International Journal on Optimization and Applications

IJOA. Vol. 05, Issue No. 02, Year 2025, www.ijoa-journal.com

Cloud and shadow IT: the flip side of digital costs

AMZIL AIMAD

LAB SIM

Ecole HEEC Marrakech

aimad.amzil@eheec.ac.ma

Abstract— The phenomenon of shadow IT (SIT), also known as parallel or phantom computing, is constantly expanding, particularly as the use of cloud-based tools becomes increasingly widespread. This paper, based on qualitative research and a case study focused on reducing IT costs within a public transportation company, aims to explore in depth the method for identifying and assessing the hidden costs associated with cloud-based SIT.

An innovative approach is presented in this paper, highlighting the possibility of identifying this type of shadow IT not only through technical solutions, but also by leveraging financial account data and analytical information available in financial tools. This innovative approach paves the way for a better understanding of the financial implications of cloud-based shadow IT and underscores the importance of considering these hidden costs in organizations' financial and strategic analyses.

Keywords— *Shadow IT; IT management control ; hidden costs; cloud*

I. INTRODUCTION

Since the COVID-19 pandemic, remote work has grown considerably, changing traditional work methods. Employees now have the option of using their own IT equipment from home, and this development has led to the rise of Shadow IT (SIT) (Abbas & Alghail, 2023). Shadow IT is defined as the use of digital technologies, particularly cloud-based solutions, by employees without the formal approval of the Information Systems Department (ISD). Shadow IT is also called "parallel IT" or "phantom IT," and encompasses all the tools and software used by employees in their professional activities but which escape the control of IT teams (Meiller, 2020). Consequently, these unapproved technologies can pose significant risks to businesses, particularly in terms of security, compliance, and cost management.

According to Mell & Grance (2011), cloud computing is characterized by access to shared, configurable resources such as networks, servers, applications, and services that can be updated and accessed on demand. This situation is exacerbated by the proliferation of cloud computing, a technology that allows access to computing resources via the internet. While this technology is extremely beneficial for business flexibility, it also facilitates the use of cloud services without the knowledge or involvement of IT departments. This practice, uncontrolled by CIOs, constitutes a form of Shadow IT, making cost and risk control increasingly difficult for businesses. The public cloud represents fertile ground for the development of Shadow IT. Indeed, in a public cloud environment, data and applications are hosted by a third-party provider, which is a major contrast to traditional IT where the organization controls all resources (Satyanarayana, 2012). Software-as-a-Service (SaaS) cloud services are particularly affected by this phenomenon. In this model, companies are responsible for securing their data and managing user access. Employees, seeking quick and convenient solutions, resort to widespread data management tools or collaboration platforms without adhering to IT department validation protocols. Consequently, these tools escape all control in terms of security, compliance, and cost monitoring.

Shadow IT can be divided into several categories, including Greynet, which refers to network applications installed by end users to circumvent IT restrictions; content applications used to create and access data; and utilities used for system optimization or device cleanup (Vankayalapati, 2025). While these applications may meet immediate employee needs, they pose a significant risk of data leaks or security policy violations because they operate outside the control of IT teams.

This phenomenon has significant implications for IT governance within organizations. Shadow IT erodes the authority of the IT department and compromises the effectiveness of information systems management (Khalil & Samhan, 2025). Indeed, the IT department, traditionally responsible for aligning IT strategy with organizational objectives, sees its power diminish as employees act autonomously to adopt unapproved tools and services. This user autonomy, coupled with the rise of cloud computing and remote work, has transformed IT into a decentralized activity, escaping the traditional control of IT departments (Li et al., 2018). This loss of control leads to security problems, unforeseen costs, and non-compliance with applicable regulations, such as the GDPR, exposing companies to legal and financial penalties.

Furthermore, Shadow IT generates hidden costs that escape the notice of finance managers. These costs include unforeseen expenses related to securing data on unvalidated platforms, costs of non-compliance with regulatory standards, and indirect costs associated with managing tools used by employees without IT department involvement (Silic et al., 2025).

One of the most problematic aspects of Shadow IT lies in the invisibility of the tools used, which makes them difficult for IT managers to track and control. This invisibility complicates the management of associated costs and risks. Indeed, although many employees use these tools to improve their productivity, they often believe that the benefits of using them outweigh the potential risks. Employees consider their increased productivity as compensation for potential security breaches. This behavior is often reinforced by a theory of insufficient deterrence: sanctions or the guilt employees feel for violating security policies are not enough to deter their use of unauthorized tools. This situation demonstrates that managing Shadow IT requires more than sanctions; it requires a comprehensive IT governance strategy that includes clear processes, detection tools, and ongoing communication with employees (Silic et al., 2017).

To address the challenges posed by Shadow IT, companies must develop clear governance strategies and defined processes to better control the tools used by their employees. Implementing technical detection solutions is essential to identify unapproved applications and monitor the use of cloud services. Access management tools, application monitoring systems, and strict tool approval policies must be established to reduce the impact of Shadow IT on security and costs. Furthermore, raising employee awareness of IT security and the importance of adhering to company policies is crucial. Companies must also work in an interdisciplinary manner, involving both CFOs and CIOs, to understand the financial implications of Shadow IT and better control the hidden costs associated with this phenomenon (Ilesanmi, K. D. (2025)). The hidden costs generated by Shadow IT can be compared to those used in finance, where companies often underestimate expenses related to unvalidated services, leading to long-term financial losses (Alkousheh et al., 2025). To address the Shadow IT problem, companies must adopt a comprehensive approach that includes validation processes, detection tools, and a clear communication policy between the various departments within the company. Improved IT governance and the integration of security and compliance practices from the tool selection phase will help limit the impact of Shadow IT on IT resource management.

Overall, Shadow IT is a complex phenomenon that requires a strategic response and strengthened IT governance to mitigate its risks. By adopting a proactive approach that combines technical tools, clear governance and constant communication with employees, companies can better manage cloud infrastructure and reduce the risks associated with the uncontrolled use of cloud services

II. LITERATURE REVIEW

A. The Rise of Cloud Computing Practices and Their Impact on Organization and the Roles of Stakeholders

Chin et al. (2025) highlight that two opposing forces characterize the evolution of shadow IT. On the one hand, users adopt unofficial or informal technologies in response to internal information systems deemed inadequate to meet operational needs. This dynamic contributes to weakening the IT department's decision-making power, while reducing process standardization and compliance with security standards. On the other hand, a recentralization process is underway, aiming to deactivate parallel technologies and re-establish centralized control over information systems.

The various definitions of shadow IT agree that this practice is primarily initiated by employees themselves (Rakovic et al., 2020). These individuals choose unauthorized IT tools when IT department guidelines fail to meet their expectations, are perceived as too costly, or are simply not communicated effectively. A blurred line between professional and personal use can also lead to the misuse of existing tools, resulting in non-compliant technology manipulation.

Gonzalez et al. (2025) link the concepts of shadow IT and business-managed IT, reflecting a loss of IT department control over technology choices. According to these authors, the absence of internal restrictions from the IT department or management facilitates the proliferation of shadow IT. In the context of SaaS solutions, this situation is exacerbated by the behavior of vendors who often bypass purchasing departments or the IT department, concluding contracts directly with business units without prior consultation with IT managers (Scalabrin Bianchi et al., 2022). Akinade et al. (2025) note, however, that although cloud solution vendors seek to maximize their revenue, they ensure transparent and fair billing for their customers. This direct contracting method between business units and cloud service providers reduces implementation times, which are often constrained by internal IT processes. However, Akinade et al. (2025) highlight that cloud adoption goes beyond a simple technological choice; it represents a genuine evolution in management practices. This change requires a tripartite dialogue involving the IT department, business units, and decision-making bodies (such as the executive committee) to define and regulate the use of cloud solutions. within the organization. In this configuration, the IT department becomes a central player in technology governance, intervening both strategically and operationally to guide the use of cloud technologies, now required by management, functional departments and end users (Daniel et al., 2025).

B. Opportunities and Risks Associated with Cloud Information Systems (CIS)

B.1. Opportunities

Cloud information systems (CIS) offer several significant opportunities and advantages. The integration of cloud services enables ubiquitous access to data, regardless of location, time, or access method (Gonul Kochan et al., 2026). These systems can be developed in-house or acquired from external providers. Initially, CIS took various forms, often initiated by end users. Their development began in the late 1980s, a period during which end users were responsible for their implementation, although their management and integration into IT strategy remained the responsibility of the Information Systems Department (ISD). Today, the rise of mobile technologies allows employees to connect to applications via their smartphones, possessing the technical skills to install these tools independently, often without perceiving the risks associated with this autonomy (Rahman & Hossain, 2024).

Employee adoption of information systems (IS) fosters improved efficiency, speed, and creativity, and can stimulate innovation within organizations (Jaradat et al., 2026). Furthermore, these systems facilitate real-time communication and knowledge sharing, particularly in organizations spread across large geographical areas (Thompson, 2025). CIOs can play a key role in encouraging the use of IS, notably by training employees on the associated risks and raising awareness of information security best practices (Ammar, 2025). This approach can generate "reasoned deviant behavior" among employees, who take advantage of the benefits of IT systems, such as time optimization and ease of use of IT tools. However, this risk-taking is often accompanied by countermeasures, such as justifications based on "denial of harm" or the adoption of neutralization strategies through security measures. Cloud-based solutions offer advantages in terms of time savings, relying on turnkey offerings, and increased flexibility to cope with activity peaks thanks to external shared hosting (Huy & Phuc, 2025). They also offer cost-reduction advantages, allowing for the differentiation of capital expenditures (CAPEX) related to physical infrastructure from operating expenses (OPEX) related to non-amortizable external services (Mostefaoui et al., 2022). However, the authors emphasize that "the cloud has a recurring cost," which could weigh on companies' IT budgets in the long term. Indeed, unlike on-premises applications whose costs are absorbed after license amortization, cloud services generate ongoing costs throughout the usage period or contract.

According to Shen & Chen (2022), several hidden costs can be associated with cloud solutions, including over- or under-provisioning of resources, an increased number of administrators due to the use of multiple applications, storage costs, promises of free access below certain usage thresholds, contracting for unnecessary services, uncontrolled user adoption, service reversibility, contract exit fees, maintenance, network costs, and the risks associated with regulatory changes requiring updates to ensure compliance.

B.2. Risks Associated with Cloud Information Systems (CIS)

The adoption of cloud information systems (CIS) generates several significant risks, particularly regarding documentation and service management. Indeed, the lack of systematic documentation concerning outsourced data and processes is a major issue, which can lead to inefficient information management and organizational risks. This lack of documentation can result in situations where internal know-how is retained by employees, thus increasing the risks of duplication, inconsistent data (Foster, 2025), and, in some cases, data loss (Wuersch et al., 2023). The location of data in cloud environments also raises significant questions in the event of an incident, due to the potential difficulties in identifying the responsible party or the appropriate contact person to resolve the problems.

Another major risk lies in the increased vulnerability to attacks, such as viruses, which can compromise data integrity and security (Legros, 2022). In sectors such as healthcare, delays in digital transformation, often linked to a lack of resources, lead employees to adopt workarounds, thus exacerbating the risks associated with the use of IT systems (Singun, 2025). Firewall vulnerabilities, for example, allow the downloading of unsecured applications or the dissemination of sensitive data on private mobile devices. This situation also raises legal questions regarding data ownership: when an employee stores work-related information in the cloud, they may be considered the owner of that data, even if they are not authorized to act on behalf of the company.

From an organizational perspective, the cloud presents an additional risk due to long-term contractual commitments, sometimes making it difficult to terminate or revise contract terms. External financial auditors, tasked with verifying compliance with the Sarbanes-Oxley Act (SOX) and its Section 404 on the reliability of financial reporting for publicly traded companies, often identify user-developed systems (UDSs) as a major weakness in internal control. Indeed, these systems can facilitate the manipulation of non-compliant data (Akinsola, 2025).

Furthermore, information generated by UDSs is often perceived as less credible by managers compared to information from traditional systems, such as Enterprise Resource Planning (ERP) systems, which limits its use in the decision-making process (Liutkevičienė et al., 2026). Consequently, managers seek to reduce the use of these unofficial systems (Washik et al., 2026).

C. Cloud-based Information Systems as a Generator of Hidden Costs

We argue that cloud-based information systems (ISS) generate costs that companies are unable to identify transparently. These costs, by their very nature difficult to measure, can be likened to the "hidden costs" encountered in finance. Hidden costs are defined as those not represented in a company's information systems, such as budgets, income statements, general ledger accounting, cost accounting, and dashboards (Zajac & Goranova, 2026). Conversely, a visible cost is defined as a clearly identified cost category within these information systems, and which has three main characteristics:

- A recognized name (e.g., personnel costs),
- A specific measurement (e.g., the amount of salaries and social security contributions),
- A monitoring system (e.g., monthly analysis of payroll trends, with targets for cost reduction).

Zajac & Goranova (2026) distinguish two categories of hidden costs: "historical costs" and "opportunity costs." The former are real costs, but diluted across the various cost lines of existing information systems, while the latter result indirectly from malfunctions, although they are not directly included in visible costs (Kude & Huber, 2025). Furthermore, Zhao et al. (2025) emphasize the importance of the procurement function in managing the total cost of ownership. This cost, which is frequently used in IT cost analysis, encompasses not only the acquisition cost but also the costs associated with malfunctions, such as those related to breakdowns or poor quality, which are, in themselves, hidden costs.

In the context of IT systems, some costs can be considered historical hidden costs. Indeed, these costs often escape the attention of the Information Systems Department (ISD), even though they are potentially present in the company's accounts. This phenomenon is partly linked to a lack of transparency regarding the use of cloud systems within organizations. This leads to the following research proposition, which we will examine in the third part of this article:

- Proposition 1: Cloud information systems can be considered as historical hidden costs.

D. Methods for Detecting and Controlling Cloud Information Systems (CIS)

Gërxhani & Cichocki (2023) point out that, due to their informal nature, shadow systems, or CIS, are rarely detected overtly. However, several technical solutions can be implemented to limit or control the use of CIS, such as establishing blacklists or whitelists to block access to certain sites (Kamjou et al., 2024). Furthermore, managing user authentication allows for restricting access to network resources and, consequently, to sensitive company data (Martseniuk et al., 2024). Other technical methods, such as analyzing support tickets, conducting employee surveys, or verifying the software installed on end-user devices, can also be used to detect the existence of CIS. Furthermore, the use of statistical methods and machine learning algorithms applied to security firewall logs can contribute to the identification of these systems (Aljabri et al., 2022).

A review of the literature reveals that the cloud plays a central role in the development of cloud information systems (LIS), which are primarily generated by individuals within organizations but can also originate from business units. The Information Systems Department (ISD) seeks to control this phenomenon due to the resulting security, risk, and quality issues. Initially, it is essential to identify LIS—a process currently reliant on manual and technical approaches—in order to better control it. This leads to the following research proposition, which we will explore in the third part of this article:

- Proposition 2: Technical solutions represent the most direct means of detecting cloud information systems (LIS).

It is worth noting that banning and monitoring strategies often prove ineffective, as most employees can circumvent these restrictions by using mobile applications that do not require administrative privileges to install (Liutkevičienė et al., 2014). Network management policies can offer simple solutions, such as centralizing management and maintenance of updates (Aljabri et al., 2022). However, according to Akinsola (2025), personal norms and potential sanctions do not exert significant pressure on the adoption of IT systems. In contrast, individual perceptions of informal and formal controls strongly influence the organizational climate and employee ethics. Chen et al. (2022) emphasize that an approach involving strict IT control—such as prohibiting business departments from installing IT tools—reduces risk while maximizing efficiency.

IT governance defines the rights and responsibilities for decision-making, thereby facilitating the appropriate use of IT resources and enabling the IT department to respond to risks associated with IT security. Behavioral, performance, and socialization controls must be adapted for managing the use of cloud- and internet-based digital technologies, taking into account their specific characteristics (Zhao et al., 2025). A prerequisite for the effective management of these systems lies in identifying the costs associated with IT security. These controls can be implemented, in particular, through the analysis of user development documentation. By identifying instances of IT security, the IT department can propose new working practices, require business units to use only IT-approved tools, coordinate actions, and centralize the registration of IT instances. A division of tasks between the IT department and business units then becomes essential. Thus, the IT department will handle generic activities common to several departments, while the business units will focus on specific developments to optimize transaction and production costs. This reflection leads to the following research proposition, which we will examine in the third part of the article:

- Proposition 3: Appropriate governance enables the detection and control of the SIT.

In the following section, we will compare our three research propositions within the framework of our field study and discuss their implications in the conclusion.

III. Field Study Based on a Case Study in the Information Systems Departments (ISDs)

A. Case Study Presentation

This research is based on a field study conducted using the case study method, which allows for the analysis of specific situations and the testing of theoretical hypotheses. According to Yin (2018), each case study constitutes an independent research project, capable of either confirming or refuting a theoretical framework, while also offering the possibility of generating new elements and perspectives. The qualitative method adopted in this study allows for in-depth analysis, with detailed information gathered from various sources: interviews with key individuals, internal documents, and quantitative management data, thus serving to measure and illustrate the concepts studied.

The case study focuses on IT and telecommunications costs within a Moroccan construction group with over 2,000 employees. This group has six business line IT departments, each dedicated to a specific subsidiary, as well as a cross-functional IT department responsible for support functions, and a Group IT department in charge of joint projects. Each business line IT department is responsible for its own costs, while the Group IT department oversees the harmonization of strategic decisions and ensures consistency of control and governance at the global level.

This group has launched an ambitious cost-saving plan, supported by working groups tasked with identifying processes, costs, risks, and problems encountered, with the aim of proposing an improvement plan. The IT cost reduction program comprises nine specific projects, illustrated in Figure 1 below.

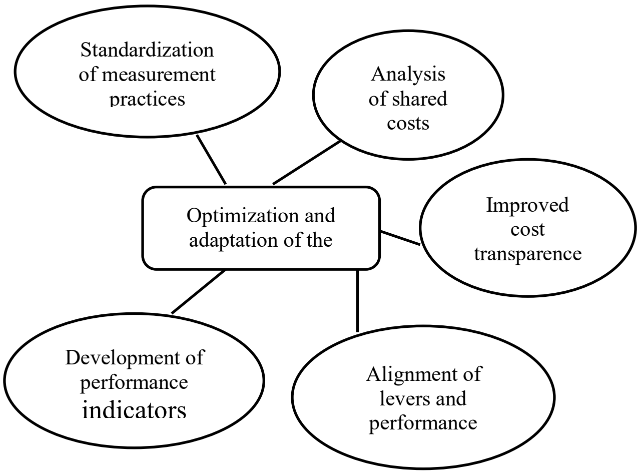
Figure 1: Presentation of the 9 projects in the cost reduction program

Number	Project
1	Governance of MOA/MOE responsibilities
2	Financial transparency and cost management
3	IT service outsourcing
4	IT Product and Service Acquisition Process
5	Centralized management of project portfolios and maintenance
6	Standardization of technologies and processes
7	Application streamlining and decommissioning
8	Application streamlining and decommissioning
9	Optimization of non-production environments

Source: by the author

Among these projects, the one related to finance was deemed particularly crucial, as it occupies the second position in the program. The specific objectives of this project are detailed in Figure 2 below.

Figure 2: Objectives of Project 2 - Financial Component


Standardization of measurement practices
Analysis of shared costs
Optimization and adaptation of the
Improved cost transparence
Development of performance indicators
Alignment of levers and performance

Source: by the author

B. Data Collection and Analysis Methods

The researcher was involved in a consulting engagement focused on the financial aspects, primarily concerning return on investment and cost optimization during 2022. The project was structured around four main sessions, which enabled the collection of data and information relevant to this research on shadow IT.

The researcher undertook a consulting engagement focused on the financial aspects, primarily concentrating on return on investment and cost optimization in 2022. The project took place over four main sessions, allowing for the collection of data and information relevant to this research on shadow IT.

The first phase involved 15 scoping interviews with management controllers and 7 CIOs or project managers for cost reduction initiatives. The second step involved collecting information such as organizational charts, procedures, reference documents, and data files on stock prices, purchase volumes, and transactions.

The four workshops in the third step addressed cost reduction initiatives, economic transparency, procurement, financial monitoring, and key performance indicators. Finally, the fourth step enabled the formalization of the target, including the organization, objectives, and cost-saving plan, as well as the target processes.

The quantitative data used in this study primarily relates to the first two months of the project, during which the team focused on identifying the scope of IT costs. This scope encompasses all of the group's IT costs, including both those recorded by the IT department and those associated with shadow IT. This identification allowed for the quantification of the extent of shadow IT. Although the researcher did not participate in the data production, the data was provided to them and analyzed for the purposes of this study.

As part of this mission, the researcher conducted fifteen interviews with participants from diverse populations to gather qualitative information.

In addition to the interviews, several relevant documents were collected during Phase 2. These documents included organizational charts, procedures, reference materials, detailed cost analyses, process maps, and a list of applications used, along with their status regarding potential decommissioning.

Phase 3 consisted of organizing five half-day workshops focused on cost reduction projects, their financial monitoring, and the associated governance. These workshops allowed participants to work on defining the IT cost base, assessing the amount of shadow IT, and developing potential cost reduction strategies.

All of this data—interview transcripts, workshop notes, end-of-mission reports, collected documents, and the researcher's continuous presence within the Group for six months—made it possible to:

- Describe the methods used to detect shadow IT, particularly by analyzing the accounting records and definitions used within the Group;

• Understand the governance issues and power dynamics between IT managers and the finance department;

• Gather verbatim comments from participants through coding of responses during interviews, in order to illustrate the analyses.

C. Results

The group's objective was to reduce costs over a two-year period in response to a significant increase in outsourcing costs. To this end, external firms were consulted to conduct comparative analyses and obtain industry data. These actions resulted in a substantial amount of financial and operational data.

As part of this study, the group identified costs related to shadow IT, estimated to represent a portion of total IT costs. The definition used to describe shadow IT was as follows: "Shadow IT includes all IT expenditures not incurred within IT departments or joint structures responsible for IT projects." This definition aligns with previous research, emphasizing that expenditures not approved by the Information Systems Department are identified by the departments responsible for the spending, whether IT departments or joint structures.

IT expenditures were meticulously examined to establish a benchmark for assessing potential savings. To achieve this, several analytical approaches were used to detail the costs:

• Organization: Costs were analyzed within each business IT department, as well as across the various organizational structures. Some costs were directly allocated to the IT departments, while others were recorded within the business structures.

• Expense Types: Costs were classified into three main categories: IT department costs, costs of mixed structures managing IT projects, and costs associated with shadow IT, originating from external organizations not involved in IT cost management.

• Nature of Expenses: Expenses were grouped into three main categories: purchases and external expenses (subcontracting, hardware, software, telecommunications, etc.), labor (salaries, social security contributions), and direct capitalized purchases.

A detailed analysis was performed using an Excel file to list the costs, based on an extract from the accounting ERP system covering all group costs. The management controller received authorization from senior management to access financial data beyond the IT departments. Several criteria were used to specifically identify IT costs, focusing particularly on organizational structure and excluding costs related to shadow IT within departments and joint structures responsible for IT projects. This approach allowed for the precise quantification of shadow IT costs. Expenses related to SaaS cloud services were subject to inconsistent accounting treatment. Invoices from cloud application providers were recorded in different expense categories, sometimes categorized as software license fees, sometimes as IT services, and even as non-IT services when SaaS solutions were integrated into broader offerings. This diversity of treatment led to an imperfect classification of information systems costs, as these were not systematically identified as such by financial management systems. This situation is partly explained by the absence, during the period in question, of a sufficiently explicit accounting framework for the treatment of software solutions.

To address these ambiguities, a revision of the accounting rules for software was undertaken, leading to the introduction of the concept of "IT solution." This conceptual shift broadens the traditional view of software by encompassing all digital functionalities that enable the processing, securing, and transmission of data, regardless of its physical medium. The implementation of this new accounting framework aims to consolidate IT costs into a unified category, thereby facilitating their identification and monitoring. However, while this clarification improves the allocation of expenses related to information systems, it does not, on its own, guarantee a comprehensive identification of the costs associated with cloud usage outside the core IT department. Analysis of the method chosen by the company to identify these costs reveals an approach based on the use of accounting categories dedicated to information technology and telecommunications. This approach offers the advantage of a common and standardized language, facilitating the initial detection of IT expenses. However, the costs thus identified only cover part of the scope of so-called "invisible" information systems, as they correspond to expenses incurred at the operational level without being directly managed by the IT department. This characteristic distinguishes the approach adopted from much academic work, which focuses primarily on the uses and costs incurred by end users.

Discussions with financial management stakeholders have led to the development of a more comprehensive method for identifying these expenses. This method is based on the observation that organizations are increasingly using external providers offering business services that integrate digital tools, particularly in cloud environments. In this context, IT costs are often included in overall billing, making their direct identification difficult. A cross-referencing approach between the costs related to business services and a list of cloud solution providers thus appears to be a relevant lever for improving the detection of these expenses, although this method is still under development.

Finally, the analysis of external costs related to information technology and telecommunications reveals that expenses incurred outside the central IT department represent a significant portion of overall costs. This share is particularly pronounced for software-related expenses, and even more so for those related to its provision through leasing, an area where cloud solutions play a dominant role. These results underscore the growing importance of information systems not directly managed by the IT function, particularly in the field of software solutions.

Interviews conducted with financial management personnel and operational managers involved in cost control initiatives highlighted the indirect effects of IT rationalization policies on business practices. In a context of budget constraints, several entities were unable to secure application development or upgrades from the central IT department.

This situation was part of a broader program aimed at streamlining the application portfolio, one of the main objectives of which was to reduce the number of applications in service in order to reallocate financial resources to maintaining tools deemed priorities. Analysis of the application portfolio, supported by enterprise architecture studies, identified a significant number of applications likely to be retired over a multi-year period, based on assumptions regarding their average lifespan. However, decommissioning applications proved to be a particularly complex process, requiring adjustments to operational practices, substantial technical interventions, and careful management of associated data. While this approach represented a significant lever for reducing expenses, its gradual implementation limited its immediate impact on expected savings.

Faced with the impossibility of using new in-house solutions, some operational stakeholders opted for alternative solutions by directly engaging external providers offering cloud-based applications. This choice allowed them to meet their functional needs while charging the costs to their own budgets, outside the established IT governance framework. This situation illustrates a characteristic case of unofficially recognized information systems, as defined in the literature, where digital solutions are used within the organization without formal validation from the IT department. These practices can also be analyzed as hidden costs, insofar as the associated expenses escape the IT function's monitoring and control mechanisms and are not fully integrated into existing management information systems.

The observed situation highlights a loss of confidence among some operational stakeholders in the central IT function, leading them to adopt alternative methods of consuming digital resources, primarily through cloud solutions. Initially, these uses remained largely invisible to the financial management systems of the information systems. The comments gathered during the interviews reflect a shared sense of disconnect between the organizational constraints imposed by IT governance and the demands for responsiveness and flexibility expressed by operational activities. The interviewees particularly emphasized the perceived slowness of internal development and validation processes, as well as the inadequacy of certain standardization approaches to the specific and urgent needs of the business. Faced with these constraints, using external providers offering rapidly deployable solutions appears to be a pragmatic response for ensuring business continuity. This trend is all the more striking given that it involves managers initially committed to controlling IT spending, but who have prioritized immediate operational efficiency.

This choice has led to the implicit outsourcing of certain IT decisions and the allocation of corresponding costs to operational budgets, outside the control of the IT department. This mechanism has thus contributed to the development of practices related to information systems that are not officially recognized, widening the gap between the actual use of digital technologies and formal governance frameworks.

Following the findings from the initial phases of the project, the organization initiated a change in its governance to better regulate these practices. The actions implemented focused in particular on structuring IT procurement processes and strengthening the associated financial oversight. The objective is twofold: firstly, to streamline and centralize decisions regarding the acquisition of digital solutions in order to limit uncontrolled use; secondly, to improve the visibility and monitoring of IT expenditures, including those incurred outside the traditional scope of the IT function.

IV. DISCUSSION

From a theoretical perspective, this research demonstrates that business units, as well as IT professionals within these units, do not consider shame to be a major obstacle to the development of shadow IT (SIT). Indeed, several respondents explicitly stated that they deliberately circumvent formal procurement policies. They use SIT solutions and conceal the associated costs. The cost-cutting context in which this study was conducted prevented IT managers from adopting deviant behaviors to leverage the benefits of the IT system. Financial governance took precedence: monitoring the IT budget was deemed more crucial than implementing security or mitigation measures (Akinsola, 2026).

This research addresses the three propositions formulated in the literature review:

Proposition 1: Cloud-based IT systems can be likened to historical hidden costs.

This proposition is validated. Cloud applications were directly ordered by business units without approval or budget allocation from the IT department. These costs, invisible in the IT department's financial information system, were nevertheless detectable in the Group's overall financial system. They therefore correspond to historical costs, since they escape the IT department's direct control while being recorded in the Group's accounts.

Proposition 2: Technical solutions are the simplest way to detect cloud-based IT infrastructure (STI).

This proposition is not validated. The case study reveals that a method not described in the literature can identify STI costs. Analysis of accounting and analytical accounts made it possible to detect IT expenditures incurred outside the IT department. The method used by management control to identify these costs is based on the assumption that costs are recorded outside the IT department and in mixed structures managing IT projects.

Hidden opportunity costs, resulting from inefficient practices or malfunctions, remain invisible in the accounts and require further evaluation.

Proposition 3: Appropriate governance enables the detection and control of STI.

This proposition is partially validated. Although the Group implemented an IT cost reduction plan and documented governance rules, these efforts did not prevent business units from contracting directly with suppliers for IT services without going through the IT department. However, financial governance enabled the identification of IT-related costs, thus facilitating their control. Financial indicators were established to monitor compliance with the rules and measure their effectiveness. Subsequently, governance was strengthened through stricter procurement rules, mandating the use of a centralized service center for IT purchases.

One of the significant findings of this study lies in the formalization of a classification of IT-related costs. This classification identifies four groups of IT costs:

- Category A expenses: These costs are directly borne by the IT department. They represent the majority of external costs in this study.

- Category B expenses: These costs are incurred by departments other than IT and represent a portion of external costs. In some cases, such as for cloud-based applications, these costs can even reach a higher level. These expenses fall into the category of shadow IT, meaning they are hidden from the IT department.

- Category C expenses: These costs are borne directly by end users, for example, for using applications on their own devices. Although these costs cannot be measured by the company, they result in hidden costs for the IT department and other departments. These practices can lead to malfunctions, data loss, and overconsumption of IT resources. Incidents related to the use of incompatible applications have been reported. Furthermore, sensitive data is circulating on unsecured platforms, violating security policies.

- B' Expenses: Initially classified as Category C, these expenses can increase Type B costs. They represent IT expenses directly incurred by users but reimbursed by business departments through expense reports. Although these costs have been identified, their valuation has been deemed disproportionate to their financial impact.

Another major contribution of this study lies in enriching the definition of hidden costs. This research highlights the intentional concealment of certain IT costs by business managers who do not have the authority to generate such expenses. These managers, while involved in controlling IT costs, are outside the scope of the IT department and lack direct access to business accounts.

This study also underscores the importance of strict governance for shadow IT and highlights the key role of finance in legitimizing IT system decisions. The research focuses on cloud computing, emphasizing the need for precise contracts with external partners. Strengthened procurement governance has improved collaboration between business units and the IT department.

Furthermore, this study highlights the importance of a systemic approach involving senior management. This intervention facilitated the detection of hidden costs and the creation of a dedicated IT procurement service center. It is emphasized that the mistake of gradually phasing out beneficial cloud applications must be avoided.

It is important to note that this analysis is based on a specific case, and a future study could explore the strategies and mechanisms in place within this company in greater depth. Establishing procurement governance and a service center could streamline costs. It would also be relevant to assess the opportunity costs associated with using cloud computing to inform future research on this topic.

V. CONCLUSION

Information Technology Services (ITS), particularly cloud-based services, extend beyond end users within companies. In the case study, the identified costs include services that deliberately consumed IT resources without the approval of the IT department. The case study confirms that ITS detection can be achieved beyond traditional technical means, such as connection monitoring. In this instance, we introduced a practical and operational methodology based on accounting principles, enabling the identification of ITS costs through the analysis of accounting records and, subsequently, through cross-referencing with suppliers, thus facilitating the identification of cloud services.

Our research, conducted prior to the recent revisions to accounting rules (2024) by the French Accounting Standards Authority (ANC), has demonstrated that broadening the scope of the "software" account, now called "IT solution," will facilitate more comprehensive and accurate monitoring of cloud-related costs, thereby improving visibility into ITS.

This study makes an original contribution, notably by adopting a financial approach to IT analysis and refining Savall and Zardet's (2020) definition of hidden costs. It has formalized a typology of IT costs, distinguishing between:

- IT costs directly charged to the IT department, which are not considered IT or hidden costs.

- Costs related to business units, without IT approval, which constitute both IT and hidden costs.

- Costs directly incurred by end users, which are not directly part of the company's costs but may constitute IT.

The last two cost categories can lead to hidden opportunity costs, generating quality issues and security risks. IT is, by its very nature, a hidden cost because, although it is identifiable at the company level, IT managers often lack sufficient visibility into these costs. Strengthened governance, coupled with clearer accounting rules and rigorous monitoring of financial indicators, could improve the detection and control of IT systems. Furthermore, consolidated procurement governance will allow for better definition of purchasing rules and control of IT-related costs. Our results reveal significant tensions between the IT department, business units, and the finance department, but also that the company studied ultimately prioritized strict financial governance, thus ensuring better control of IT-related costs.

REFERENCES

[1] Abbas, M., & Alghail, A. (2023). The impact of mobile shadow IT usage on knowledge protection: an exploratory study. *VINE Journal of Information and Knowledge Management Systems*, *53*(4), 830-848.

[2] Akinsola, K. (2025). Legal Compliance in Corporate Governance Frameworks: Best Practices for Ensuring Transparency, Accountability, and Risk Mitigation. *Accountability, and Risk Mitigation (January 31, 2025)*.

[3] Akinade, A. O., Adepoju, P. A., Ige, A. B., & Afolabi, A. I. (2025). Cloud security challenges and solutions: A review of current best practices. *Int J Multidiscip Res Growth Eval*, *6*(1), 26-35.

[4] Aljabri, M., Alahmadi, A. A., Mohammad, R. M. A., Aboulnour, M., Alomari, D. M., & Almotiri, S. H. (2022). Classification of firewall log data using multiclass machine learning models. *Electronics*, *11*(12), 1851.

[5] Alkousheh, H., Alkousheh, Y., Qawaqzeh, R., Al Juneidi, L., Al-Zerikat, L., Hussain, A., & Al-Latayfeh, M. (2025). The hidden cost of digital learning: a cross-sectional study assessing the prevalence of computer vision syndrome (CVS) among medical students in Jordan. *BMJ open*, *15*(1), e093939.

[6] Ammar, S. F. (2025). Unveiling the rivalry of cloud ERP dialectics, underpinning logics and roles of accounting and information system professionals. *International Journal of Accounting Information Systems*, *56*, 100728.

[7] Chen, W., Gao, L., Xu, X., & Zeng, Y. (2022). Does Stricter Command-and-Control Environmental Regulation Promote Total Factor Productivity? Evidence from China's Industrial Enterprises. *Discrete Dynamics in Nature and Society*, *2022*(1), 2197260

[8] Chin, T., Li, Q., Mirone, F., & Papa, A. (2025). Conflicting impacts of shadow AI usage on knowledge leakage in metaverse-based business models: A Yin-Yang paradox framing. *Technology in Society*, *81*, 102793.

[9] Daniel, S., Olaoye, G., & Ejaz, U. (2025). Data migration in the cloud database: A review of vendor solutions and challenges.

[10] Foster, C. J., Plant, K. L., & McIlroy, R. C. (2025). The never-ending nightshift: Insights into organisational adaptation during COVID-19. *Safety Science*, *184*, 106740.

[11] Gërxhani, K., & Cichocki, S. (2023). Formal and informal institutions: understanding the shadow economy in transition countries. *Journal of Institutional Economics*, *19*(5), 656-672.

[12] Gonzalez, A., Riemenschneider, C., & Green, G. (2025). Cloud computing implementation: a field study of business unit IT self-sufficiency. *Information Technology & People*.

[13] Huy, P. Q., & Phuc, V. K. (2025). Pathways of SME globalization: unveiling the role of niche market leadership and intelligent cloud-based accounting information system. *International Journal of Information Technology*, 1-18.

[14] Ilesanmi, K. D. (2025). Regulation of Shadow Banks and Its Implication for Financial Stability in Emerging Economies. In Shadow Banking and Financial Risk in Emerging and Developing Markets: The Growth and Development of Non-Bank Financial Intermediation (pp. 233-252). Cham: Springer Nature Switzerland.

[15] Jaradat, Z., Al-Hawamleh, A., Al-Tahat, S., & Mohammed, A. (2026). Exploring the impact of cloud computing-based accounting information systems on Sustainable Development Goal 8: evidence from the industrial sector in Saudi Arabia. *Competitiveness Review: An International Business Journal*, *36*(1), 39-60.

[16] Kamjou, E., Scott, M., & Lennon, M. (2024). Green infrastructure inequalities in informal settlements. *Habitat International*, *147*, 103058.

[17] Khalil, S., & Samhan, B. (2025). The impact of cloud adoption on talent management: an exploratory study from the "learning organization" perspective. *The Learning Organization*, *32*(4), 601-619.

[18] Kude, T., & Huber, T. L. (2025). Responding to platform owner moves: A 14-year qualitative study of four enterprise software complementors. *Information Systems Journal*, *35*(1), 209-246

[19] Legros, P. (2022). L'impératif de sécurité des données de santé, de la nécessité technique à l'obligation juridique. *Revue internationale de droit économique*, (3), 13-37.

[20] Li, W., Wang, B., Liu, W., Huang, Y., Huang, Y., Huang, W., ... & Huang, C. (2025). Digital image correction assisted absolute phase unwrapping for phase shifting profilometry based on connected domain segmentation. *Optics Communications*, *578*, 131488.

[21] Liutkevičienė, I., Hansen, D., & Rytter, N. G. M. (2026). Organisational mechanisms for building digital process improvement capabilities to foster SME competitiveness and growth. *Production Planning & Control*, 1-17.

[22] Martseniuk, Y., Partyka, A., Harasymchuk, O., Nyemkova, E., & Karpinski, M. P. (2024). Shadow IT risk analysis in public cloud infrastructure. In *CSDP* (pp. 22-31).

[23] Meiller, Y. (2020). Digital transformation, covid-19 crisis, digital transformation. *ESCP Business School Impact Paper*.

[24] Mostefaoui, A., Merzoug, M. A., Haroun, A., Nassar, A., & Dessables, F. (2022). Big data architecture for connected vehicles: Feedback and application examples from an automotive group. *Future Generation Computer Systems*, *134*, 374-387.

[25] Rahman, S., & Hossain, M. Z. (2024). Cloud-based management information systems opportunities and challenges for small and medium enterprises (SMEs). *Pacific Journal of Business Innovation and Strategy*, *1*(1), 28-37.

[26] Rakovic, L., Duc, T. A., & Vukovic, V. (2020). Shadow IT and ERP. *Journal of East European Management Studies*, *25*(4), 730-752.

[27] Satyanarayana, S. (2012). Cloud computing: SAAS. *Computer Sciences and Telecommunications*, (4), 76-79.

[28] Scalabrin Bianchi, I., Vaquina, A., Pereira, R., Dinis Sousa, R., & Dávila, G. A. (2022, November). A benefit dependency network for shadow information technology adoption, based on practitioners' viewpoints. In *Informatics* (Vol. 9, No. 4, p. 95). MDPI.

[29] Shen, H., & Chen, L. (2022). A resource-efficient predictive resource provisioning system in cloud systems. *IEEE Transactions on Parallel and Distributed Systems*, *33*(12), 3886-3900.

[30] Silic, M., Silic, D., & Kind-Trüller, K. (2025). From Shadow It to Shadow AI–Threats, Risks and Opportunities for Organizations. *Strategic Change*.

[31] Singun, A. J. (2025). Unveiling the barriers to digital transformation in higher education institutions: a systematic literature review. *Discover Education*, *4*(1), 37.

[32] Thompson, L. (2025). Cloud-Based Management Information Systems: A Paradigm Shift in Enterprise Resource Planning. *OTS Canadian Journal*, *4*(6), 62-73.

[33] Vankayalapati, R. K. (2025). Architectural foundations of hybrid cloud. The Synergy Between Public and Private Clouds in Hybrid Infrastructure Models: Real-World Case Studies and Best Practices, 17.

[34] Washik, M., Hylving, L., & Koutsikouri, D. (2026). Coping Strategies for Tensions Between Digital Data and Data Practices in Data-Driven Organizations.

[35] Wuersch, L., Neher, A., & Peter, M. K. (2023). Digital internal communication: An interplay of socio-technical elements. *International journal of management reviews*, *25*(3), 614-639.

[36] Yin, R. K. (2018). Case study research and applications. Design and Méthods (éd. Sixth). Los Angeles: Sage.

[37] Zajac, E. J., & Goranova, M. (2026). When the principal is the firm's problem: principal costs and their corporate governance implications. *Academy of Management Review*, *51*(1), 25-56.

[38] Zhao, X., Li, X., Wang, A., & Fang, J. (2025). The impact of energy prices on electric vehicle adoption: From a perspective of consumer expectations. *Sustainable Futures*, *9*, 100437.