and reliability of financial reporting.

However, the study did not consider cybersecurity risks as a factor affecting AIS performance.

This study introduces cybersecurity measures as a critical dimension influencing AIS protection and information quality.

- **Muda, et al. (2025). The Relationship between Information Systems Components and Organizational Value.**

This research explored the relationship between information systems components and organizational value. It found that effective information systems enhance operational efficiency and decision-making processes.

The study focused on system value but did not evaluate security mechanisms protecting these systems.

Our research fills this gap by assessing how cybersecurity measures contribute to securing AIS and preserving organizational value.

CHAPTER 1:

Theoretical Framework of Cybersecurity and Accounting Information Systems

1. General Framework of Cyber Security:

Cyber security is the most serious subject since cyber dangers and attacks are overgrowing. Attackers are now adopting more complex tactics to target the systems. Individuals, small-scale companies or major organization, are all being touched. So, all these organizations whether IT or non-IT firms have grasped the necessity of Cyber Security and focused on adopting all available steps to cope with cyber threats.

1.1. Concept of Cybersecurity:

In today's digital environment, enterprises increasingly rely on information technologies to run their operations. However, this dependency exposes companies to severe cyber dangers. Therefore, in this section, we will explore the notion of cybersecurity, starting with its definition.

1.1.1. Definition of cyber security:

Cyber security has been characterized in many ways by different academics. According to AL Ashqar et al. (2012), it refers to a collection of actions aimed at preserving human and financial resources linked with information and communication technologies, limiting possible losses caused by risks or threats, and assuring the speedy recovery of systems.

Similarly, Banga (2019) regards cyber security as a process involving the analysis, identification, and mitigation of risks associated to cyber-attacks, as well as the exchange of information to increase the efficacy of networked information systems. In the same context, Al-Bar et al. (2018) describe cyber security as a mix of technological and administrative procedures meant to prevent unauthorized access and misuse of information systems, while preserving data confidentiality, privacy, and the continuity of operations (Almomani & et al, 2021).

Based on these concepts, cyber security may be regarded as an integrated framework of technical measures, rules, and principles aimed at protecting sensitive information and decreasing cyber threats, hence assuring the security and stability of companies and society as a whole. The notion of cybersecurity work derives from the fact that it offers the protection of information by preserving its integrity, confidentiality, and availability in addition to protecting the credibility, accountability, and validity of the information. Based on its study, it appeared that there is a difference between the efficiency and efficacy of cyber security, as the Benzel (2011) discloses that its impact on the efficiency of cloud computing can be detected through a variety of critical factors: The construction of various resources, the separation of data assets, and the usage of

external resources. This leads to raising the quality of cloud computing by cyber security and increasing its relevance regarding the efficacy of cyber security. Facundo, Nadia, and Victor (2020), the authors indicated that the success of cyber security depends on numerous elements that must be committed to and examined continually to uncover the flaws through which information may be hacked and stolen (Almomani & et al, 2021).

1.1.2. Importance of Cyber Security:

Cyber security is crucially essential because it protects information, systems, and society from escalating digital dangers. It plays a critical role in securing modern digital ecosystems. Its value may be appreciated through the following major aspects:

- Protection of Sensitive Information: Cyber security maintains the protection of sensitive data such as financial records, personal information, and organizational data, preventing unauthorized access and data breaches.
- Ensuring Data Integrity: It prevents data from being altered or tampered with, ensuring that information stays accurate, dependable, and trustworthy for decision-making processes.
- Protection of Organizational Reputation: A security breach can damage the reputation and credibility of an organization. Cyber security helps maintain trust among customers, partners, and stakeholders (Pfleeger & Pfleeger, 2015).
- Supporting Business Continuity: By preventing and mitigating cyber threats, cyber security ensures that business operations continue without major interruptions (National Institute of Standards and Technology, 2018)
- Compliance with Legal and Regulatory Requirements: Organizations must comply with data protection laws and regulations. Cyber security helps meet these requirements and avoid legal penalties (Stallings, 2017).
- Protection of National Security: At a broader level, cyber security is essential for protecting critical infrastructure (such as energy, banking, and defense systems) from cyber threats (National Institute of Standards and Technology, 2018)

1.1.3. Cyber security objectives:

Cyber security aims to achieve a set of fundamental objectives to secure information systems and ensure data integrity by developing advanced policies, procedures, and technologies to counter these threats. These objectives include protecting the confidentiality of information, maintaining its integrity, ensuring its availability when needed, and enhancing trust in the digital environment.

- Protecting the infrastructure of information security and citizens' private data.
- Taking all necessary preventive measures to protect citizens and institutions from potential risks resulting from the use of various technologies.
- Protecting information from attacks by understanding the latest technologies and techniques used in this field, and identifying the methods used by attackers in order to anticipate and prevent attacks before they occur.
- Protecting operating systems from unauthorized access attempts and ensuring the continuous and secure functioning of information systems.
- Studies have shown that achieving these objectives contributes to the stability of institutions, the security of their operations, and the protection of their data and employees' information. This also enhances employees' psychological security, which positively affects their performance.

Cybersecurity plays a key role in improving the performance of institutions, whether educational, industrial, or governmental. It helps organizations develop and achieve better (وليد و آخرون، 2022)

1.2. Cyber Security Components:

Cyber security is a multidimensional concept that relies on the interaction of several key components to ensure the effective protection of information systems. These components encompass human, technological, organizational, and legal aspects, all of which must work together to reduce cyber risks and enhance system security.

1.2.1. Human Components :

The human element is considered one of the most critical components of cyber security, as individuals often represent both the first line of defense and the weakest link in security systems. Employees, system users, and managers play a significant role in maintaining security through their awareness, behavior, and adherence to security policies. A lack of training or awareness can lead to security breaches such as phishing attacks or password misuse. Therefore, organizations must invest in continuous education and training programs to strengthen users' ability to recognize and respond to cyber threats. (Stallings, 2017)

1.2.2. Technological Components :

The technological component includes all hardware, software, networks, and security tools used to protect information systems. This involves the implementation of firewalls, intrusion detection systems, encryption techniques, and authentication mechanisms. These technologies are essential

for preventing unauthorized access, detecting potential threats, and ensuring the confidentiality and integrity of data. Effective use of advanced technologies significantly reduces system vulnerabilities and enhances overall security performance. (Pfleeger & Pfleeger, 2015)

1.2.3. Organizational Components:

The organizational component refers to the set of policies, procedures, and governance frameworks that guide cyber security practices within an organization. This includes security policies, risk management strategies, internal controls, and incident response plans. A well-defined organizational structure ensures that security responsibilities are clearly assigned and that appropriate measures are implemented to manage cyber risks. Moreover, strong governance enhances accountability and supports the integration of cyber security into overall business strategies. (National Institute of Standards and Technology, 2018)

1.2.4. Legal and Regulatory Components :

The legal and regulatory component involves compliance with laws, standards, and regulations related to information security and data protection. Organizations are required to adhere to frameworks such as ISO/IEC 27001, which provide guidelines for establishing effective information security management systems. Compliance not only helps in avoiding legal penalties but also strengthens the organization's credibility and trustworthiness. Furthermore, legal measures play a crucial role in protecting personal data and ensuring privacy in the digital environment. (International organization for standardization, 2018)

In conclusion, cyber security components are interdependent and must be integrated to achieve a comprehensive security framework. The effectiveness of cyber security strategies depends on the balance and coordination between human awareness, technological tools, organizational practices, and legal compliance. (International organization for standardization, 2018)

1.3. Types of cyber threats:

With the rapid development of information technologies, organizations are uncreating that may affect their systems and data. Understanding these threats has become essential in order to identify potential risks and ensure effective protection of information systems.

1.3.1. Malware:

Malware is an application or software which can generally be stealthily put on A device. In most circumstances, the user has no awareness of the existence of malware on their Device. The word malware denotes a variety of dangerous applications and quite often Infects systems in many ways. The objective of malware is to violate the computer's Security, install harmful software, and then studies the environment with the Opportunity to spread further. The most prevalent dangers to malware are the loss of Control over the device, the loss of privacy when using the device, the loss of private and secret information, and last but not least the decline in processing power or even the operation of the device. (Jan & Ludek , 2019)

The main types of malwares include:

- Adware (installation of junk advertising software)
- Spyware (private device monitoring)
- Virus (software which connects to an authorized program and then causes Various damage to HW and SW and is able to distribute itself)
- Worm (autonomous software which does damage to HW and SW)
- Trojan (software which contains hidden features that threaten the device is not Able to propagate without the user's help)
- Backdoor (software which contains hidden functions and opens computer Communication ports)
- Rootkits (software which allows masking the presence of malicious software on A device)
- Keylogger (software steals login and password)
- Ransomware (Data loss due to encryption)

The source of the threat using malware is generally devices already included in the botnet. The source of the threat is therefore the hardware or software on the Network. Malware occurs since 1986. Within the recorded occurrence of CSIRT Czech Republic since 2008, the botnet attack rate to selected information systems has an Average of 94 cases per year. The malware development trend was highest in 2014. (Jan & Ludek , 2019)

1.3.2. Phishing:

Phishing is a cyberspace crime using social engineering techniques. The goal is to gain access to user bank accounts or other money accounts as well As a way of getting users' personal data. Phishing uses spam to send it in bulk to "serious" Messages, which have links at first sight to serious websites and Applications. These pages are only copies of the real ones and are meant to

create A sense of security and then the user gives the information to the hackers. Phishing is stealing victims' money or personal data. Threats include loss of identity, Loss of funds, and existential problems but even if it is malware installation Loss of control over your device, loss of your own private data, or enlistment in a botnet Pharming is an advanced kind of phishing that aims at raising funds, installing malware or personal data. Pharming is an attack on the DNS server of an internet Provider. The user does not know that it is a fake web site when he visits his online Bank. Spear Phishing is a type of phishing that targets a specific individual or organization. The attack is very often organized by an Organized group and aimed at a specific objective. The goal of Spear Phishing is to contact a person within the organization and use that person to access the internal network, install malware or obtain private or classified data (Jan & Ludek , 2019)

The threat actor that uses phishing is usually an attacker. It can be a Person or a group of people organized in a group. They can also threaten devices already in the botnet. Thus, the danger originates from the person, Person or hardware on the network. Phishing exists since 1987 but it started to spread only around the World in 2003 and in the Czech Republic in 2006 (Jan & Ludek , 2019).

1.3.3. Ransomware :

Ransomware is sometimes called blackout ware. The blackmail software is intended to block users from accessing the device, or his private or classified information for a certain period of time or until the ransom is paid. The original ransomware was a program that locked users out of their accounts. Ransomware second generation is Software which doesn't deny access to the user computer account but locks and encrypts the user's private and confidential data. Ransomware uses powerful encryption Algorithms to lock and selectively encrypts data, so as to make the attack target the Most important parts of the device system. The primary objective of ransomware is to Generate income in various currencies. The biggest threat of ransomware is losing important Data and even after paying the requested amount, data availability is not guaranteed.

The source of the threat via ransomware is usually a device already part of the botnet or an infected device. The hardware is therefore the source of the threat. (Jan & Ludek , 2019)

1.3.4. Software:

Ransomware has been around since 1989, when the first blackmail software was a trojan called AIDS. 2005: Ransomware goes big time. The Police virus and then Crypto locker were already pretty well known. The present threat to ordinary communication and Information devices is the

threat of Ransomware. Czech Republic did not attack cybernetic critical infrastructure ransomware in Czech Republic in the critical infrastructure and CSIRT data (Jan & Ludek , 2019).

1.4. Cyber Security Risks:

Cyber security has become an urgent need in the digital society and a necessity for the Development, development and support of this specialty, which is considered a sensitive and essential detail in cyberspace that competes with the necessary needs in our daily Lives due to the dependence of individuals and institutions all over the world on modern Technology. From this standpoint, the National Institute has given NIST Standards and Technology defines cyber security as "protecting electronic communications systems and Services, including the information contained in them, from damage.", and indicators of the occurrence of cyber risk can be classified according to the following indicators. (marioush & Al-obaidi, 2026)

- Origin. An indicator to determine whether the hacking process originated from Within the organization or by an external party to achieve personal interests or to leak Information for the benefit of another party.
- Classification According to the Method Through Which the Cyber-Attack is Carried Out. As it is classified into more than one type Denial of service, Phishing. Eavesdropping attack, Password attack, Scripting attack, malicious software, Zero-day Attack
- Lack of Preventive Behaviors. Which is one of the indicators that help a cyberattack occur, and is represented by individuals or institutions not encrypting the password or installing anti-virus programs within the electronic systems in place.

From the foregoing, the two researchers conclude that cyber security threats originate from financial institutions' inadequate dependence on current technological tools and their lack of proper Protection capabilities for their electronic systems. This may undermine the infrastructure of their system, or may hurt their reputation or ownership owing to the theft of sensitive Data, which causes them financial loss (marioush & Al-obaidi, 2026).

2. Accounting Information Systems Concept:

In the context of digital transformation, organizations increasingly rely on information systems to manage their financial and accounting information systems (AIS) play a crucial role in ensuring the efficient collection, processing, and storage of financial data. therefore, understanding their components and functions has become essential for improving organizational performance.

2.1. definition of accounting information systems:

Accounting Information Systems (CAIS) are regarded a vital pillar for management, enabling the fulfillment of its tasks and responsibilities. CAIS represents the combination of two primary fields: accounting and information systems.

It integrates computer technology, human resources, and accounting standards, which together increase the availability of accurate and timely information for decision-making and managerial assistance. Proper deployment of CAIS benefits a company by decreasing risks, eliminating human mistakes, and supporting its fundamental objectives. Computerized accounting information systems are characterized as "an integrated set of subsystems, both tangible and intangible, that work together to process financial transaction data." CAIS also incorporates numerous primary and subsidiary components, establishing the system's structural framework, which regulates the phases and procedures of the accounting cycle. (marioush & Al-obaidi, 2026)

Accounting is a data identification, gathering, and storage procedure as well as an information production, measurement, and communication process. By definition, accounting is an information system, as an AIS collects, records, stores, and processes accounting and other data to create information for decision makers. This is demonstrated in Figure an AIS can be a paper-and-pencil manual system, a complicated system incorporating the latest in IT, or something in between. Regardless of the strategy selected, the procedure remains the same. The AIS must collect, enter, process, store, and report data and information. The paper and pencil or the computer hardware and software are only the tools used to create the information (Romney & Steinbart, 2017)

2.2. Objectives of accounting information systems:

The basic purpose of accounting is to offer valuable and reliable financial information to individuals and institutions, helping them in making informed and sensible decisions. Accounting Information Systems (AIS) focus on how information is gathered, processed, and turned from raw data regarding the activities and operations of economic units into meaningful and relevant information. This lets diverse divisions within a company to successfully use, store, and manage the information in their everyday operations. The fundamental objective of AIS is to offer accurate and timely information to internal users, including as management, employees, and trade unions, as well as external users, including suppliers, creditors, banks, and tax authorities (Chiyad, 2024).

There are three objectives of the accounting information system to accomplish the system's Main purpose.

2.2.1. Objectives of daily support of operations:

In every economic organization, daily activities and occurrences, known as accounting operations, entail financial transactions between parties that transfer economic value as a result of administrative choices. Examples include receiving cash from debtors, paying creditors, or purchasing and selling items. Accounting operations also encompass non-financial procedures, such as purchase orders or sales orders, because they effect the accounting process. These transactions, whether financial or non-financial, are conducted methodically through accounting records and books using defined processes and procedures. The processing of data is standardized across all sorts of economic units—whether service, manufacturing, or commercial companies. Specialized subsystems, such as inventory management, accounts receivable, and accounts payable, are utilized to handle certain sorts of processes, assuring accurate and efficient accounting within the business (Chiyad, 2024)

2.2.2. Objectives of supporting decision-making:

This aim comprises delivering all accounting information essential for the decision-making process, ensuring it corresponds with the organization's activities of planning, organizing, regulating, and assessing performance. This procedure is conducted by the operation and processing of information entered into accounting information systems. Many economic institutions utilize AIS to process current and future financial information, such as expected revenues for upcoming years, by preparing planning and flexible budgets, comparing them with actual production results, identifying deviations, and analyzing their causes in order to address them effectively (Chiyad, 2024).

The system delivers a wide range of information that companies need to make proper and informed decisions. For example, AIS gives precise data on revenue patterns for the past and current years, enabling management to build budgets such as sales budgets, production budgets, material purchase budgets, and cash budgets. In big firms, cost accountants play a significant part in the decision-making process by presenting management with cost information, including direct materials, direct labor, and indirect industrial expenses. This information supports production managers in making decisions on the purchase or manufacture of items essential for the organization's production or manufacturing activities (Chiyad, 2024).

2.2.3. Objectives of fulfilling the Department's requirements:

Always in small-sized economic institutions such as basic institutions or solidarity Institutions or shareholders, they normally issue financial reports at the end of each financial Year to shareholders on the performance of their company and on their financial situation, dividends and taxable income to third parties. As far as major companies such as mergers, holding or Public ownership have various and varied requirements, like in large industrial firms, These enterprises must provide the necessary and necessary information to investors, Creditors, suppliers, financial analysts and the general public by providing them with Information contained in the financial statements on income and financial position for the Current year and the previous year to assist them in making investment decisions (Chiyad, 2024).

2.3. Importance of accounting information systems:

The growing complexity of economic activities and the prevailing uncertainty in the business environment have reinforced the need for effective Accounting Information Systems (AIS). These systems are designed to generate relevant, reliable, and timely accounting information that supports decision-makers in selecting the most appropriate alternatives and minimizing uncertainty.

The importance of accounting information can be highlighted through the following points:

- Accounting information constitutes a strategic resource for management, as it enhances planning, organizing, controlling, and performance evaluation, thereby contributing to the achievement of organizational goals with greater efficiency and effectiveness.
- A significant number of administrative failures can be attributed to the lack of accurate, sufficient, and timely information, which is essential for supporting sound decision-making processes.
- Accounting information ensures the measurement and recording of economic events in monetary terms, transforming raw data into structured financial reports that provide meaningful insights to internal and external users. (Al-saati, et al., 2022)

2.4. components of accounting information systems:

before presenting the components of the accounting information system, it is necessary to realize that this system is a structured framework that incorporates numerous parts to efficiently process and handle accounting information. The following diagram demonstrates this structure.

Figure 1:Components of accounting information systems

Source: Adapted from the NIST cyber security framework (national institute of standards and technology 2018)

The accounting information system is like any system consisting of a set of elements to achieve its goal. So, we find that accounting information systems commonly formed of six main elements: people, instructions and procedures, software, data, information technology infrastructure and internal controls.

The following is an explanation of each component in detail.

2.4.1. People (the Human Element):

The persons participating in accounting information systems are the system users. Professionals who may need to utilize an organization's AIS include accountants, business analysts, consultants, managers, auditors, and chief financial officers. The technology also allows external users of the company to access information as requested. For example, consultants may utilize the information in the AIS to examine the success of the company's pricing system by reviewing sales data, cost data, and revenue. Therefore, the AIS must be built to fulfill the demands of its users. In addition, the system should be user-friendly, work smoothly, and improve efficiency rather than inhibit it (Elsharif, 2019).

2.4.2. Technical components:

Your ability to plan and manage business operations depends partially on your knowledge of the technologies available. For instance, can we control manufacturing without understanding of robotics Obviously, technical improvements have a major influence on information systems; enterprise systems, ERP systems, e-business, databases, and intelligent systems are merely a few

examples. Technology is the foundation on which AIS and business operations rely (Marshall B & Paul John, 2020).

2.4.3. Hardware:

Hardware refers to the physical components and equipment that constitute the foundation of any information system. This comprises computers, servers, networking equipment, storage devices, and peripheral devices. The performance, reliability, and efficiency of an information system primarily depend on its hardware. In companies, hardware provides data storage, processing, and communication, making it a crucial aspect of the information system infrastructure (Muda & et al, 2025).

2.4.4. Software:

The software portion of the accounting information system is the computer program employed to save, retrieve, store, process and analyze the firm's financial data. Before computers exist, accounting information systems were hand-operated, paper-based systems, but currently, most organizations are utilizing computer software as the basis of the system of accounting information. Reliability, quality, and security are important factors of the functional software for the accounting information system. Managers rely upon information that generated by the system to create suitable resolutions of the organization, and they require high-quality information to conduct these right judgments. Accounting information systems programs can be built to satisfy the particular demands of various forms of enterprises. If an existing program does not suit a firm's objectives, the software may either be built in-house with considerable input from end users or can be produced by another company expressly for the organization (T.A.Elsharif, 2019).

2.4.5. Procedures and databases:

2.4.5.1. Internal controls :

All organizations face risks in both their daily operations and long-term management activities. Some risks are beyond the control of management. For instance, an earthquake may disrupt operations or damage buildings and equipment. However, managers can take measures to minimize the negative effects of such events, such as ensuring that buildings are designed to resist earthquake damage. In general, management has the responsibility to reduce risks or mitigate their impact whenever possible. These processes are known as controls, Accountants have traditionally played a key role in designing and implementing controls that reduce risks affecting an

organization's financial position. They are typically experts in controls that address risks in broad categories, including:

- The risk of asset theft or misuse.
- The risk of errors in accounting data or information.
- The risk of fraudulent activities by employees, managers, customers, or vendors.

Risks associated with IT systems, such as:

- Incorrect data input
- Errors in data processing
- Computer fraud
- Security breaches
- Hardware or software failures
- Natural disasters affecting computer system operations (Romney & Steinbart, 2018)

2.4.5.2. Databases:

Your past accounting courses have stressed accounting as a reporting function .the whole accounting cycle ,however ,includes data gathering and storage ,and these parts must become part of your knowledge base.in addition important to a complete understanding of Ais are the available in these databases and methods of retrieving those data .to perform analysis ,to prepare information for management decision making, and to audit a firm's financial records, an accountant must be able to access and use data from public and private databases (Ulric J & et al, 2018).

3. Cyber security in Accounting Information Systems:

3.1. The Relationship Between Cybersecurity and Accounting Information Systems:

Since cybersecurity is one of the key pillars for guaranteeing the protection of digital systems, stored data, and sensitive information within cyberspace from various threats and cyberattacks that are constantly evolving alongside technological advancement, it is closely related to information systems in general and accounting information systems in particular. As businesses depend more and more on modern technology to manage their operations, protecting these systems has become crucial and unavoidable. (آمال سالم ، 2025)

Because they play a crucial role in gathering, processing, storing, and evaluating financial data—a fundamental component of effective management and financial decision-making—Accounting

Information Systems (AIS) are highly valued in both governmental and economic institutions. Due to their widespread usage in a variety of conventional and digital activities, including electronic financial services, e-commerce, and e-administration, these systems are more vulnerable to numerous cyberthreats.

Cybersecurity is essential in this situation because it offers a range of safeguards and preventative processes to protect these systems from viruses, breaches, and efforts to alter or delete data. Any flaw or failure in cybersecurity frameworks might have major repercussions, such as significant financial losses, interruption of business operations, loss of important data, harm to sensitive information infrastructure, and a drop in stakeholder trust.

As a result, cybersecurity goes beyond only safeguarding data; it also guarantees business continuity and improves the dependability and legitimacy of the results produced by Accounting Information Systems. Because a strong cybersecurity framework is essential to guaranteeing the efficacy and efficiency of these systems within businesses, the connection between cybersecurity and AIS may be characterized as both complimentary and interdependent (آمال سالم ، 2025).

3.2. Cybersecurity as a Strategic Necessity in Accounting Information Systems:

Cybersecurity has expanded tremendously alongside the rising digitization of the accounting industry. It was formerly regarded a strictly technical issue related to the IT area, largely focused with safeguarding hardware, software, and networks against disturbances. However, with the growing complexity of Accounting Information Systems (AIS) and the expanding dependency of enterprises on digital technology, cybersecurity risks have grown more serious and now directly threaten the dependability and integrity of accounting data.

The digital transformation of AIS has enabled the automation and integration of financial activities into centralized systems, but it has also raised susceptibility to numerous cyber dangers such as data breaches and ransomware attacks. These vulnerabilities can adversely influence financial information and threaten the veracity of financial reporting, which may eventually decrease stakeholder trust. Consequently, cybersecurity is increasingly considered as a vital factor in protecting the integrity of accounting systems.

To address these risks, firms are required to establish complete cybersecurity plans that involve technology solutions, policies, procedures, and personnel training. Cybersecurity has also become a significant facet of corporate governance, needing attention at all organizational levels. As AIS becomes important to company processes, cybersecurity is no longer considered as a simply

technological worry but as a basic necessity for business continuity and sustainability (Andi, 2024).

4. Cyber Security Measures :

In modern organizations, Accounting Information Systems (AIS) are essential for processing, storing, and communicating financial information. However, the increasing reliance on digital platforms exposes these systems to various cyber threats, including unauthorized access, data breaches, and malicious attacks. Therefore, implementing effective cybersecurity measures has become a critical requirement to ensure the security and reliability of accounting data.

Cyber security measures encompass a combination of technical and behavioral practices aimed at protecting information systems from potential risks. In the context of AIS, these measures contribute to maintaining the confidentiality, integrity, and availability of financial information, which are fundamental principles of information security (Romney & Steinbart, 2021).

4.1. Use of Internet Security Software:

The use of antivirus and anti-malware software is essential for detecting and preventing cyber threats. These tools help protect accounting systems from malicious programs that may compromise sensitive financial data.

This measure enhances data protection by preventing unauthorized access and system damage. However, its effectiveness depends on regular updates to ensure protection against newly emerging threats (William, 2018).

4.2. Strong Password Management:

Strong password policies require users to create complex passwords that include letters, numbers, and special characters, and to update them regularly.

Passwords represent the first line of defense in AIS security. Weak or reused passwords increase the risk of unauthorized access, which may lead to financial data manipulation or fraud (James A, 2016).

4.3. Regular Software Updates:

Updating operating systems and applications ensures that known security vulnerabilities are patched and fixed.

Cybercriminals often exploit outdated software to gain system access. Regular updates reduce these risks and contribute to system stability and security (Kenneth C & Jane P, 2020).

4.4. Social Media Security Management:

Users should limit the sharing of personal information on social media platforms and adjust privacy settings appropriately.

Excessive information sharing can facilitate social engineering attacks, which may indirectly compromise AIS security by targeting system users (Michael E & Herbert,J, 2019).

4.5. Securing Home Networks:

Protecting home networks involves using strong passwords, encryption protocols, and Virtual Private Networks (VPNs) to secure internet connections.

With the rise of remote work, unsecured networks can expose accounting systems to external threats. VPNs help ensure secure data transmission across networks (Stallings, 2017)

4.6. Personal Computer Protection:

This includes enabling firewalls, installing antivirus software, and maintaining system updates.

Personal computers are key access points to AIS. If compromised, they may allow attackers to gain full access to financial systems and sensitive data (Romney & Steinbart, 2021).

4.7. Mobile Device Security:

Mobile devices should be secured using strong authentication methods such as two-factor authentication (2FA) and by installing applications only from trusted sources.

Mobile devices increase flexibility but also introduce security risks. Proper protection reduces the likelihood of unauthorized system access (Kenneth C & Jane P, 2020).

4.8. Use of Updated Operating Systems:

Using modern and updated operating systems ensures access to the latest security features and protections.

Outdated systems contain known vulnerabilities that can be easily exploited, making them a major security risk for AIS environments (Stallings, 2017).

Cybersecurity measures in Accounting Information Systems require an integrated approach that combines technological solutions with user awareness and behavioral practices. The effectiveness of these measures lies in their complementarity, as no single control can provide complete protection. By implementing these practices, organizations can enhance the security of financial data, ensure the reliability of accounting information, and reduce the risks associated with cyber threats.

CHAPTER 2:

A Case Study on the Application of the Sage Accounting System at the Tebessa Phosphate Company.

1. Introduction to the Company and the activity unit:

In order to complement the theoretical part of this study, a practical approach was conducted within a real organization. This section aims to present the host company and the activity unit, in order to better understand the working environment and the use of the accounting information systems in practice.

1.1. Company Overview (Tebessa Phosphate Company):

The Phosphate Mines Company (SOMIPHOS) was established as a result of structural changes that occurred within the organizational environment of FERPHOS, which itself emerged from the restructuring of SONAREM under Executive Decree No. 83-441 issued on July 16, 1983.

Following these changes, FERPHOS became a public company composed of seven subsidiary entities managed by the group's general management. Among these subsidiaries is the Phosphate Mines Company (SOMIPHOS), located in Tebessa, which consists of five units: Djebel Onk Mining Complex (CMDO), Annaba Port Facilities (IPA), Center for Applied Research and Development (CERAD), Administrative Headquarters (DUS), and Land Transport Unit (UTR).

1.1.1. Company definition:

The Phosphate Mines Company (SOMIPHOS), based in Tebessa, began operating independently from FERPHOS on January 1, 2005. Its capital amounts to 1,600,000,000. The company is composed of the following units:

- Djebel Onk Mining Complex (CMDO): includes a natural phosphate extraction mine and a processing plant located in Bir El Ater, Tebessa.
- Annaba Port Facility (IPA): responsible for handling and shipping phosphate products intended for export.
- Center for Applied Research and Development (CERAD): responsible for monitoring and analyzing the internal performance of the company.
- Administrative Headquarters (DUS): responsible for supervising and managing the different units of the company.
- Land Transport Unit (UTR): responsible for transporting phosphate products from Bir El Ater to Annaba.

1.1.2. General Objectives of the Company:

The company aims to achieve several objectives, including:

- Developing production, export, and distribution of phosphate products.
- Enhancing the company's capabilities to ensure the exploitation of phosphate reserves.
- Achieving economic and financial profitability and increasing production and sales.
- Maintaining current customers and attracting new ones.
- Ensuring continuity in order to generate profits.
- Developing investments and optimizing production capacity.

1.1.3. Main Activities of the Company:

Three primary producing operations are carried out by the Phosphate Mines Company:

The largest phosphate deposit in Algeria is located in the Djebel Onk region in southeastern Algeria, with estimated reserves of 2 billion tons. Phosphate processing is carried out through two methods, Wet washing process., Dry process for dust removal.

The company produces four types of phosphate with different BPL levels. The current production is estimated at 1 million tons. Exported phosphate is the main product of the company, which is transformed by other countries into phosphoric acid and fertilizers. Raw phosphate consists of fossil remains and marine bones. The four types have the same components but differ in their composition ratios.

The company relies mainly on phosphate, as it represents approximately 51% of its total revenue.

1.1.3.1. DO20 Phosphate :

During the production process, a by-product called DO20 is generated. It is a residue of the production process. Djebel Onk phosphate is characterized by high porosity and solubility in weak organic acids. DO20 is used as a soil conditioner for saline, acidic, and sandy soils, and as a fertilizer for agricultural use.

1.1.3.2. Current Efforts in Phosphate Extraction and Processing:

In response to economic, financial, and technological developments, the company works to maintain its position in the market and attract new customers through a strategic approach based on partnerships and contracts.

1.1.4. Organizational Structure (Overview):

The organizational structure of the company includes the Chief Executive Officer (CEO), who is the head of the company and represents the highest level of responsibility. His main tasks include:

- Achieving the company's objectives and plans.
- Implementing the decisions of the Board of Directors.
- Presiding over management meetings and following up on their implementation.
- Managing employee-related issues and ensuring workplace health and safety.
- Supervising the general management of the company.
- Approving budget management strategies.

1.2. Organizational Structure of Somiphos Phosphate Company:

1.2.1. Directorates, Departments, and Units in Place:

After its separation from Fer Phos, Somiphos established an organizational structure that aligns with its operational requirements and helps its supervisors perform their duties efficiently. The structure is integrated to ensure the effective completion of tasks, as follows:

- First Level: Includes the Directorates.
- Second Level: Includes the Departments.
- Third Level: Comprises the Units.

The organization has four main directorates, in addition to the Applied Research and Development Center, the Djebel onk mine complex, and the Annaba port facilities. These will be presented in the following table:

Table 1: Somiphos departments

Directorate	Service
Accounting Department	- Supervised by the Finance and Accounting Directorate. - Handles the organization's accounting affairs and oversees a unit responsible for analytical accounting, namely the Analytical Accounting Unit.
Finance Department	- Also supervised by the Finance and Accounting Directorate.

	- Responsible for executing the organization's various financial operations and works in coordination with the Accounting Department. - Comprises two units: the Treasury Unit and the Collection Unit
Export Department – Zone 1	Handles all export operations, including the preparation and execution of orders for customers located in Zone 1, which primarily includes European countries.
Export Department – Zone 2	Handles export operations related to Zone 2, which includes countries in Asia and Latin America (generally the new markets).
Customer Relations Department	Its main mission is to maintain existing customers and work on developing, growing, and strengthening relationships with them while meeting their needs. Continuously seeks to acquire new clients. Oversees the conclusion of agreements and contracts with clients.
Equipment Procurement Department	Responsible for acquiring various supplies and equipment, including furniture, office supplies, machinery, tools, and other equipment, as well as maintaining existing equipment and machinery. Supervised by the Trade Directorate, which ensures the provision of the necessary production equipment for the directorate's activities.
Information Resources Department	Supervised by the Resources Directorate. Its role is to provide, collect, and transmit the necessary information required by the organization, whether internal (related to the organization) or external (related to its environment). Ensures the flow of information between different units within the organization. Responsible for creating communication channels between the organization and its stakeholders.
Training Department	Subordinate to the Resources Directorate, it oversees the continuous training of the organization's human resources to improve performance and increase productivity. Organizes training courses to qualify employees. Recently, it conducted an English language training course for all administrative staff to enhance

	their skills due to the increasing use of English in interactions with various clients, especially new ones.
Legal Affairs Department	Handles the organization's legal matters, ensuring that all its activities have legal validity. Resolves various issues and disputes that may arise between the organization and other parties.

Source: Information provided by the IT department of tebessa phosphate company

In addition, there is another organizational framework represented by secretariats, with one secretariat at each directorate, providing necessary support to the directorate.

The organization also has a dedicated department for quality management, overseeing the quality of the company's products while considering environmental factors and global quality standards. Somiphos has obtained the ISO certification, demonstrating the international excellence of its operations.

Furthermore, the organization is equipped with security, technical, and communications units, all working in an integrated manner to ensure the smooth functioning of the company's activities.

Table 2 presents the different departments under the Finance and Accounting Directorate, highlighting their main tasks and their role in managing the organization's financial and accounting operations

Table 2:Departments under the finance and accounting directorate

1	Detailed tasks of the Finance and Accounting Directorate	Supervision
Finance and Accounting Directorate	- Budget: Prepare and plan; monitor execution. - Accounting & Reporting: Manage accounts; produce financial reports. - Asset Management: Oversee inventory and maintenance. - Financial Control: Monitor expenses and revenues.	- She supervises all accounting operations and the financial affairs of the organization. - It includes two main departments: the Accounting Department and the Finance Department.

	- Financing & Collection: Handle funding and collect dues.	

Source: Information provided by the IT department of tebessa phosphate company

Table 3 illustrates one of the key departments within the Finance and Accounting Directorate, namely the Accounting Department, by outlining its main functions and internal structure:

Table 3:finance and accounting directorate-departments

2	Their Functions	Supervision
Accounting Department	- Responsible for the organization's accounting affairs and oversees a unit that handles related matters - It includes two units: the Treasury Unit and the Collection Unit.	- Supervised by the Finance and Accounting Directorate.

Source: Information provided by the IT department of tebessa phosphate company

Table 4 presents the Resources Directorate by explaining its main role in managing the organization's resources, as well as its different departments:

Table 4: Departments of the human resources directorate

3	Supervision	Its branches
Resources Directorate	It oversees the organization's resources of various types and works to provide them in a manner that meets the requirements of the organization's functions.	It is divided into four departments: - Information Resources Department - Legal Affairs Department - Training Department - Human Resources Department

Source: Information provided by the IT department of tebessa phosphate company

Table 5 presents the Information Resources Department by outlining its main functions, particularly in managing information systems, ensuring data security, and supporting decision-making within the organization:

Table 5: Departments of the information technology directorate

4	Main Functions	Supervision

Information Resources Department	Managing databases and information systems (MIS) to support different departments. Ensuring information security through protection measures such as firewalls and antivirus systems. Providing technical support and maintenance for hardware and software. Digitalizing processes to improve efficiency and reduce costs. Supplying management with reports, budgets, and schedules to support decision-making. Developing networks and communication systems within the organization.	It is supervised by the Resources Directorate.

Source: Information provided by the IT department of tebessa phosphate company

1.2.2. Phosphate – Ils Tsks :

- Achieve the set goals and plans.
- Implement the orders and directives of the Board of Directors.
- Chair directorate meetings and follow up on the implementation of their resolutions.
- Manage employee affairs and ensure workplace health and safety.
- Oversee the general administration of the organization.
- Approve strategies related to budget management.
- Maintain direct communication with higher authorities as the company's main representative abroad.

1.2.3. Responsibilities of the Resources Directorate:

- Develop the company's strategies in human resources management.
- Prepare training plans, recruitment plans, and career path plans.
- Supervise the staff units of the company's subsidiaries and coordinate between them.
- Draft the company's internal regulations and prepare periodic reports to be presented to the General Manager.

Marketing Directorate: This directorate is responsible for the following:

Marketing Directorate – Responsibilities:

- Market the phosphate products according to the planned program.
- Search for new markets and clients to distribute the company's products.
- Study changes in global markets and adapt accordingly.
- Ensure customer satisfaction by meeting their needs.
- Receive international delegations and clients.
- Prepare periodic reports and submit them to the executive management.

Accounting and Finance Directorate – Responsibilities:

- Perform various accounting tasks at the company level.
- Prepare accounting plans and annual financial summaries.
- Prepare the annual budget.
- Manage financial operations and monitor banking activities.
- Conduct necessary financial studies and analyses.

1.3. Key Cultural Values at Somiphos Phosphate Company (Somiphos):

Key Cultural Values at Somiphos Phosphate Company (Somiphos):

- Conduct regular performance evaluations for managers and provide corrective measures when necessary to fully satisfy customers.
- Implement policies for continuous skill renewal and training for employees at all levels, resulting in a highly qualified workforce.
- Consider creativity as a cornerstone of success, always seeking innovation to adapt to internal and external environmental changes.
- Prioritize customer care as a key factor for the company's sustainability.
- Respond quickly and continuously to competitive pressures.
- Rely on a communication system that allows free exchange of ideas and information among employees.
- Promote teamwork and participation to achieve tasks efficiently.
- Introduce modern systems and devices to keep up with changes.
- Follow streamlined policies and procedures to facilitate daily work.
- Focus on adapting to the surrounding environment and new realities.
- Listen to employees, consider their suggestions, and continuously invest in their training and development.
- Provide support and dedicate time, effort, and resources to development projects and attract highly skilled professionals.

2. Description of the Accounting System Used at SOMIPHOS (Sage 100c):

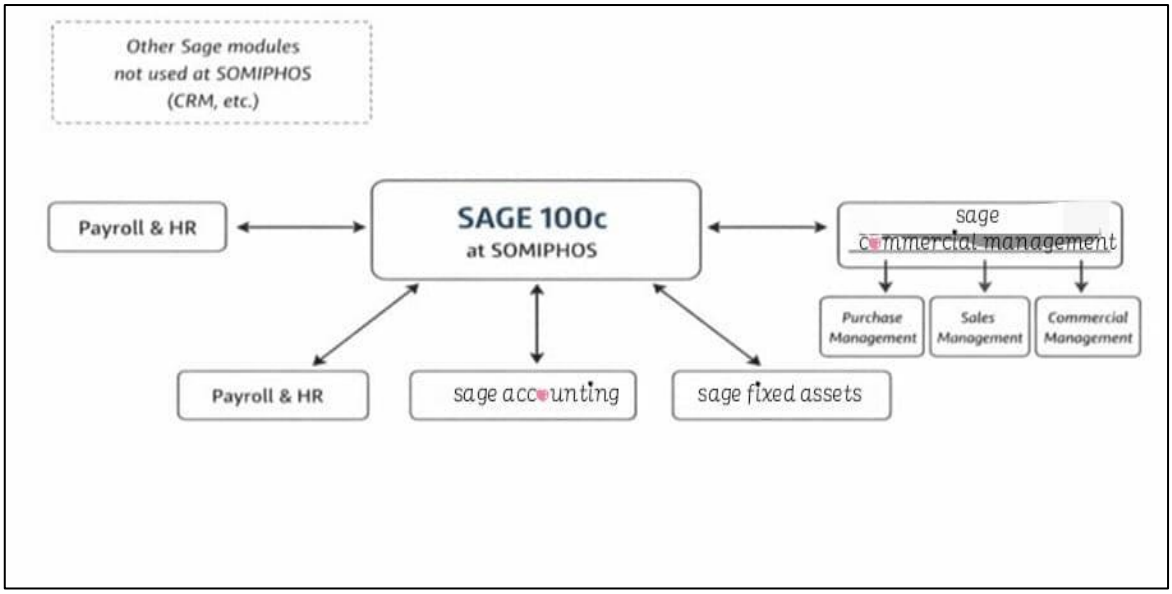
The accounting and financial management of a company requires the use of reliable tools capable of ensuring the recording, processing, control, and presentation of accounting and administrative information. In this context, SOMIPHOS relies on an integrated management solution based on Sage 100c, which is one of the most widely used software packages in the field of accounting, human resources, payroll, and commercial management. This system allows the company to manage its various operations in a computerized environment while ensuring the consistency and security of financial and administrative data.

The implementation of Sage 100c at SOMIPHOS reflects the company's commitment to modernizing its management methods and replacing manual procedures with digital tools that improve productivity, accuracy, and traceability.

The software enables the processing of daily accounting transactions, the management of payroll and human resources data, the monitoring of fixed assets, and the supervision of commercial operations such as purchases and sales. Through this integrated system, the different departments of the company can work with structured and reliable information.

The following figure presents the main modules of the Sage 100C system used at SOMIPHOS, highlighting the different functional components that contribute to managing accounting and administrative operations within the company.

Figure 2:Main sage 100c modules used at SOMIPHOS



Source: Information provided by the IT department of tebessa phosphate company

It is important to note that Sage 100c offers a wide range of modules adapted to different business functions. However, not all of these modules are used at SOMIPHOS. The company mainly uses the modules related to Payroll and Human Resources, Accounting, Fixed Assets, and Commercial Management. Other modules offered by Sage, such as CRM, exist within the Sage environment but are not currently used by SOMIPHOS.

This section presents the accounting system used at SOMIPHOS through Sage 100c. It first describes the main modules implemented in the company, then explains the methods used for data processing, and finally analyzes the interface and practical use of the system.

2.1. System Modules:

Sage 100c is composed of several specialized modules designed to manage the main administrative, financial, and commercial activities of an organization. At SOMIPHOS, the modules effectively used are Payroll and Human Resources, sage accounting, Sage Fixed assets, and Sage Commerciale management. These modules are interconnected and allow the circulation of information between the various functions of the company.

Table 6:sage 100c modules used at SOMIPHOS and their functions

Module	Main Function	Example of Use at SOMIPHOS
Payroll & HR	Employee and salary management	Payroll processing, employee records
Sag accounting	Accounting processing	Journal entries, ledgers, statements
Fixed assets	Fixed asset management	Asset registration, depreciation
Sage Commercial Management	Commercial operations	Purchases, sales, commercial documents

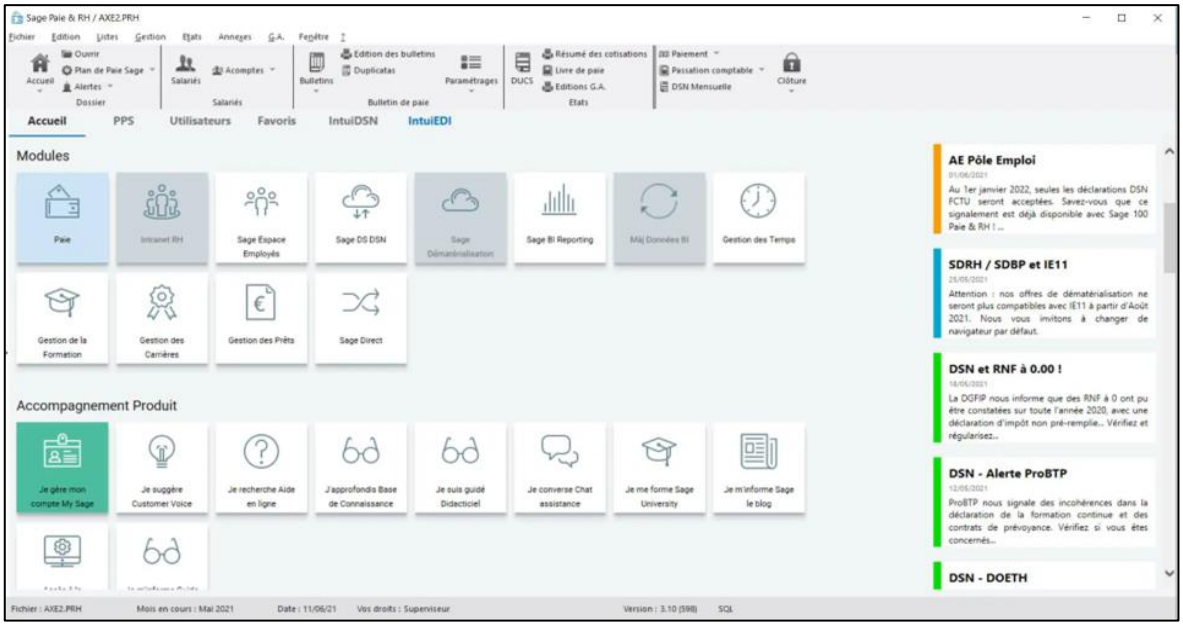
Source: Information provided by the IT department of tebessa phosphate company

2.1.1. Payroll and Human Resources Module:

One of the most important modules used at SOMIPHOS is the Payroll and Human Resources module. This module is dedicated to the management of employee information and the preparation of payroll. It plays a central role because human resources management is closely linked to financial management and accounting operations.

The Human Resources aspect of the module allows the company to maintain and update employee records. Each employee has an administrative file containing personal and professional information such as identification data, job position, department, recruitment date, family situation, salary category, and other information necessary for personnel administration. This digital management of employee records facilitates the organization and retrieval of HR data.

Figure 3:Payroll and human resources module in the sage system



Source: Information provided by the IT department of tebessa phosphate company

information, department, job position, recruitment date, family situation, salary category, and other information necessary for personnel administration. This digital management of employee records facilitates the organization and retrieval of HR data.

The payroll aspect of the module enables the calculation of salaries and the preparation of payroll documents. It takes into account the different elements of remuneration, such as the basic salary, allowances, bonuses, indemnities, deductions, social contributions, and taxes. Through this computerized process, payroll calculations are performed more rapidly and with greater precision than in a manual system.

Another important function of this module is the generation of payroll outputs. It allows the production of payroll slips, payroll summaries, declarations related to social and fiscal obligations, and other documents required for administrative and financial follow-up. In addition, payroll data can be transferred to the accounting module, which ensures consistency between salary expenses and accounting records.

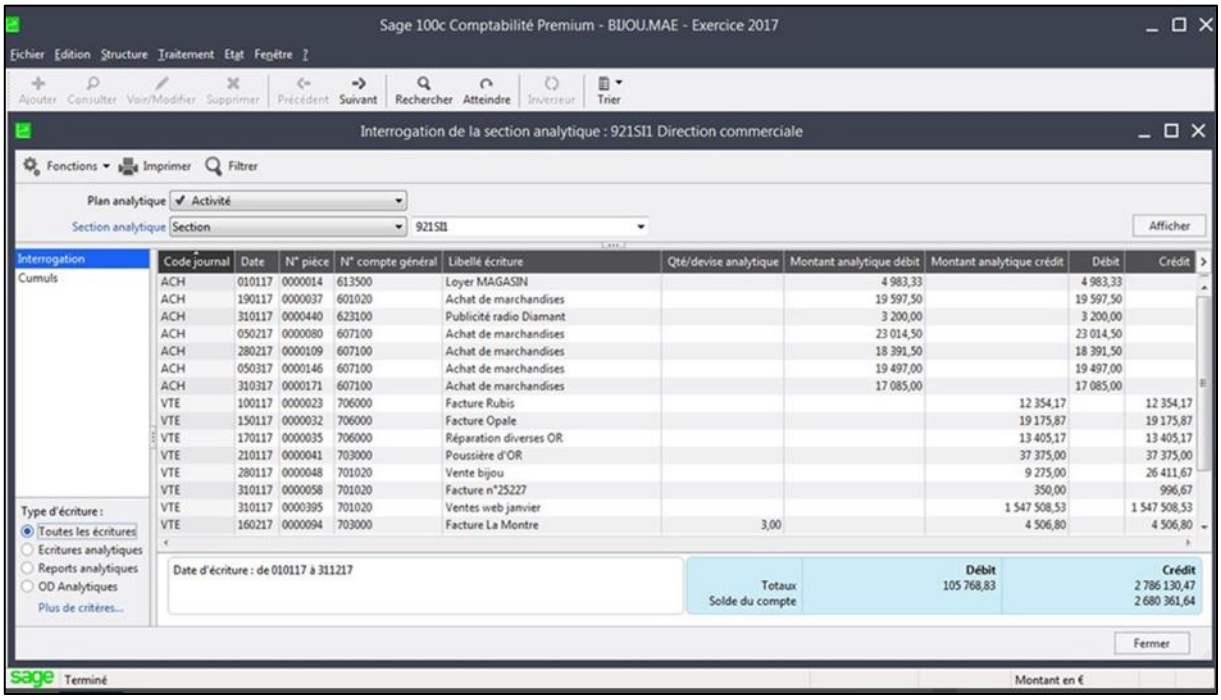
Thus, the Payroll and Human Resources module contributes not only to the management of employees but also to the reliability of financial information related to personnel expenses, which often represent a significant part of company costs.

2.1.2. Sage accounting module :

The Sage accounting module is the central component of the accounting system used at SOMIPHOS. It is through this module that the company records, classifies, and processes its accounting operations. It forms the basis of financial management and ensures that all accounting transactions are recorded according to accounting principles and regulatory requirements.

This module allows the management of the chart of accounts used by the company. Each accounting account is identified by a code and a label, which facilitates the classification of operations according to their nature. Through this structure, the company can distinguish assets, liabilities, expenses, revenues, and other accounting elements.

Figure 4:accounting transactions interface in the sage system



Source: Information provided by the IT department of tebessa phosphate company

Sage accounting is also used for recording daily accounting transactions. These transactions include supplier invoices, customer invoices, payments, receipts, bank operations, cash operations, adjustment entries, and other accounting movements. The software allows entries to be recorded

in specialized journals such as purchase journals, sales journals, bank journals, cash journals, and miscellaneous operation journals.

The automation provided by Sage accounting is particularly important. Once entries are validated, the system updates account balances automatically, posts data to the ledger, and prepares summaries such as the trial balance. This reduces the risk of human error and improves the speed of accounting processing.

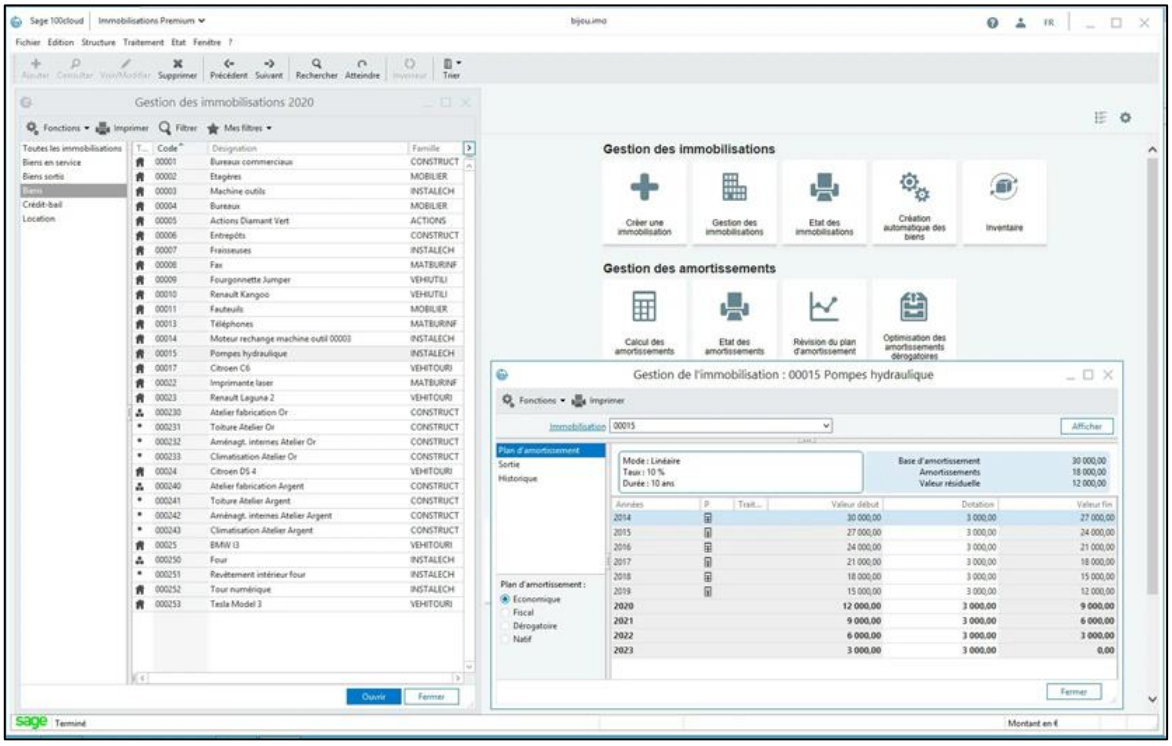
The module also supports the preparation of accounting and financial documents. It makes it possible to generate the general ledger, trial balance, journal reports, and financial statements. These outputs are necessary for management, control, audit, and statutory reporting purposes.

Therefore, Sage accounting constitutes the core of the accounting information system at SOMIPHOS. It ensures the processing and monitoring of financial operations in a structured and secure digital framework.

2.1.3. Sage fixed assets module :

The Sage fixed assets module is used at SOMIPHOS for the management of fixed assets Since the company owns important material and industrial assets, the management of fixed assets is an essential function within the accounting system.

Figure 5:Fixed assets management interface in the sage system



Source: Information provided by the IT department of tebessa phosphate company

This module allows the registration and tracking of all immobilized assets owned by the company. These may include buildings, industrial equipment, vehicles, furniture, computer equipment, and other long-term assets used in the company's activities. For each asset, the system stores information such as the identification code, description, acquisition date, acquisition value, depreciation method, useful life, and current status.

One of the main advantages of Sage fixed assets is the automation of depreciation calculations. The software makes it possible to calculate depreciation according to the accounting rules and parameters defined for each asset. These calculations are essential for determining the annual depreciation expense and the net book value of fixed assets.

The module also facilitates the management of asset movements and events. It can record acquisitions, transfers, disposals, revaluations, and other modifications affecting the fixed asset portfolio. This ensures better visibility over the life cycle of assets and strengthens control over company property.

Another important aspect is the integration with accounting. Depreciation expenses and asset-related entries can be transferred to Sage accounting, this ensuring consistency between fixed asset management and general accounting records. This integration is particularly useful for preparing

financial statements and for ensuring that asset-related accounting information is accurate and up to date.

Consequently, Sage fixed assets helps SOMIPHOS manage its fixed assets in a more precise and organized way, while ensuring compliance with accounting requirements.

2.1.4. Sage Commercial Management Module :

Another major component used at SOMIPHOS is Sage sales management. This module is dedicated to the management of commercial operations and plays an important role in the circulation of information between operational management and accounting management.

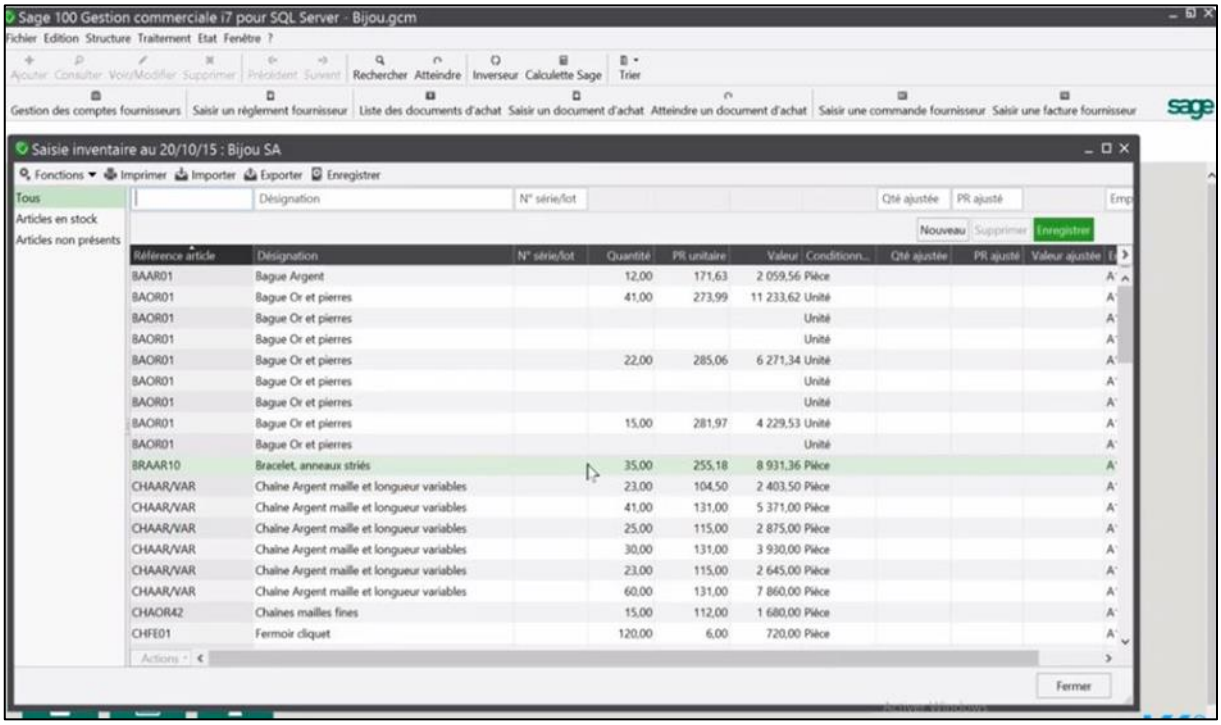
At SOMIPHOS, Sage commercial management includes three major areas:

- purchase management,
- sales management,
- commercial management in the broader sense.

2.1.4.1. Purchase Management :

The purchase management function allows the company to manage supplier-related commercial operations. It supports the recording and follow-up of purchase transactions such as purchase requests, supplier orders, delivery tracking, and supplier invoices. Through this function, the company can better supervise expenditure flows and monitor commitments toward suppliers.

Figure 6:Inventory management interface in the sage commercial module



Source: Information provided by the IT department of tebessa phosphate company

This part of the module helps ensure better organization of procurement operations. It allows the retrieval of information related to suppliers, purchased products or services, quantities, prices, and due dates. It also contributes to improving traceability and internal control over purchase operations.

2.1.4.2. Sales Management :

The sales management function is used to manage customer-related commercial operations. It covers the recording of sales transactions, customer orders], deliveries, invoices, and the follow-up of receivables. This function enables the company to have a clear view of its commercial activity and to ensure the consistency of sales information.

Sales management also facilitates the preparation of commercial documents such as quotations, order forms, delivery notes, and invoices. Once these operations are validated, the related data can be transferred to the accounting system. This integration reduces duplication in data entry and improves the reliability of financial information linked to revenues.

2.1.4.3. Commercial Management :

Beyond purchases and sales, Sage Gestion Commerciale provides a broader framework for managing commercial flows. It centralizes commercial information, facilitates transaction

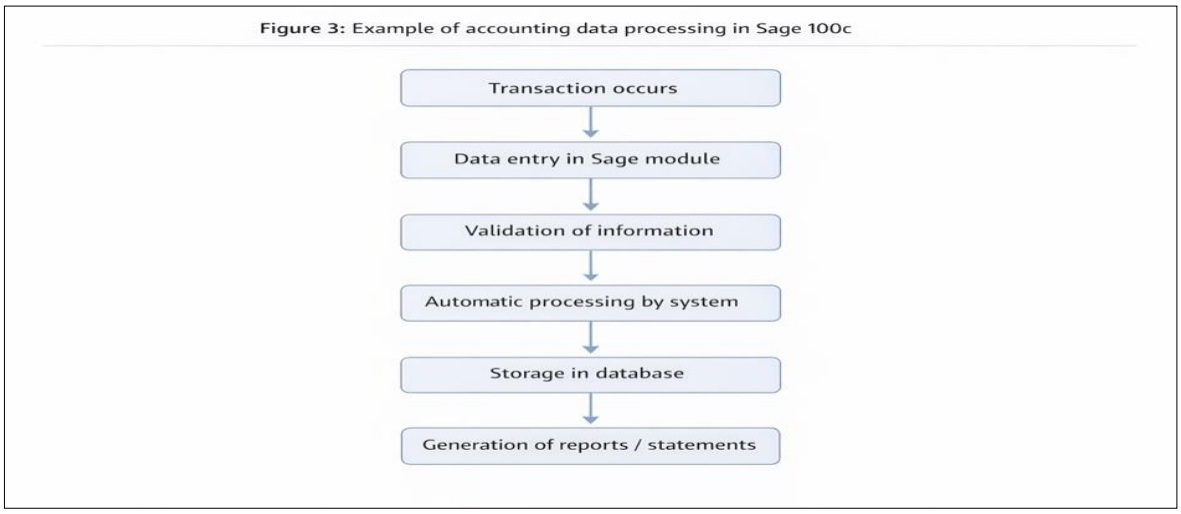
monitoring, and contributes to the preparation of commercial reports. It therefore acts as an interface between operational commercial activities and accounting processing.

The use of this module at SOMIPHOS strengthens the link between commercial transactions and accounting records. Purchases and sales carried out within Sage Gestion Commerciale generate information that can later be integrated into accounting processing, thereby ensuring coherence across the management system.

2.2. Data Processing Methods:

The effectiveness of the Sage 100c system at SOMIPHOS does not depend only on the modules used, but also on the way data is processed. Data processing within the system is based on computerized methods that ensure the registration of operations, the automatic treatment of information, and the secure storage of data.

Figure 7:Example of accounting data processing sage 100c



Source: Information provided by the IT department of tebessa phosphate company

2.2.1. Recording Daily Transactions :

The recording of daily transactions is one of the fundamental functions of the Sage system. At SOMIPHOS, daily operations are entered into the system according to their nature and according to the module concerned.

In the accounting module, daily transactions include supplier invoices, customer invoices, cash and bank movements, payments, receipts, and various adjustment entries. These transactions are recorded in appropriate journals and classified according to accounting rules.

In the Payroll and Human Resources module, the data entered may concern employee information, payroll variables, allowances, deductions, and attendance or administrative data necessary for salary preparation.

In the Sage fixed assets module, the recorded data may concern asset acquisitions, depreciation parameters, asset transfers, disposals, or other fixed asset events.

In Sage Commerciale management, daily transactions relate to purchases, sales, supplier operations, customer operations, quotations, orders, delivery notes, and invoices.

This recording of daily operations in a digital system improves accuracy, speeds up the processing of information, and facilitates later consultation of recorded transactions.

2.2.2. Digital processing of accounting and administrative data:

Once data is entered into Sage 100c, the software processes it digitally. This means that the system automatically classifies, calculates, updates, and organizes the information according to predefined rules.

For example, when an accounting entry is validated in Sage accounting, the system posts it automatically to the relevant accounts and updates the balances. In the payroll module, the software calculates salary amounts, deductions, contributions, and net pay. In the fixed asset module, it calculates depreciation and updates asset values. In the commercial management module, it processes purchase and sales information and prepares commercial documents.

This digital processing reduces the workload associated with manual calculations and minimizes the risk of error. It also allows the company to obtain updated information in real time, which improves decision-making and financial monitoring.

2.2.3. Storage and management of information in system databases:

The storage of data in system databases provides several advantages. It allows the secure conservation of large volumes of information, facilitates the retrieval of historical records, and improves traceability. It also supports the generation of reports and financial statements based on reliable and centralized information.

At SOMIPHOS, this digital storage contributes to better organization of accounting and administrative records. Instead of relying only on manual archives, the company can access structured information through the system, which improves operational efficiency.

2.2.4. Reliability, Security, and Traceability of Data:

Another important feature of data processing in Sage 100c is the reliability and security of information. The system ensures that data is entered, processed, and stored according to authorization levels and internal control procedures.

Users generally access the modules according to their functions. this limits unauthorized access to sensitive financial or HR information. In addition, the system keeps a trace of operations performed, which strengthens transparency and accountability.

Through these mechanisms, SOMIPHOS benefits from a more secure and controlled accounting information system, capable of supporting both operational activities and managerial oversight.

2.3. System Interface and Usage:

The usefulness of Sage 100c at SOMIPHOS also depends on the way users interact with the system. The software provides an interface through which employees can enter data, retrieve information, generate reports, and print documents necessary for accounting and administrative management.

2.3.1. Data Entry Procedures:

The data entry procedures in Sage 100c depend on the module being used. However, in general, the user begins by accessing the software through an authentication process. Once connected, the user chooses the relevant module according to the task to be performed.

In Sage accounting, the user enters accounting entries through dedicated journals and forms. In the Payroll and Human Resources module, the user updates employee records and payroll variables. In Sage fixed assets, the user records fixed asset details and related operations. In Sage Gestion Commerciale, the user enters purchase and sales data through commercial documents and transaction forms.

The interface generally includes structured fields, menus, lists, and validation functions. These elements guide the user during data entry and reduce the risk of incomplete or incorrect input. Therefore, the system facilitates standardized and controlled entry of financial and administrative data.

2.3.2. Information Retrieval Methods :

Sage 100c enables users at SOMIPHOS to retrieve information in a fast and organized way. Users can search for information by reference, date, account, employee, supplier, customer, asset code, or transaction type.

For example, the accounting department may retrieve journal entries, account balances, ledgers, or trial balances. The HR department may retrieve employee records and payroll summaries. The fixed asset manager may consult the list of immobilizations, depreciation schedules, and asset histories. Commercial users may retrieve supplier documents, sales invoices, and transaction histories.

This retrieval functionality is essential because it allows the company to use recorded data not only for registration purposes but also for control, analysis, and decision-making.

2.3.3. Report Generation :

One of the major strengths of Sage 100c is the ability to generate reports. At SOMIPHOS, the software can produce accounting, payroll, asset, and commercial reports depending on the module used.

Sage accounting can generate documents such as the general ledger, journal reports, trial balance, and financial statements. The Payroll and Human Resources module can generate payroll slips, payroll summaries, and administrative reports related to employees. Sage fixed assets can provide fixed asset lists, depreciation tables, and asset movement reports. Sage Gestion Commerciale can produce purchase reports, sales reports, invoice lists, and other commercial summaries.

These reports are useful for internal management, financial control, auditing, and administrative follow-up. They also help managers obtain a global view of company operations.

2.3.4. Printing of Financial Statements and Management Documents:

In addition to on-screen consultation, Sage 100c allows the printing of reports and statements. This function remains important for documentation, archiving, managerial review, and formal administrative use. At SOMIPHOS, printed outputs may include accounting statements, payroll slips, fixed asset reports, purchase and sales documents, and financial summaries. The possibility of printing these documents provides support for both operational work and compliance with internal or external requirements.

2.3.5. Practical Usefulness of the Interface:

The interface of Sage 100c contributes to the effectiveness of the system because it provides users with a structured and organized work environment. It simplifies daily operations, accelerates data entry and retrieval, and improves the quality of generated documents.

For SOMIPHOS, this means that the accounting and administrative departments can work more efficiently, with better control over information and improved coordination between functions such as accounting, payroll, fixed asset management, purchases, and sales.

The accounting system used at SOMIPHOS is based on Sage 100c, an integrated management solution that supports the company's accounting, administrative, HR, fixed asset, and commercial activities. The main modules effectively used by the company are the Payroll and Human Resources module, Sage accounting, Sage fixed assets, and Sage Commerciale management, the latter including purchase management, sales management, and commercial management. Other modules offered by Sage, such as CRM, exist but are not currently used at SOMIPHOS.

The use of these modules enables the company to record daily transactions, process accounting and administrative data digitally, store information securely in system databases, and generate reliable reports and financial statements. The Sage 100c interface further facilitates data entry, information retrieval, and document printing.

Overall, Sage 100c plays a central role in the modernization of management at SOMIPHOS. It improves the reliability of information, strengthens internal control, and supports the company in its transition toward more efficient and digitalized management practices.

3. Technical and Security Aspects of the System (Sage 100c):

The use of an integrated management system such as Sage 100c does not only improve the performance of accounting, payroll, fixed asset, and commercial operations, but also raises important technical and security considerations. Since the system manages sensitive financial, administrative, and human resources information, its reliability depends on the existence of appropriate security mechanisms capable of protecting data against unauthorized access, loss, alteration, and misuse.

At SOMIPHOS, Sage 100c is used as a digital platform for processing accounting and administrative information. Consequently, the protection of this system is essential for ensuring the confidentiality, integrity, and availability of data. Security in such a context involves both

technical measures, such as password protection, access rights, encryption, and backup procedures, and organizational measures, such as internal controls and user supervision. Without these protections, the system could become vulnerable to accidental errors, misuse, or malicious actions that might affect the quality and credibility of accounting information.

This section presents the technical and security aspects of the Sage 100c system. It first examines the security measures applied to protect access and data, then analyzes the role of internal controls in preserving information integrity, and finally discusses the risks and vulnerabilities associated with system use.

Table 7:main security and cyber security measures related to sage 100c

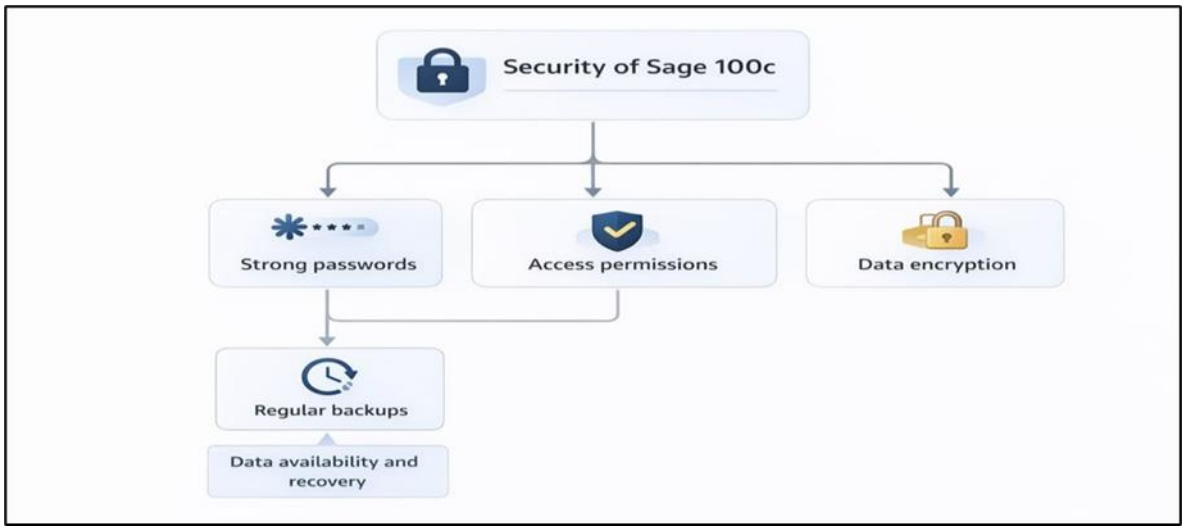
Measure	Objective	Expected Result
Strong passwords	Protect access	Reduce unauthorized access
Access permissions	Limit user actions	Better internal control
Encryption	Protect confidential data	Better confidentiality
Backups	Ensure recovery	Business continuity
Updates and patches	Correct vulnerabilities	Better system Security
User training	Reduce human error	Better cybersecurity awareness

Source: Information provided by the IT department of tebessa phosphate company

3.1. Security Measures:

The security of Sage 100c is based on a set of preventive and protective measures intended to safeguard the system and the information it contains. These measures concern user authentication, access authorization, data protection, and data backup. In an accounting information system, such safeguards are indispensable because financial and administrative information must remain confidential, accurate, and available whenever needed.

Figure 8:Main security measures protecting sage 100c

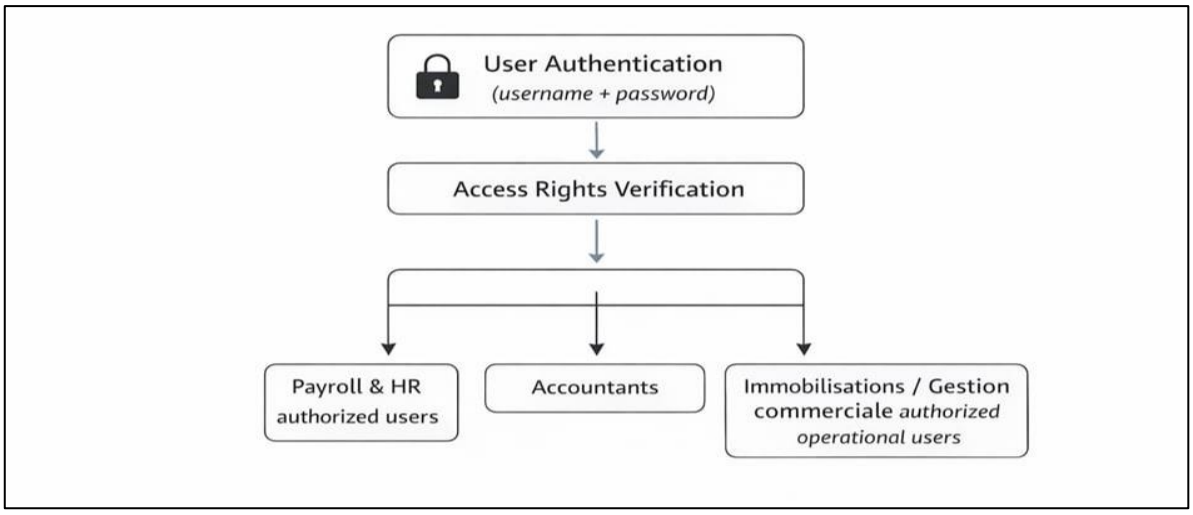


Source: Information provided by the it department of tebessa phosphate company

3.1.1. Implementation of Strong Passwords and Access Permissions:

One of the first levels of protection in Sage 100c is the use of user authentication mechanisms, particularly usernames and passwords. Access to the software is generally restricted to authorized users only. Each employee using the system is assigned credentials that allow access according to their function and responsibilities.

Figure 9:Principle of access control in sage 100c



Source: Information provided by the IT department of tebessa phosphate company

The implementation of strong passwords is essential because weak passwords can expose the system to unauthorized access. A strong password typically combines letters, numbers, and special characters and avoids obvious personal references or predictable combinations. In the context of

Sage 100c, the use of strong passwords reduces the likelihood that unauthorized persons can access sensitive accounting, payroll, or commercial information.

In addition to passwords, Sage 100c relies on access permissions to control user activity inside the system. Not all users should have the same level of access. For example, an HR or payroll officer may need access to the Payroll and Human Resources module, while an accountant may mainly use Sage accounting. Similarly, access to Sage fixed assets or Sage Gestion Commerciale may be limited to employees responsible for those functions. This division of access rights is important because it ensures that each user can only view or modify the information relevant to their role.

Access permissions also contribute to internal security by limiting sensitive operations such as the modification of accounting entries, the validation of payroll, or the management of fixed asset values. By assigning permissions according to responsibilities, the company reduces the risk of intentional misuse or accidental manipulation of critical information.

Therefore, strong passwords and carefully defined access rights constitute the first line of defense for protecting Sage 100c at SOMIPHOS.

3.1.2. Data Encryptions :

Another important security measure in the use of Sage 100c is data encryption. Encryption is a process that transforms data into a protected form so that it cannot be read or exploited by unauthorized persons. In an accounting and administrative environment, this measure is especially important because the system contains confidential data such as payroll records, financial balances, supplier information, customer information, and fixed asset values.

Encryption can be applied during data storage or during data exchange. When data is stored in protected form, the risk of exposure in case of unauthorized access to files or databases is reduced. Likewise, when data is transferred between components of the system or between user stations and servers, encryption helps protect it against interception.

The importance of encryption lies in the fact that accounting and administrative information has both strategic and legal value. Payroll data, for example, contains sensitive personal and financial details related to employees. Accounting data reflects the financial position of the company. Commercial data includes purchase and sales information that may be confidential. For these reasons, protecting such information through encryption strengthens the overall security of the system.

Even when encryption is not always visible to end users, it remains a major technical safeguard that contributes to protecting the confidentiality of the information processed by Sage 100c.

3.1.3. Regular Backups :

Regular backups are another essential security measure associated with Sage 100c. A backup consists of creating copies of system data so that it can be restored in case of loss, corruption, or system failure. Since Sage 100c manages important accounting and administrative information,

the absence of effective backup procedures could lead to serious operational and financial consequences.

The role of backups is to guarantee the continuity of. If the system is affected by hardware failure, software malfunction, accidental deletion, or cyber incident, backup copies can be used to recover the information and resume activity. This is particularly critical in the case of accounting data, because the loss of journal entries, payroll records, or fixed asset data could disrupt financial reporting and administrative processes.

Regular backups also support legal and managerial requirements. Historical accounting data must often be preserved for several years, and backup procedures help ensure that such information remains available over time. In addition, having reliable backup copies reassures management that the information system can withstand incidents without complete data loss.

To be truly effective, backup procedures must be performed on a regular basis and verified periodically. A backup that exists but cannot be restored does not provide real protection. Therefore, the security of Sage 100c depends not only on making backups, but also on ensuring that they are usable and complete.

3.1.4. Importance of Combined Security Measures:

The security measures applied to Sage 100c are more effective when they operate together rather than separately. Strong passwords protect access, permissions limit user actions, encryption protects data confidentiality, and backups preserve data availability. Each of these measures addresses a specific aspect of system security, but together they create a more robust protection framework.

For SOMIPHOS, the implementation of such measures is essential because Sage 100c is at the center of important processes involving accounting, payroll, fixed assets, and commercial

operations. The reliability of the system therefore depends on the existence of these technical safeguards.

3.2. Internal Controls and Information Security:

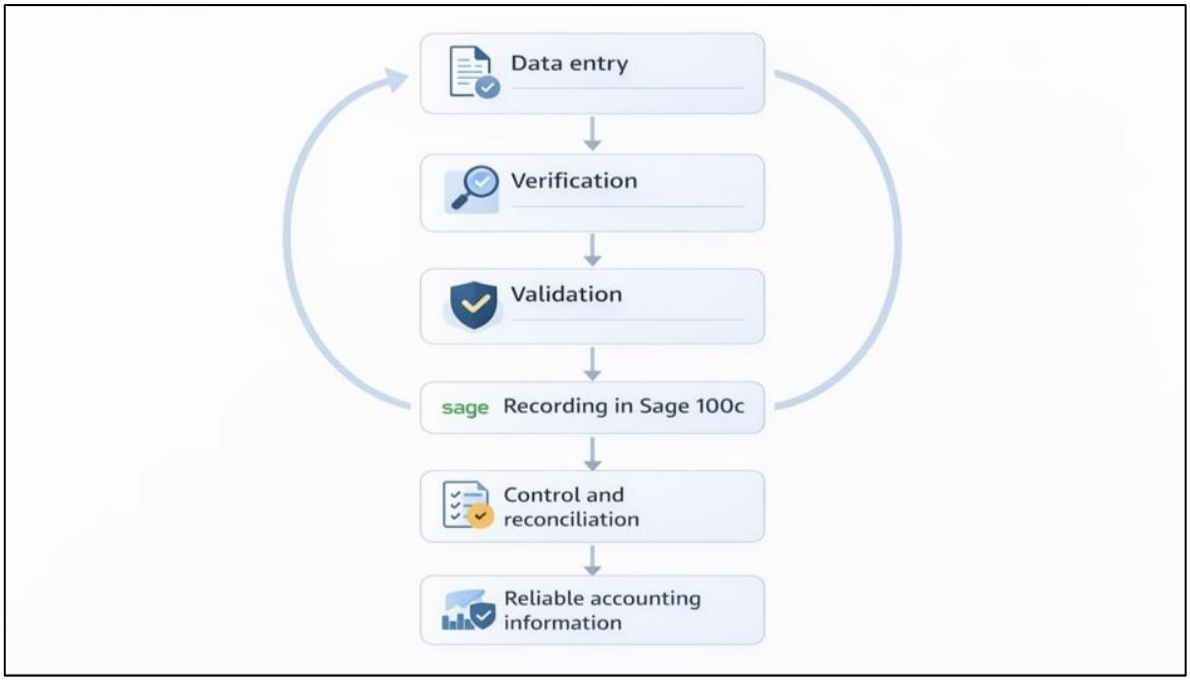
Beyond technical protection, the security of Sage 100c also depends on the existence of internal controls. Internal controls are the procedures, rules, and organizational mechanisms established to ensure that operations are performed correctly, that information remains reliable, and that errors or irregularities are detected in time. In an accounting system, these controls are necessary to maintain data integrity and to protect the company against misuse or operational weaknesses.

3.2.1. Role of Internal Controls in Maintaining Data Integrity:

Data integrity refers to the accuracy, completeness, and consistency of information stored and processed within the system. In Sage 100c, maintaining data integrity is particularly important because the software handles accounting entries, payroll records, fixed asset values, and commercial documents that must be reliable for decision-making and reporting purposes.

Internal controls help maintain this integrity in several ways. First, they establish clear procedures for data entry, validation, and modification. Users are expected to follow defined steps when recording transactions, which reduces the possibility of incomplete or inconsistent information being introduced into the system.

Figure 10:Internal control process ensuring data integrity



Source: Information provided by the IT department of tebessa phosphate company

Second, internal controls can include separation of duties. This principle means that critical tasks should not all be concentrated in the hands of one person. For example, the person who enters an accounting transaction should not always be the same person who validates or authorizes it. In payroll, the preparation of salaries may be separated from their final approval. Such separation reduces the risk of fraud and strengthens the reliability of the process.

Third, internal controls support traceability. Sage 100c can record the actions performed by users, such as data entry, modification, validation, or consultation. This traceability makes it easier to identify the origin of an error or irregularity and encourages greater responsibility in the use of the system.

Finally, internal controls contribute to consistency between modules. Since Sage 100c integrates accounting, payroll, immobilizations, and commercial management, controls are needed to ensure that data transferred from one module to another remains coherent. For instance, payroll data transferred to accounting must reflect the actual payroll processed, and depreciation entries from Sage fixed assets must correspond to recorded asset data.

Thus, internal controls play a central role in ensuring that the information processed through Sage 100c remains reliable and trustworthy.

3.2.2. Procedures for Preventing Unauthorized Access:

Preventing unauthorized access is a major objective of information security. In Sage 100c, access should be limited to users who have a legitimate professional need to use the system. Technical measures such as passwords and permissions are important, but they must be supported by organizational procedures.

These procedures include the creation of individual user accounts rather than shared accounts. Individual accounts allow the company to know exactly who has accessed the system and what operations were performed. This strengthens accountability and reduces anonymity in the use of the software.

Another preventive measure is the periodic review of user rights. Over time, an employee's role may change, or an employee may leave the company. If access rights are not updated accordingly, the system may remain exposed to unnecessary risks. Therefore, internal procedures should ensure that user accounts are regularly reviewed and adjusted.

The use of controlled authorization for critical functions is also important. Certain actions, such as modifying validated accounting records, changing payroll parameters, or altering fixed asset values, should be restricted to authorized personnel only. These controls reduce the likelihood of sensitive data being manipulated without supervision.

In addition, access procedures should include awareness of confidentiality obligations. Users must understand that the information contained in Sage 100c is sensitive and that unauthorized consultation, disclosure, or modification is prohibited. This human dimension is an essential part of information security.

3.2.3. Procedures for Preventing Errors :

Errors represent one of the most common threats to the reliability of an information system. In the case of Sage 100c, user mistakes in data entry, validation, calculation parameters, or reporting can have significant consequences on accounting accuracy and administrative management.

Internal procedures help reduce such risks by establishing controls before, during, and after data entry. Before entry, users should be trained and informed about the correct procedures to follow. During entry, the system may provide validation rules, required fields, and warnings that help detect anomalies immediately. After entry, review and reconciliation procedures allow errors to be identified and corrected.

For example, accounting entries can be checked for balance and consistency before posting. Payroll results can be reviewed before final validation. Fixed asset records can be compared with supporting documents. Commercial operations can be verified against purchase orders, delivery notes, or invoices. These procedures help reduce the risk of inaccurate data affecting the whole system.

Therefore, internal controls are not only aimed at preventing fraud or unauthorized access, but also at minimizing the ordinary mistakes that can arise in daily system use.

3.2.4. Relationship Between Internal Controls and System Security:

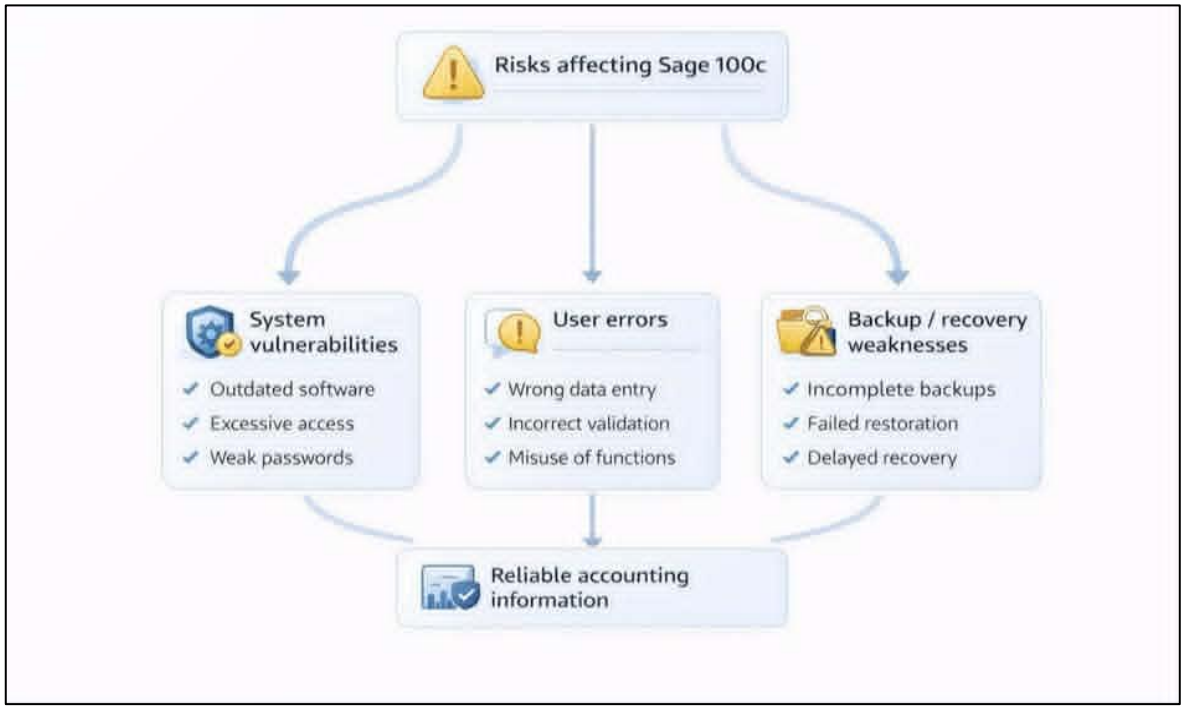
Internal controls and technical security measures are closely related. Technical tools alone cannot guarantee information security if organizational procedures are weak. Likewise, internal procedures are less effective if the system lacks technical safeguards. In Sage 100c, the security of information depends on this combination of technological and organizational protection.

At SOMIPHOS, the role of internal controls is therefore essential for ensuring that Sage 100c remains a reliable accounting and administrative tool. They support the credibility of the data, reinforce system discipline, and reduce the exposure of the company to errors and irregularities.

3.3. Risk Assessment:

Despite the presence of security measures and internal controls, no information system is entirely free of risk. Sage 100c, like any digital system, may face vulnerabilities related to technical weaknesses, user behavior, or insufficient recovery planning. Risk assessment is therefore necessary to identify potential threats and to understand how they may affect system reliability and information security.

Figure 11:Main risks effecting the sage 100c information system



Source: Information provided by the IT department of tebessa phosphate company

3.3.1. Identification of System Vulnerabilities :

A system vulnerability is a weakness that can be exploited or that may lead to failure, data loss, or unauthorized access. In the context of Sage 100c, vulnerabilities may exist at different levels.

One possible vulnerability concerns weak authentication practices. If passwords are too simple, reused, or poorly managed, unauthorized individuals may gain access to the system. This is especially serious in a system that contains payroll, accounting, and commercial information.

Another vulnerability may arise from excessive user privileges. If access rights are not carefully limited, some users may have the ability to consult or modify data beyond their actual responsibilities. This increases the risk of misuse, fraud, or accidental damage.

Technical vulnerabilities may also affect the infrastructure supporting Sage 100c. Hardware failures, software malfunctions, outdated components, or interruptions in the information system environment can compromise data availability and continuity of operations. Since Sage 100c depends on the proper functioning of databases and system resources, any weakness in the technical environment can affect the reliability of the application.

Furthermore, insufficient monitoring of system activity can also be considered a vulnerability. If unusual actions, failed login attempts, or repeated data anomalies are not detected, the company may not identify a problem until it has already affected the integrity of information.

The identification of these vulnerabilities is important because it helps the organization adopt more appropriate protective measures.

3.3.2. Risks Associated with User Errors:

One of the most significant risks in the use of Sage 100c is the risk of user error. Even when the software is technically reliable, incorrect human actions can compromise data quality and system effectiveness.

User errors may occur during data entry. For example, a wrong account code, an incorrect amount, a mistaken date, or the omission of required information may affect the accuracy of accounting records. In payroll, incorrect employee parameters or salary inputs may result in payroll miscalculations. In fixed asset management, an error in depreciation parameters may affect the valuation of immobilizations. In commercial management, mistakes in purchase or sales entries may distort operational and financial reporting.

Another form of user error concerns incorrect interpretation or misuse of system functions. A user may validate a transaction prematurely, modify data without proper verification, or generate reports with unsuitable parameters. Such errors may not always be immediately visible, but they can affect the reliability of outputs and managerial decisions.

The risk of user error is often linked to insufficient training, lack of supervision, work overload, or weak procedural guidance. Therefore, risk reduction requires not only system controls but also adequate user support and clear work instructions.

3.3.3. Weaknesses in Backup and Data Recovery Procedures:

Although backups are an important security measure, weaknesses in backup and data recovery procedures can create major risks for the company. A backup policy may exist in principle, but if it is incomplete, irregular, untested, or poorly organized, it may fail to protect the system when an incident occurs.

One possible weakness is the absence of sufficiently frequent backups. If backups are not performed regularly, recent accounting and administrative data may be lost between two backup cycles. Another weakness concerns storage conditions. If backup copies are not protected properly, they may themselves be damaged, lost, or accessed by unauthorized persons.

A further risk appears when recovery procedures are not tested. In some cases, organizations discover only after a failure that backup files cannot be restored correctly. This transforms what

seemed to be a protection measure into a false sense of security. For a system like Sage 100c, where continuity of accounting and payroll operations is essential, ineffective recovery procedures can have serious consequences.

Weaknesses may also exist when recovery responsibilities are not clearly defined. If no one is specifically responsible for verifying backups and managing restoration procedures, the company may face delays and confusion during a technical incident. This can prolong service interruption and increase operational losses.

Therefore, backup and recovery procedures must be evaluated not only by their existence, but by their actual effectiveness in protecting the continuity of Sage 100c operations.

3.3.4. Overall Importance of Risk Assessment:

Risk assessment is not intended to show that Sage 100c is unreliable, but rather to recognize that every information system requires continuous vigilance. By identifying vulnerabilities, understanding the role of user errors, and evaluating the strength of backup and recovery procedures, the company can improve the resilience of its accounting and administrative system.

For SOMIPHOS, such risk assessment is particularly important because Sage 100c supports critical processes related to payroll, accounting, immobilizations, and commercial management. Any weakness affecting this system may have consequences on operational continuity, financial reporting, and information credibility.

The technical and security aspects of Sage 100c are essential for ensuring the reliability and continuity of the accounting and administrative system used at SOMIPHOS. The implementation of strong passwords, access permissions, data encryption, and regular backups provides an important foundation for protecting the system against unauthorized access, data loss, and misuse.

In addition to these technical measures, internal controls play a major role in preserving data integrity, preventing errors, and reinforcing information security. They ensure that the use of Sage 100c is governed not only by technical safeguards but also by organizational discipline and traceable procedures.

However, the system remains exposed to certain risks, including technical vulnerabilities, user errors, and weaknesses in backup and recovery procedures. For this reason, risk assessment must remain a continuous process aimed at identifying weaknesses and improving system resilience.

Overall, Sage 100c offers a structured and secure environment for managing accounting, payroll, fixed assets, and commercial data, but its effectiveness depends on the proper implementation of both technical safeguards and internal control procedures

3.4. Application of Cybersecurity within the Information System:

The digital transformation of organizations has significantly improved the management of accounting, administrative, and commercial activities. However, this transformation has also increased exposure to cyber threats that may affect the confidentiality, integrity, and availability of information systems. In an environment where financial data, payroll records, fixed asset information, and commercial transactions are processed through digital tools such as Sage 100c, cybersecurity becomes an essential component of system management.

At SOMIPHOS, the information system based on Sage 100c supports important functions such as accounting, payroll and human resources, fixed asset management, and commercial management. Since these modules process sensitive and strategic information, the application of cybersecurity measures is necessary to protect the system against unauthorized access, malicious actions, accidental data loss, and operational disruption. Cybersecurity is therefore not limited to technical protection only; it also includes preventive practices, monitoring activities, and user awareness aimed at ensuring the security of information over time.

The practical application of cybersecurity within the information system involves several complementary measures. These include the regular updating of software and systems, the monitoring of system activities, and the training of users in good cybersecurity practices. When such measures are implemented effectively, they produce important positive outcomes, including the protection of financial information and the strengthening of data reliability. At the same time, the analysis of cybersecurity application allows the formulation of recommendations that can help improve the level of security within the organization.

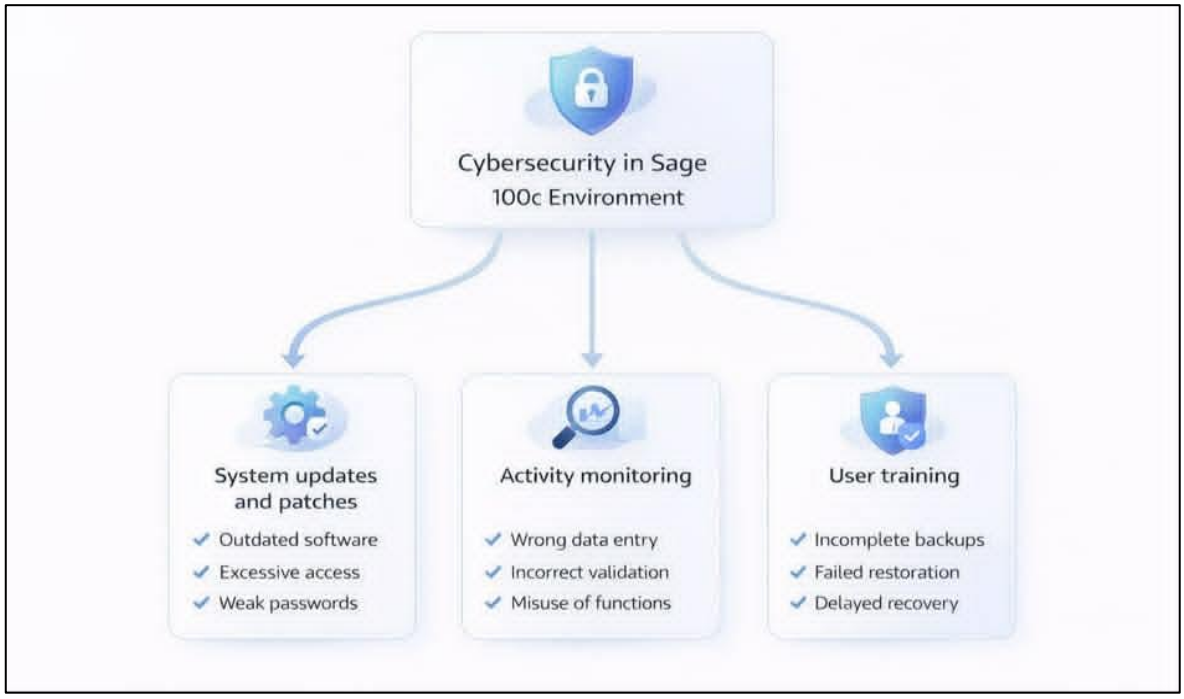
This section presents the practical application of cybersecurity within the information system used at SOMIPHOS. It first discusses the main practical security measures, then explains the outcomes of implementing these measures, and finally proposes recommendations for enhancing information security.

3.4.1. Practical Security Measures :

The practical application of cybersecurity in an information system depends on the adoption of concrete and continuous measures that reduce exposure to cyber risks. In the case of Sage 100c

and the related information system used at SOMIPHOS, these practical measures concern software maintenance, activity monitoring, and user training. Such measures are necessary because cyber threats may arise from technical weaknesses, malicious attempts, or human error.

Figure 12:Application of cyber security measures within the sage 100c environment



Source: Information provided by the IT department of tebessa phosphate company

3.4.2. Regular System Updates and patches:

One of the most important practical cybersecurity measures is the regular installation of system updates and patches. Software systems, including management applications, operating systems, and supporting infrastructure, may contain vulnerabilities that can be exploited if they are not corrected in time. Updates and patches are therefore necessary to close known security gaps and improve the stability of the system.

In the context of Sage 100c, regular updates help maintain the security and proper functioning of the modules used by SOMIPHOS, such as Sage accounting, Sage fixed assets, Payroll and Human Resources, and Sage Gestion Commerciale. By applying updates, the organization reduces the likelihood that attackers can exploit outdated software components. This is particularly important because the information handled by the system includes sensitive accounting and administrative data.

Regular patching also contributes to operational reliability. Beyond security correction, updates may improve performance, correct technical malfunctions, and strengthen compatibility between

software components. Thus, maintaining an updated environment is both a security measure and a technical management practice that supports system continuity.

However, the effectiveness of updates depends on their regularity and control. Delayed or ignored patches may leave the system exposed for a long period. For this reason, cybersecurity within the information system requires an organized process for monitoring software versions and applying necessary updates.

3.4.2.1. Monitoring of System Activities to Detect Suspicious behavior:

Another practical security measure is the monitoring of system activities. Monitoring consists of observing and reviewing the operations carried out within the information system in order to detect abnormal or suspicious behavior. In an environment where many users interact with Sage 100c, activity monitoring is essential for identifying possible security incidents.

Suspicious behavior may take different forms. It may involve repeated failed login attempts, unusual access outside normal working patterns, unauthorized attempts to consult restricted data, unexpected modifications of accounting records, or unusual activity in payroll and commercial data. If such behavior is not detected in time, it may compromise the confidentiality or integrity of the information stored in the system.

Monitoring also contributes to accountability and traceability. By keeping a record of user actions, the organization can know who performed a specific operation, when it was done, and in what context. This is useful not only for detecting malicious activity but also for investigating errors and reinforcing discipline in system use.

In practice, system monitoring should not be viewed as a one-time action but as a continuous process. Cyber security threats can evolve rapidly, and abnormal signs may appear at any time. Therefore, regular supervision of activities related to Sage 100c and the surrounding infrastructure is an important safeguard for the information system at SOMIPHOS.

3.4.2.2. User Training on cybersecurity Best Practices:

Cyber security within an organization cannot rely only on technical protections. The human factor is equally important, because users themselves may either strengthen security or become a source of vulnerability. For this reason, user training on cybersecurity best practices is considered one of the most practical and effective security measures.

At SOMIPHOS, employees using Sage 100c handle accounting, payroll, fixed asset, and commercial information. If they are not sufficiently aware of cybersecurity risks, they may unintentionally expose the system to threats. For example, a user may choose a weak password, share credentials with another person, open a suspicious file, or neglect secure handling of sensitive information. Such actions can create opportunities for unauthorized access or data compromise.

Training helps reduce these risks by teaching employees the correct security behavior. This includes the use of strong passwords, the importance of keeping credentials confidential, the need to verify suspicious messages or files, and the obligation to follow internal security procedures. Training may also include guidance on reporting unusual incidents, avoiding unsafe practices, and understanding the importance of protecting the company's financial and administrative information.

Another benefit of user training is that it creates a cyber security culture within the organization. When employees are aware that cybersecurity is part of their daily responsibilities, they become more vigilant and more cooperative with internal control procedures. Therefore, training is not only an educational action but also a strategic measure for strengthening the overall resilience of the information system.

3.4.2.3. Complementarity of Practical Security Measures:

The practical measures applied in cyber security are more effective when they are combined. Regular updates reduce technical vulnerabilities, monitoring helps detect suspicious activity, and user training reduces risks linked to human behavior. Each measure addresses a different dimension of cyber security, but all of them contribute to protecting the information system used by SOMIPHOS.

Consequently, the practical application of cyber security within the system is not limited to installing protective tools. It requires a combination of technical maintenance, continuous observation, and human awareness in order to provide a more complete level of protection.

3.4.3. Practical Outcomes of Implementing Cybersecurity Measures:

The implementation of cyber security measures within an information system is justified not only by the existence of threats, but also by the practical benefits that result from stronger protection. In the case of Sage 100c at SOMIPHOS, the application of cybersecurity measures has important outcomes for the protection of information, the reliability of data, and the continuity of system use.

3.4.3.1. Protection of Financial Information from Unauthorized Access or Theft:

One of the most direct outcomes of implementing cyber security measures is the protection of financial information from unauthorized access or theft. The information system used at SOMIPHOS contains highly sensitive data, including accounting records, payroll information, fixed asset values, supplier and customer data, and commercial documents. If this information were accessed by unauthorized persons, the company could face financial, legal, and reputational consequences.

Cyber security measures such as controlled access, strong authentication, monitoring, and secure system management help reduce this risk. By limiting access to authorized users only, the company protects confidential financial data against internal misuse and external intrusion. By detecting suspicious activity, the organization can respond before information is extracted, altered, or misused.

The protection of financial information is particularly important because such data has strategic value. Accounting balances, payroll information, and commercial records can reveal the financial situation of the company, its obligations, and its operational activities. Therefore, safeguarding this information is not only a technical issue but also a matter of organizational security and business continuity.

3.4.3.2. Increased Reliability and Integrity of Accounting Data:

Another important outcome of implementing cyber security measures is the increased reliability and integrity of accounting data. Reliability means that the data can be trusted, while integrity refers to the fact that the information remains complete, accurate, and unaltered except through authorized actions.

In a system such as Sage 100c, data reliability is essential because financial statements, payroll calculations, fixed asset reports, and commercial records are all based on the information stored in the system. If data is altered without authorization, corrupted through system weakness, or damaged by improper user actions, the resulting reports may become inaccurate and misleading.

Cyber security measures contribute to data integrity by protecting the system against unauthorized modifications and by reducing the impact of technical or human threats. For example, activity monitoring can help identify irregular changes, updates can correct software weaknesses that may affect data, and user training can reduce entry mistakes or unsafe handling of information.

As a result, the organization benefits from accounting and administrative data that is more reliable for operational use, managerial decision-making, auditing, and reporting. In this sense, cyber security is closely linked to accounting quality, because protecting the system also protects the credibility of its outputs.

3.4.3.3. Improvement of Trust in the Information System:

Beyond direct protection and data integrity, cyber security measures also improve trust in the information system. When users know that Sage 100c is maintained, monitored, and protected, they are more confident in using it as a reliable working tool. Management also gains greater confidence in the information produced by the system.

This trust is important because the effectiveness of a digital system depends not only on its technical existence but also on the confidence that users and decision-makers place in it. If the system is perceived as vulnerable or unreliable, its outputs may be questioned, and users may hesitate to depend on it fully. By contrast, a protected system strengthens confidence in financial records, payroll results, and management reports.

3.4.3.4. Support for Operational Continuity:

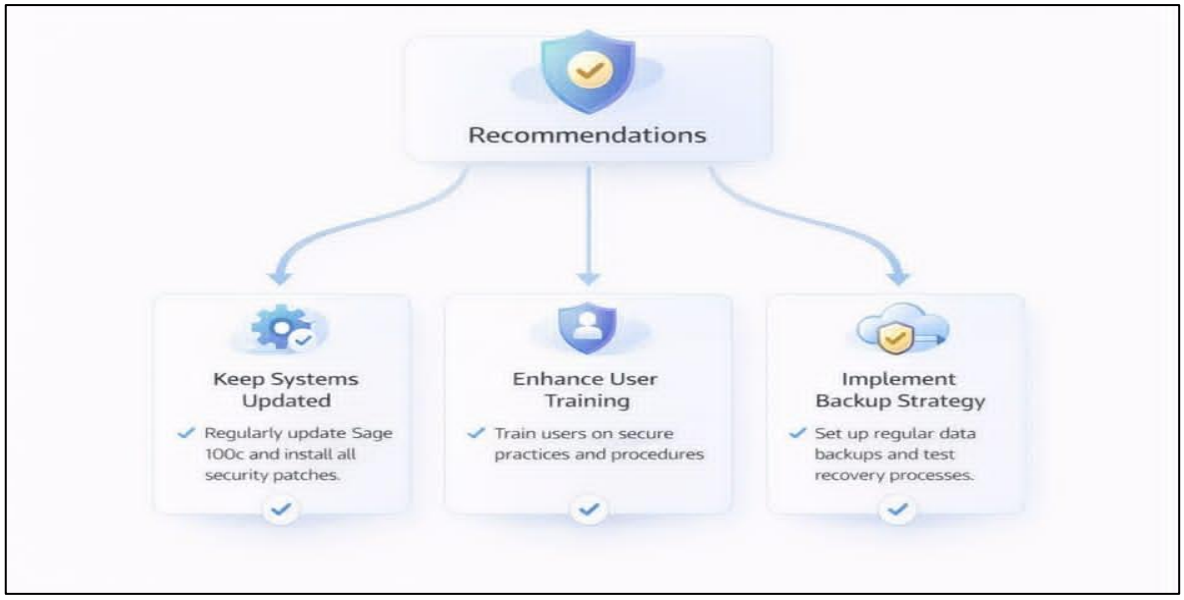
Cyber security measures also support the continuity of organizational activities. A system affected by intrusion, data loss, or major technical incident may interrupt accounting, payroll, or commercial operations. Such interruption can delay reporting, salary processing, or operational follow-up.

By reducing vulnerabilities and improving system protection, cyber security measures decrease the probability of such disruption. In this way, they contribute not only to information protection but also to the continuity of services supported by Sage 100c within SOMIPHOS.

3.4.4. Recommendations for Enhancing Information Security:

Although practical cyber security measures may already be present, information security remains a continuous challenge that requires regular improvement. For this reason, it is necessary to formulate recommendations aimed at strengthening the protection of the information system and ensuring that cybersecurity remains an active concern within the organization.

Figure 13:Recommendations to enhance security in sage 100c



Source: Information provided by the IT department of tebessa phosphate company

3.4.4.1. Strengthening Passwords and Access Control Policiesl:

A first recommendation is the strengthening of passwords and access control policies. Since access to Sage 100c is the entry point to sensitive accounting, payroll, and commercial information, the management of user authentication must be particularly rigorous.

This recommendation involves requiring stronger passwords, encouraging regular password renewal, preventing password sharing, and ensuring that user accounts are strictly personal. It also involves reviewing access rights regularly so that each employee has only the permissions required for their current responsibilities. When access rights are broader than necessary, the system becomes more exposed to misuse or unauthorized manipulation.

In addition, critical functions should be reserved for specifically authorized users. Sensitive actions such as modifying validated accounting entries, changing payroll parameters, or altering important commercial records should be limited and supervised. Strengthening access control in this way would improve the overall protection of the Sage 100c environment at SOMIPHOS.

3.4.4.2. Raising Employee Awareness through Continuous Training:

A second recommendation is the continuous raising of employee awareness through training. Cyber security is not a one-time matter but an ongoing issue. Even if users receive initial instructions, risks evolve over time, and new forms of cyber threats may appear.

Continuous awareness programs can help employees remain attentive to secure practices. Such programs may remind them of the importance of strong passwords, confidentiality of credentials, careful use of digital tools, and immediate reporting of suspicious situations. They may also help users understand how their daily actions can influence the security of financial and administrative information.

This recommendation is particularly relevant because human error remains one of the main causes of security incidents. Through continuous training, SOMIPHOS can reduce the risk that employees unintentionally expose Sage 100c or the surrounding information system to threats.

3.4.4.3. Developing and Enforcing a Clear Cybersecurity Policy within the Organizations:

A third recommendation is the development and enforcement of a clear cyber security policy within the organization. A cybersecurity policy is a formal document that defines the principles, responsibilities, rules, and expected behavior related to information security.

The existence of such a policy is important because it provides a common framework for all employees and departments. It clarifies what is allowed and what is prohibited, specifies how access should be managed, explains the obligations of users, and defines how incidents should be reported and handled. Without a clear policy, security practices may remain informal and inconsistent.

For SOMIPHOS, a cyber security policy would help formalize the protection of the information system used with Sage 100c. It would also strengthen coordination between management, IT personnel, and system users. The enforcement of the policy is just as important as its formulation. Rules must not only exist on paper, but must also be communicated, applied, and monitored in practice.

3.4.4.4. Promoting a Long-Term Cyber security Approach:

Another recommendation is to adopt a long-term cyber security approach rather than treating security as a temporary or isolated concern. The protection of Sage 100c and the associated information system requires continuity, periodic evaluation, and adaptation to new risks.

This means that SOMIPHOS should regularly review its security practices, identify new vulnerabilities, update its procedures, and assess whether current safeguards remain sufficient. A

long-term approach would allow the company to move from reactive protection to more proactive and preventive information security management.

The application of cyber security within the information system used at SOMIPHOS is an essential condition for protecting the Sage 100c environment and the sensitive information processed through it. Practical security measures such as regular system updates, activity monitoring, and user training contribute significantly to reducing cyber risks and strengthening the protection of accounting, payroll, fixed asset, and commercial data.

The implementation of these measures produces important positive outcomes. It protects financial information from unauthorized access or theft, improves the reliability and integrity of accounting data, strengthens trust in the information system, and supports the continuity of organizational operations. These outcomes show that cyber security is not only a technical necessity but also a factor of organizational efficiency and information quality.

However, the level of protection can always be improved. Strengthening passwords and access control policies, raising employee awareness through continuous training, and developing a clear cybersecurity policy are essential recommendations for enhancing information security. By adopting these measures in a structured and continuous manner, SOMIPHOS can further reinforce the resilience of its information system and ensure safer use of Sage 100c in support of its management activities.

Conclusion:

In light of the context of rapid digital transformations and the growing challenges they pose to information security, this study entitled “Evaluation of Cybersecurity Measures in the Protection of Accounting Information Systems”, seeks to address the research problem related to the effectiveness of these measures in protecting accounting information systems within organizations, and particularly the case of the Tebessa Phosphate Company, in a digital environment characterized by increasing threats and cyber risks that are increasing in complexity.

The work was supported by an applied study, the aim of which was to connect the theoretical concepts with the practical reality, to analyze the level of implementation of cybersecurity measures in the studied organization and to assess its effectiveness in protecting the accepted accounting system.

The theoretical part of the study dealt with the conceptual bases of cybersecurity as a strategic framework for the protection of information, emphasizing the main threats and risks faced by accounting information systems. It defined the role of these systems in organizations to support decision-making processes and emphasized the complementary relationship between cybersecurity and accounting information systems as a basic requirement for data integrity and reliability.

On a practical level, the study has explored the reality of the Tebessa Phosphate Company through a study of its accounting system Sage 100c focusing on the processing of data within the system and assessing the security measures implemented, particularly those relating to access management, data protection and backup systems. It also considered the role of internal controls in strengthening information security and identified the key weaknesses and potential risks to system effectiveness, either human or technical factors.

The study results show that the implemented cybersecurity measures have a significant contribution to the protection of accounting information systems, but their effectiveness is relative and depends on the degree of integration of these measures, their continuous updating, as well as the awareness of the users and the commitment of the organization to strengthen the culture of information security.

Therefore, the effective and sustainable protection of accounting information systems must be achieved by a comprehensive approach based on the integration of technical, organizational and human aspects, to deal with the changing cyber threats and improve the reliability of information

1. Hypothesis Testing:

Through addressing the research topic and analyzing the relationship between cybersecurity measures and the protection of accounting information systems, the validity of the hypotheses proposed in the introduction has been verified. These hypotheses formed the basis of this study. The main findings obtained can be presented as follows:

- **Main hypothesis:**

Cybersecurity measures are effective in protecting accounting information systems.

This hypothesis is correct, as cybersecurity procedures are an essential element aimed at securing sensitive financial data from various electronic threats, whether internal or external. These measures also contribute to the confidentiality, integrity, and availability of data, which enhances the reliability of the accounting system.

- **The first hypothesis:**

The use of systems like Sage improves data security and reliability.

Yes, this hypothesis is correct, according to the results of the experimental study. as it indicates that the use of the Sage system effectively contributes to enhancing data security and improving its reliability. This system provides a secure environment aimed at protecting data from risks such as unauthorized access and unintentional errors. Moreover, applying access control features to all accounting transaction records enhances system transparency and improves the accuracy of the institution's accounting information.

Accordingly, the study results confirm that the use of systems such as Sage effectively improves data security and enhances its reliability within the accounting information systems of the studied institution.

- **The second hypothesis:**

Implementing cybersecurity practices reduces cyber risks and threats.

This hypothesis is considered correct because the study results have shown that applying cybersecurity practices within the institution effectively contributes to reducing various cyber risks and threats. As these practices work to protect accounting information and data through the application of preventive measures and techniques aimed at reducing the likelihood of cyber-attacks and security breaches.

Adopting threat detection system mechanisms, regular software updates, and password policies helps strengthen institutional security, indicating that implementing cybersecurity practices leads to a reduction in cyber risks and threats within the institution.

- **The Third Hypothesis:**

In light of the findings reached, it can be said that the hypothesis is correct, as it is clear that the effectiveness of accounting information systems depends greatly on the level of implementation of cybersecurity procedures within them. The more the institution adopts effective security measures such as controlling user access permissions and implementing backups, the greater the system's efficiency in protecting accounting data. These procedures have also contributed to reducing cyber risks and threats that may affect the accounting workflow within the institution, which confirms that cybersecurity is an essential element in improving the effectiveness of the accounting information system in the institution under study.

2. Results of the Study:

The study results highlight that the implementation of cybersecurity measures within the institution under study effectively contributed to enhancing the efficiency of accounting information systems by reducing digital risks and strengthening data reliability, which positively reflected on improving system performance and supporting its stability.

The use of the Sage 100c system contributes to enhancing the security of accounting data through strict control over access permissions, where each user is granted only the permissions related to their job tasks. Additionally, the system records and tracks all accounting operations, which enhances transparency and facilitates monitoring and auditing processes.

Cybersecurity is considered an important element within the institution under study, due to its role in protecting accounting information systems and securing financial data from various digital threats. It also contributes to ensuring the continuous operation of the system in a safe and stable digital environment, making it an essential necessity that cannot be dispensed with in light of increasing digital challenges and risks.

Digital processing within the Sage 100c system contributes to improving the quality of accounting operations in terms of speed and accuracy, by entering and processing data according to specific rules, which reduces human errors and increases the reliability of accounting information.

Implementing cybersecurity mechanisms such as strong passwords, data encryption, and regular backups helps enhance the protection of information from risks of loss or tampering by providing multiple layers of protection that ensure the confidentiality and integrity of the data

The study showed that the effectiveness of the accounting information system largely depends on the implementation of effective security procedures, such as encryption, authentication systems, and backups. These procedures contribute to protecting accounting data from the risks of loss or breach, and ensure the preservation of its confidentiality and integrity.

3. Study recommendations:

Based on the results obtained, we can formulate the following recommendations, which are directed on one hand to the studied institution, and on the other hand to the state and other economic institutions:

- Algerian economic institutions should keep up with modern innovative technologies and digital transformations, especially those related to artificial intelligence, cybersecurity, the Internet of Things, and virtual reality. This can be achieved through conferences, research, and international or local seminars, as well as by following the latest developments in information and communication technology risks in order to take appropriate measures.
- Algerian economic institutions must have a good understanding of the information technology environment and all its related aspects, and establish control plans characterized by continuous updates in response to internal and external changes in order to avoid related risks, in accordance with international standards and regulations.
- We propose that the SOMIPHOS company rely on external cybersecurity experts to evaluate the implemented system and provide security and preventive recommendations.
- SOMIPHOS must address existing weaknesses within the institution by acquiring advanced security and protection systems, and by promoting cybersecurity awareness among employees across the institution and its branches through investment in this field.
- Decision-makers, whether at the level of economic institutions or the state, should make security and protection a priority rather than an option, by developing comprehensive security strategies, integrating them from the beginning of operations rather than at the end, and encouraging creativity and innovation among the competencies within Algerian economic institutions.
- It is also recommended to provide qualified offices and professionals who can offer consulting services to institutions in the field of cybersecurity, as well as to bring in specialists from other countries to exchange ideas and expertise.

- The Algerian legislator must take into account technological developments and changes by issuing laws and establishing plans and strategies that are adapted to modern technologies.

4. Future research perspectives:

We have attempted through this study to cover both the theoretical and practical aspects of the topic as much as possible. In order to further continue research in this field, we propose the following topics as future research perspectives:

- Cybersecurity and its role in reducing cybercrime.
- The contribution of ISO standards in strengthening cybersecurity within Algerian economic institutions.
- Cybersecurity as a mechanism to support and improve the performance of Algerian economic institutions.
- Requirements for the implementation of cyber intelligence in economic institutions.
- Cyber financial intelligence and its role in combating financial and accounting fraud.
- The extent of the adoption and use of early warning systems in Algerian economic institutions and their role in enhancing and achieving cybersecurity.

References

1. Al Azzam & Al Debei M (2021). **The Efficiency and Effectiveness of the Cyber Security in Maintaining the Cloud Accounting Informatio**. Academy of strategic management journal.
2. Almomani, Shehab, AL Ebbini, & Shami (2021). **The Efficiency and Effectiveness of the Cyber Security in Maintaining the Cloud Accounting Information**. Academy of Strategic Management Journal, 20(2). doi:https://www.abacademies.org/articles/the-efficiency-and-effectiveness-of-the-cyber-security-in-maintaining-the-cloud-accounting-information-10841.html?utm_source=chatgpt.com .
3. Al-saati, F., Al-areifi, H., Al-suwailem, B., Al-mehaidib, A., Al-amari, M., & A.K, & A.K.samha. (2022, may). **the impact of accounting information tecgnology on the effectiveness of decision-making**. Electronic international multidisciplinary journal(EIMJ), 3(5), 5,6. Retrieved from file:///C:/Users/Administrator/Downloads/CybersecurityriskstoaccountinginformationsystemsandtheirimpactoncompanyvalueanappliedstudyinZainIraqTelecommunicationsCompany%20(2).pdf .
4. Andi Nurwanah. (2024). **Cybersecurity in Accounting Information Systems**:. Advances in Applied Accounting Research, 2(3), 157-168. Retrieved from https://doi.org/10.60079/aaar.v2i3.336
5. Chiyad, Abbas Fadel. (2024). accounting inormation systems and their impact on the quality of capital exenditure decisions. scholars digest-journal of multidisciplinary, 3(5), 36-37.
6. Tarek Abdelhafid Elsharif. (2019). **the belements of accounting information systems and the impact of their use on the relevance of financial information in wahda bank-benghazi**. open journal of business and management, 7(3), 456-439. Retrieved from https://file.scirp.org/Html/25-1530900_93901.htm
7. Gelinas, U., Dull , R., & Wheeler, P. (2018). **accounting information systmes**. Cengege learning.
8. International organization for standardization. (2018). ISO/IEC 27000:2018 Information technology—Security techniques—Information security management systems—Overview and vocabulary. Retrieved from https://www.iso.org/standard/73906.html%E2%81%A0
9. James A, Hall. (2016). **Accouniting information systems** (éd. 9th edition). Cengage Learning.

10. Jan Svobodas & Ludekl Lukas. (2019). **DAAAM international scientific book** . DAAAM international scientific book , 321-330.; https://www.daaam.info/Downloads/Pdfs/science_books_pdfs/2019/Sc_Book_2019-027.pdf
11. Kenneth Caroll Laudon& Jane Price Laudon. (2020). **Managment information systems :managing the digtal firm** (16th edition ed.). pearson
12. Marioush S. A., & Al-obaidi I. (2026). **cyber security risks to acounting information systems an their impact on company value** ; an applied study in zain iraq trlrcommunications company. In digital transformation in achieving sustainabke development of management economic,and applied sciencs (p. 5 and 6). springer nature switzerland.
13. Marshall B, R., & Paul John, S. (2020). **accounting information systems**. (1. ed, Ed.) Boston, Ma,USA: Pearson.
14. Michael E, W., & Herbert,J, M. (2019). Principles of information security . Cengage learning.
15. Muda, I., Gusnardi, G., Daniel, J., & Kalahe, K. (n.d.). (2025) information systems components and value for organization. journal of economic and business studies, 8(2). Retrieved from https://www.pubtexto.com/journals/journal-of-economic-and-business-studies/fulltext/information-systems-components-and-value-for-organizations
16. National Institute of Standards and Technology. (2018). **Framework for imporving critical infrastructure cybersecurity**. april16,2018. Retrieved from https://doi.org/10.6028/NIST.CSWP.04162018
17. CharlesP Pfleeger & Shari Lawrence pfleeger. (2015). **Security in computing**. Boston
18. Romney, M., & Steinbart, P. (2017). **Accounting information systems** (14 ed.). Pearson Education.
19. Romney, M., & Steinbart, P. (2018). **Accounting Information Systems** (13th ed.). Retrieved from https://www.homeworkforyou.com/static_media/uploadedfiles/AIS%20Book.pdf
20. Romney, M., & Steinbart, P. (2021). **Accouniting information systems** (15th.ed ed.).
21. Marshall Romney ‹Paul Steinbart ‹Joseph Mula ‹Ray McNamara. (2017). **accounting information systems**. 14.https://books.google.dz/books?hl=ar&lr=&id=FhTiBAAAQBAJ&oi=fnd&pg=PP1&dq=21.%09Romney+Marshall+%26+B+Steinbart+,+Pul+John+,+accounting+information+systems,14+(2017).&ots=6g8ZclhOiR&sig=6edPAXU-ZUsH3VDlDyxhwBucDzo&redir_esc=y#v=onepage&q&f=false.

22. Sarah Allawi Marioush,Ilham Mohammad wathig Al-Obaidi;. (2026). **Digital transformation in achieving sustainable development of management,economic,and applied sciences** https://link.springer.com/chapter/10.1007/978-3-032-01592-1_2.
23. Stallings William. (2017). **Effective cybersecurity**:A guide to using best practices and standards. Addison-wesley professional. Retrieved fromhttps://ptgmedia.pearsoncmg.com/images/9780134772806/samplepages/9780134772806_Sample.pdf
24. Tarek Abdelhafid Elsharif. (2019). **The elements of accounting information systems and the impact of their use on the relevance of financial information in wahda bank-benghazi libya**. open journal of business and management, 7(03), 22. Retrieved from https://file.scirp.org/Html/25-1530900_93901.htm
25. Lubna Tabassum. (2022). **Cyber Security and Safety Measures**. 02(06).
26. technology, N. i. (2018). **Framework for improving critical infrastructure cybersecurity.** doi:https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
27. Ulric Gelinas, Richard B, Dull, Patrick. (2018). **Accounting Information Systems** (13th ed ed., Vol. not applicable). Cengage AU.
28. William Stallings. (2018). **Effective Cyber Security**: A guide to using best practices and standards. addison-wesley.
29. Hudud Amal Salem, **The Effectiveness of Cybersecurity in Protecting Accounting Information Systems in the Libyan Banking Sector**: An Applied Study on Commercial Banks Operating in the City of Zawiya. The Libyan Journal of Contemporary Academic Studies ،(2025) (3) 756-777 https://ljcas.ly/index.php/ljcas/article/view/253?utm_source.
30. Aïd, Walid et al., **Cybersecurity and Digital Hygiene,** Egyptian Journal of Information Sciences, Vol. 9, No. 2, 2022, pp. 390–422.

Arabic References

1. حدود آمال سالم . (2025). **مدى فعالية االمن السيبراني في حماية نظم المعلومات المحاسبية في القطاع المصرفي الليبي**: دراسة تطبيقية على المصارف التجارية العاملة في مدينة الزاوية. المجلة الليبية للدراسات الاكاديمية المعاصرة، 2(3). صفحة 777-756
2. عيد، وليد، أحمد، فاطمة علي إبراهيم، يوسف، رحاب فايز، & السيد، وليد محمود. (2022). **الأمن السيبراني والنظافة الرقمية.** المجلة المصرية لعلوم المعلومات، 9(2)، 390–422..

Appendices

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي -تبسة-

كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير
نيابة عمادة الكلية مكلفة بالدراسات والمسائل المرتبطة بالطلبة
مصلحة التعليم والتقييم

إتفاقية التربص

المادة الاول: هذه الاتفاقية تضبط علاقة جامعة الشهيد الشيخ العربي التبسي -تبسة- ممثلة من طرف عميد كلية العلوم الاقتصادية العلوم التجارية وعلوم التسيير

مع المؤسسة : phosphate Company

مقـــــرها : -tébessa-

ممثلة من طرف :

الوظيفة: Resources Manager السيد بريك Amin Brik

هذه الاتفاقية تهدف الى تنظيم تربص تطبيقي للطلبة الاتية أسمائهم :

1- GuettaB Ikram 2- Imen Guerdi

ماستر التخصص Accounting and finance

عنوان المذكرة: Evaluating Cyber security measures in protecting accounting information systems

الاستاذ (ة) المشرف (ة) :

هذه الاتفاقية تهدف الى تنظيم تربص تطبيقي للطلبة الاتية أسمائهم :

1- ..... 2- ..... 3 .....

4 ..... 5- .....

ليسانس التخصص :

عنوان تقرير التربص:

الاستاذ (ة) المشرف(ة) :

.....

وذلك طبقا للمرسوم رقم : 88-90 المؤرخ في : 1988/05/03 القرار الوزاري المؤرخ في ماي 1989.

المادة الثانية : يهدف هذا التربص الى ضمان تطبيق الدراسات المعطاة في القسم والمطابقة للبرنامج والمخططات التعليمية في تخصص الطلبة المعنيين .

المادة الثالثة :التربص التطبيقي يجرى في مصلحة :

Finance and accounting department / Information system

الفترة من: 18/03/2026 الى : 18/04/2026

المادة الرابعة : برنامج التربص المعد من طرف الكلية مراقب عند تنفيذه من طرف جامعة تبسة والمؤسسة المعنية.

المادة الخامسة :

على غرار ذلك تتكفل المؤسسة بتعيين عون أو أكثر بمتابعة تنفيذ التربص التطبيقي هؤلاء الاشخاص مكلفون أيضا بالحصول على المسابقات الضرورية للتنفيذ الامثل للبرنامج وكل غياب للمتربص ينبغي أن يكون على استمارة السيرة الذاتية المسلمة من طرف الكلية.

المادة السادسة:خلال التربص التطبيقي والمحدد بثلاثين يوما يتبع المتربص مجموع الموظفين في وجباته المحددة في النظام الداخلي وعليه يحسب على المؤسسة أن توضح للطلبة عند وصولهم أماكن تربصهم مجموع التدابير المتعلقة بالنظام الداخلي في مجال الامن والنظافة وتبين لهم الاخطاء الممكنة.

المادة السابعة: في حالة الاخلال بهذه القواعد فالمؤسسة لها الحق في انهاء تربص الطالب بعد إعلام القسم عن طريق رسالة مسجلة ومؤمنة الوصول.

المادة الثامنة: تأخذ المؤسسة كل التدابير لحماية المتربص ضد مجموع مخاطر حوادث العمل وتسهر بالخصوص على تنفيذ كل تدابير النظافة والأمن المتعلقة بمكان العمل المعين لتنفيذ التربص.

المادة التاسعة: في حالة حادث ما على المتربصين بمكان التوجيه يجب على المؤسسة أن تلجأ الى العلاج الضروري كما يجب أن ترسل تقريرا مفصلا مباشرة الى القسم.

المادة العاشرة :تتحمل المؤسسة التكفل بالطلبة في حدود إمكانياتها وحسب مجمل الاتفاقية الموقعة بين الطرفين عند الوجوب وإلا فإن الطلبة يتكفلون بأنفسهم من ناحية النقل ، المسكن ، المطعم.

ادارة المؤسسة المستقبلة

ادارة القسم

BRIK Ahmed
Directeur des ressources

SOCIETE DES MINES DE DJEBISSA
Direction des Ressources

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي -تبسة-

كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير
نيابة عمادة الكلية مكلفة بالدراسات والمسائل المرتبطة بالطلبة
مصلحة التعليم والتقييم

إذن بالقبول لمذكرة التخرج ماستر

أنا الممضي أسفله الاستاذ (ة) : عبيد خديجة .....

المشرف على مذكرة التخرج: ماستر للسنة الجامعية : 2026/2025

فريق العمل	الاختصاص	عنوان المذكرة بالتفصيل
1- فردي إيمان .	محاسبة ومالية	Evaluating cyber security measures in protecting accounting information systems: case study of telessa Phosphate company.
2- وهاب إكرام .		

أوافق على تقديم المذكرة وهذا بعد المراجعة الكاملة .

اللقب والاسم للاستاذ المشرف: عبيد خديجة

الامضاء: ABED

تاريخ الامضاء: 2026/05/16

الادارة