Journal of Information Systems Engineering and Management
2025, 10(28s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Critical and Control Aspects due to the Absence of IT Governance in SMEs

Diana Elizabeth Moncayo[a], Israel Gonzalez-Carrasco[a]

[a] *Universidad Carlos III de Madrid, ROR: https://ror.org/03ths8210, Departamento de Informática, Avenida de la Universidad, 30 (edificio Sabatini), 28911 Leganés (Madrid), España.*

ARTICLE INFO

Received: 18 Dec 2024

Revised: 21 Feb 2025

Accepted:27 Feb 2025

ABSTRACT

This study aims to show the importance of the presence of an IT specialist within an organization. Small and medium-sized companies increasingly hire cloud solutions, which refer to servers, web hosting, drives, antivirus, etc. In addition, external companies carry out physical and logical computer maintenance once a year. This leads companies to omit a systems specialist since support is external, and it is assumed that activities in the technological area are increasingly less. It is important to demonstrate to senior management the importance of IT Governance in small and medium-sized companies. Given that there is no comprehensive strategic vision regarding the use of IT in the organization, there is a lack of knowledge of IT Governance. The objective of this work is to change the strategic vision of the senior management of an SME organization, helping to identify current problems and opportunities for improvement related to technology. Therefore, a simple technique is proposed for senior management to understand their current risk situation through specific evaluations that help determine the risk assessment in which the organization is located, triggering the need to have an IT specialist.

Keywords: IT, Governance, SMEs.

I. INTRODUCTION

The importance of SMEs lies, among other reasons, in that they generate 52% of the countries' gross domestic product and around 72% of formal employees **Error! Reference source not found.**The United Nations **Error! Reference source not found.**and the World Bank established multiple criteria that define SMEs, depending on the company's characteristics and production.

In small and medium-sized companies, there is a lack of knowledge about technology assets; in most cases, there are no systems personnel to adequately lead the significant processes for correctly managing technological assets.

The absence of expertise by company members causes the following: erroneous perceptions of the current information situation, untimely actions in the face of asset depreciation, poor hardware and software migration, and the growth of security threats, causing medium—and long-term technological obsolescence.

For this reason, it is important to highlight IT governance in an organization, which allows the company to maintain its survival and development.

An organization's survival depends on information stability, and it must consider effective information management and related IT information technology. Several elements or indicators demonstrate that an organization's assets are subject to threats and vulnerabilities.

The constant updating of technology and information management implies significant organizational changes, but it should not imply that senior management only covers a service or need.

Technology has the potential to influence management positively. Technology is often shown to act independently, solving problems by itself. However, it is not just about supporting information under the latest trend applications since it does not prevent an imminent risk from existing.

Several of the applications hosted in the cloud can present a security problem. If a risk materializes, it can affect much of an organization's critical information. On many occasions, users report that the services no longer work correctly.

No IT specialist validates the information's availability, given that the contract is for a service or several tools in the cloud.

It is important to consider that artificial intelligence raises the possibility of replacing system specialists in routine and repetitive tasks, freeing up time for activities with greater added value **Error! Reference source not found.Error! Reference source not found.**, but it is important to clarify to senior management that IT governance must validate the operations generated by AI.´

II. THE IMPORTANCE OF IT GOVERNANCE IN COMPANIES

In many cities in Ecuador and undoubtedly due to the COVID-19 pandemic, many companies have increased the use of applications and tools in the cloud, causing a significant change in the remote way processes are executed.

It is important to consider that the use of cloud applications leads to an increase in computer insecurity.

According to the cybersecurity report, Moisés J. Schwartz **Error! Reference source not found.**argues that the crisis caused by the COVID-19 pandemic at the beginning of 2020 has generated a dependency on a vital infrastructure for many users who are unaware of its existence and insecurity that spreads day by day due to cyber threats and through a study it shows that the Latin American and Caribbean region is still not sufficiently prepared to face the attacks that occur in cyberspace.

The article "IT Governance and Management Model, based on COBIT 2019 and ITIL 4, for the Catholic University of Cuenca" highlights the lack of alignment between IT and institutional objectives in Ecuadorian universities and the shortage of IT formalized committees. According to a study carried out by the Ecuadorian Corporation for the Development of Research and Academy (CEDIA), only one in ten universities has a formal IT Government **Error! Reference source not found.**

Organizations, institutions, etc., must take one step at a time because there is no such knowledge of all the methodologies and frameworks that they must apply in their organization and even more so without the presence of the IT specialist.

In this context, a methodology is proposed based on the ISO 38500 standard, which establishes evaluation and control in the organization. It is important to differentiate between research that considers the existence of weak IT governance due to the absence of established guidelines and the complete absence of recognition of the need for IT governance.

Information Technology Governance refers to a framework of structures and processes intended to direct and supervise an organization to achieve business objectives and add value while balancing risks against IT performance and its processes.

Management is unaware of the importance of IT Governance in their organization; there is no concern about technological management, which generates value for the organization's performance and establishes continuous improvement and innovation in each of its processes.

Currently, the ideology of an organization without IT Government maintains a contract for cloud services, trusting in the availability of information ensured by the external provider without considering that the most vulnerable information is at the client's risk.

This is why organizations must consider the importance of a technology specialist or a good IT governance structure, which does not generate dependency but does generate good practices for the correct management of their information.

There are some vulnerabilities that organizations need to be aware of without IT governance:

- Inadequate IT management.
- In the organization there is no culture of responsibility, which considers constant monitoring of the availability of information.
- Since there is no IT Governance in the organization, users do not follow adequate responsibility for correctly managing information.
- There is no formality in managing IT policies as an organizational culture.
- Response times to business needs are not measured.
- There are no good practices for monitoring and executing tasks.
- There is no emergency and continuity plan of the business.
- There is no repository of continuous information.
- There are no procedure and process manuals in the IT area.
- There is no controlled annual budget for the management of IT support expenses.
- No indicators help the IT area identify possible risks and establish organizational improvements.

There are factors why senior management does not consider it important to keep an active technology staff in their company:

- Lack of knowledge of computer security
- Lack of budget
- Trust in external suppliers
- Rigorous methodologies, or frameworks not applied due to their complexity.
- Misconception of IT Governance is automatic governance.

It is important to note that with the pace of technology and even more so with artificial intelligence, the technological area is not governed automatically by instructions given.

A study on the strategic management of IT demand in organizations obtained exploratory results that most senior executives do not use standards or methodologies to manage the strategic demand for IT **Error! Reference source not found.**.

The research, through a survey of 130 people, identified that only one response applies ISO 38500; that is, it was identified that most companies do not apply IT governance guidelines [8].

In a presentation, Carlos Juiz **Error! Reference source not found.**an expert in information technologies, expressed the importance of implementing an effective governance framework in organizations. It is important to identify how a company manages IT governance. To efficiently apply ISO 38500 standards, IT administration must go hand in hand with senior management, with goals and objectives, and this can be achieved by increasing the use of information technology.

He also highlights the importance of carrying out a risk assessment that your organization currently maintains to act against any risk.

All these aspects of IT governance control trigger performance measurements of all executed projects and processes, finally highlighting that adequate IT governance maximizes the value of information technologies and minimizes risk. Video Carlos Juiz **Error! Reference source not found.**.

In the research, managers or senior management personnel will carry out a questionnaire in Qualtrics in a group of selected SMEs. What is surprising as expected data is that a question is asked: Does the company have an information technology area responsible for computer equipment and systems?

In all the countries considered, many companies do not have an associated technology area; according to **Figure *1*** in Ecuador, the percentage is around 45.8%.

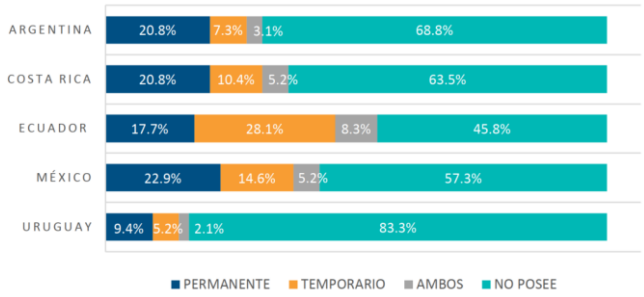

Figure 1. Effects of Digitalization on SMEs Error! Reference source not found.

This questionnaire identifies the importance of implementing structural methods or adding new areas in SMEs to adopt trends that drive solid growth. In most countries analyzed, most companies lack technical personnel specialized in information technologies, product research and development, or process innovation.

In a survey carried out in 2020, “Technological trends with the greatest impact in Ecuador”, the opinions of 180 business and technology leaders are collected; the aim is to know how innovation processes are applied in companies.

One of the questions asked, ¿What is your business operations' current technological support? This question seeks to identify the current state of companies and their technology adoption in various companies. In **Figure *2*** it can be seen in sectors such as banking, education and telecommunications, high technological support is reported. In other sectors of the companies surveyed, technological support is classified as medium and low level. These results confirm the absence of IT specialists in companies, worrying data that leads to deficient management of their technological infrastructure.

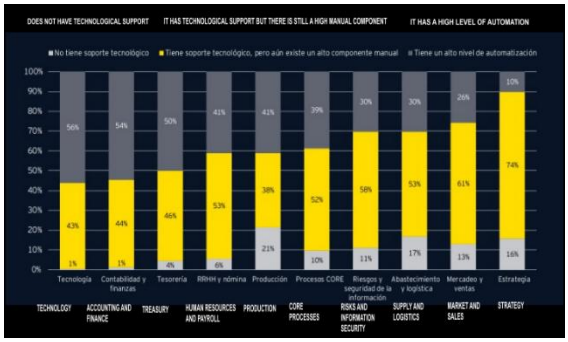

Figure 2. Technological trends with the greatest impact in Ecuador Error! Reference source not found..

The survey includes the following question: What are the main barriers and challenges that your organization faces in implementing its digital transformation agenda? The lack of budget, 50.6%, and the lack of defined business architecture may be indicators that neither the budget nor a well-defined IT Governance structure exists. **Figure *3***

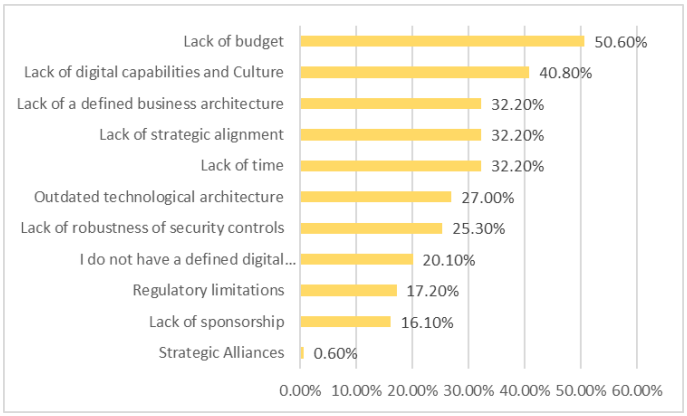

Figure 3. Technological trends with the greatest impact in Ecuador Error! Reference source not found.

III. THEORETICAL MODEL

IT governance:

The purpose of IT Governance in an organization is to promote the effective, efficient and acceptable use of information technology. It seeks to generate trust and objective evaluation and serve as a guide to establishing Corporate IT Governance.

Technological Responsible Governance:

This concept means a flexible and transformable tactic for governing Information Technologies (IT). It relies on entities' ability to react appropriately to technical changes and commercial demands.

Importance of IT governance in companies:

IT governance is essential for companies today since it establishes controls and guarantees that ensure the confidentiality, integrity and availability of information, as well as business continuity. It also helps improve strategic decision-making, aligning the organization's objectives with implementing information technologies. This leads to greater operational efficiency, lower risk of errors and better management of resources and costs. Finally, it is important to mention that IT governance is essential for the survival and success of companies **Error! Reference source not found.**.

ISO/IEC 38500:2008 establishes principles and guidelines for senior management to make effective information technology (IT) decisions, ensure alignment with corporate objectives, and maximize the value of IT investment **Error! Reference source not found.**.

COBIT is a framework that helps companies achieve their IT governance and management goals. Regarding copyright, COBIT is owned by ISACA, a non-profit professional association focused on developing, adopting, and using IT governance and information security knowledge and practices **Error! Reference source not found.**.

IV. TECHNIQUE

The work aims to generate a practical alternative to an IT Management problem by integrating some domains of good management practices in Information security. At the same time, a proposal will be created for organized management of an IT department, mitigating the risks generated by the absence of IT governance.

The technique of working with an initial approach is called "Initial step: Risk recognition based on three aspects", whose term we will call "R3ACC".

Senior management must identify all the services that represent the scope of their business.

In relation to the example in **Figure *4***, you can identify the action roles that allow effective administration for IT management, which must be identified as support, development, and constant monitoring.

IT Governance must apply good practices that ensure the availability of information and support business objectives.

The practices are a basis for IT management and can be framed in planning, organization, acquisition, service delivery, support and monitoring. This leads to reliability in the execution of good IT practices.

An IT Governance management scheme, in which constant monitoring is carried out on the services managed by the organization, does not exist. This problem produces negative results and errors in information management.

The company must know what work an IT department performs, and that is the first step in determining whether it complies with a control scheme.

Figure 4. Government Structure

Figure *4* shows how the assistance of a systems specialist in a company is crucial to guarantee effective monitoring and control and optimize technological resources. The specialist applies his or her knowledge and skills to safeguard information assets, manage risks, and maintain the proper functioning of systems. Likewise, it contributes to improving business productivity and efficiency, ensuring business continuity and promoting the appropriate and safe use of technology.

Not considering an IT Governance scheme in the company can lead to various challenges and problems. Without the IT manager, the organization may face difficulties monitoring and controlling its technological assets. This can lead to the inability to identify and mitigate security risks, such as vulnerabilities and cyber-attacks, which could compromise information confidentiality, integrity and availability.

It is important to consider that solving the functions of the systems specialist under an inappropriate role can trigger the generation of a greater number of problems, such as a lack of control over the performance and operation of the systems, which can affect the productivity and efficiency of the company's operations. Without proper management of the technology infrastructure, frequent outages, prolonged downtime, and difficulties in disaster recovery could be experienced, which could result in financial losses and damage to the company's reputation.

Lack of systems expertise can also lead to inadequate planning and execution of technology projects, which could result in delays, cost overruns, and low-quality deliveries. Additionally, the company may lack the ability to take

advantage of new opportunities and adapt to technological changes, which could affect its competitiveness in the market.

In SMEs, some small and medium-sized companies do not have IT management. If they do not, it is at least important to maintain hourly consulting, considering a support model based on good practices that can help the organization know the level of risk to which they are currently being subjected.

This article seeks to create a step-by-step model in which small and medium-sized companies can identify the degree of risk in their business activities, processes, and services. The objective is to identify the need for timely IT management to avoid future IT negligence.

Currently, several IT Governance methodologies have risk management chapters, but senior management refuses to consider them due to their complexity of implementation. This is why they seek to identify an organization's risk precisely.

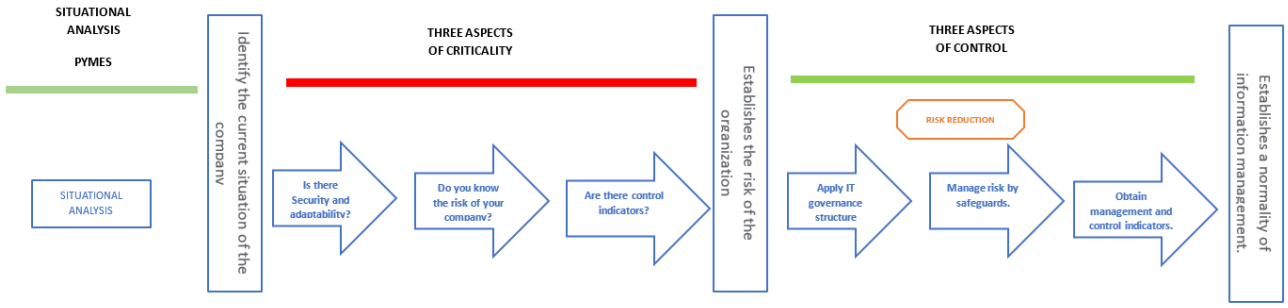

Figure 5 shows the **R3ACC** control model, on which senior management must know what are the initial actions that they must execute to know the current situation of the company:

1. Situational Analysis that involves knowing the level of risk in which the technology assets of the entire organization are found

2. Three critical aspects: corresponds to the identification of the current security that the company has.

3. Three aspects of control: corresponds to identifying documentation, good IT governance practices.

V. PROPOSED DESIGN: CONTROL MODEL

When we consider creating a quick technique, we intend to elaborate a guide where senior management can assess the organization's vulnerabilities in various aspects. This identification will be called IT Situational Assessment (VSTI).

This model proposes to validate the criticality and risk of the business by other managers of the organization considering three aspects:

i) Know if the company manages an IT Governance structure.

ii) Know the level of risk your business currently faces due to computer negligence.

iii) Carry out management IT indicators that can generate results, on which the company can monitor

and follow up on its processes and services.

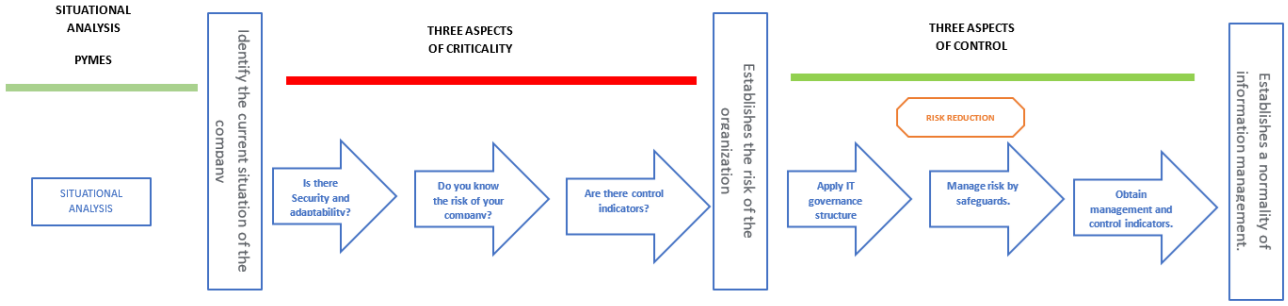

Figure 5 Situation and control model

Once the essential aspects have been validated in an organization, new improvement and control guidelines are established based on the following aspects:

iii) Know if there are process indicators on some critical business activities.

Once the essential aspects have been validated in an organization, new improvement and control guidelines are established based on the following aspects:

i) Review and apply what monitoring and control actions must be carried out to the company, maintaining a recurring IT Governance structure.

ii) Manage risk through corrective actions and safeguards that maintain timely availability of information.

iii) Carry out a file of management indicators that can generate results, on which the company can monitor and follow up on its processes and services.

a) Situational Analysis of SMEs:

The analysis of SMEs' situations implies evaluating the business environment, referring to the available technological resources and the organization's specific IT needs. This analysis allows one to understand the company's current landscape, identify problem areas, and identify opportunities for improvement related to technology.

It is important to have an IT specialist perform this analysis properly. This professional can evaluate the existing technological infrastructure, identify deficiencies, and propose solutions and improvements aligned with the company's objectives. Additionally, the IT specialist can assess the competitive environment and technology trends relevant to SMEs, which helps to make informed decisions about IT investments and growth strategies.

In many companies, despite arguing the importance of IT management, they choose not to hire the IT specialist, which is why it is suggested that the company consider the three aspects of analysis and use **Table *1*** of risk measurement to assess each asset and thus understand the level of risk to which the organization is subject.

				Qualitative Risk			
				High	Medium	Low	Average
Aspects	Name	Quantitative Risk (IFRS)	Value				
Government TI	Name1	Very High	5				
IT risks	Name2	Medium	3				
IT indicators	Name3	Very Low	1				

Table 1. Determination of risk in the company Error! Reference source not found.

b) Three Aspects of Criticality

1) Security: The security of technology assets is very important in all SMEs. An IT specialist is crucial in protecting and preventing all information the company handles. Companies should give greater focus to cybersecurity, which is undoubtedly a critical concept that goes hand in hand with ensuring the integrity and availability of information.

2) Performance and availability: The efficiency and performance of IT systems are another critical concern for all companies. An IT specialist can return the organization's infrastructure to peak performance by monitoring running systems and identifying bottlenecks to implement corrective changes. Additionally, the specialist can install contingency measures to ensure no system fails when needed and downtime is kept at zero for continued continuity.

3) Innovation and adaptability: In the current competitive environment, a company must constantly innovate and adapt to technological changes to maintain its current competitiveness. An IT specialist can identify trends, understand processes, and facilitate the implementation of appropriate technology solutions.

c) Three aspects of Control:

The three aspects of control refer to the need to have adequate control over the company's technological resources and IT operations:

1) IT Project Management: An IT specialist plays a crucial role in properly managing projects related to the implementation or upgrade of systems and technologies. An organized and well-planned approach is essential to ensure that IT projects are delivered on time, on budget and meet established requirements.

2) Supervision and maintenance: Monitoring and persistent supervision of IT systems and applications are necessary to ensure the effectiveness and security of their operation and avoid costly disturbances. The professional

is responsible for monitoring the systems' operation, installing new software versions and correcting technical errors to maintain the stability and accessibility of technological resources. This factor, like the previous ones, the company must determine if there are management indicators and what the operational performance is like.

3) Regulatory compliance: For several SMEs companies, complying with legal and regulatory requirements related to technology and information security is essential. An IT specialist can ensure that the company complies with associated regulations and standards, helping to avoid legal penalties.

Table 2 shows the format of the evaluation technique, which seeks to record the criticality levels detailed in **Table 1.** Once all the values of the "R3ACC" evaluation have been recorded, the indicator that determines the level is obtained. of risk in which the organization finds itself.

SITUATIONAL ANALYSIS PYMES		
Aspect	Applicable Control	Observations
Asset risk level		
THREE ASPECTS OF CRITICALITY		
Security		
Performance and availability		
Innovation and adaptability		
THREE ASPECTS OF CONTROL		
IT project management		
Supervision and maintenance:		
Normative compliance		
AVERAGE		

Table 2. Situational Analysis of SMEs

VI. ARTIFACT EVALUATION: CASE STUDY

For the evaluation, the SME company *"Laboratorios LIRA"* has been selected. Established in September 1977, *"Laboratorios LIRA"* launched antiseptic products on the market, covering the basic and essential needs for the health and well-being of ECUADORIANS" **Error! Reference source not found.**. The company does not maintain IT governance, nor does it associate the importance of its presence with the organization.

The organizational structure of the company does not have a systems specialist. The cloud modality is in charge of governing the company, which is why we sought to apply an assessment technique where it can be identified and evidenced in the company LIRA Laboratories, a small company dedicated to the production of pharmaceutical and cosmetic products in Ecuador, how the absence of a specialist in Information Technology (IT) generates a series of deficiencies in asset management and technology management. These deficiencies include the lack of information backups, the inadequate performance of user equipment, and the presence of technological obsolescence without being detected by senior management.

The company's lack of an IT specialist has led to inadequate management of technology assets. The absence of information backups implies a significant risk since data can be lost in the event of technical failures or security incidents. Additionally, poor performance of user equipment negatively impacts employee productivity and efficiency, resulting in additional costs and lost business opportunities.

Technological obsolescence is also an obvious problem at LIRA Laboratories. Without an IT specialist who provides advice and constant updating, the company is not able to identify and promptly address the need for technological renewal. This lack of strategic vision can lead the company to fall behind in the market, losing competitiveness compared to its competitors.

Having an information technology specialist is crucial to resolving these deficiencies and improving IT governance in the company. This professional would be responsible for establishing policies and processes for properly managing

technology assets, including implementing regular information backups. Likewise, the IT specialist would advise on acquiring and updating equipment, guaranteeing optimal performance and avoiding technological obsolescence.

When conducting the analysis, it is first identified that the company has not activated three critical aspects: safety, equipment performance and innovation.

The lack of security significantly exposes the company to a high level of cybersecurity, causing data loss and cyber-attacks. If the company does not achieve optimal performance in its operations, it will affect productive performance and competitive efficiency in the market.

The lack of availability of systems directly affects potential clients, suppliers, and employees. Without tools that directly support business continuity, they leave assets in technological obsolescence.

In control aspects, the company lacks IT projects, which indicate delays in implementing technological solutions. This is a competitive disadvantage of its Core business. Finally, the lack of regulations and complementary legal documentation in the IT environment prevents safe growth, affecting efficiency, security, and business process continuity.

SITUATIONAL ANALYSIS PYMES		
Aspect	Applicable Control	Observations
Asset risk level	5	
THREE ASPECTS OF CRITICALITY (3AC)		
Security	5	Does not maintain control and verification
Performance and availability	5	Equipment performance is not known
Innovation and adaptability	5	There are no updates
THREE ASPECTS OF CONTROL (3AC)		
IT project management	4	Projects are managed by Management
Supervision and maintenance:	3	The third-party provider manages the services and reports them
Normative compliance	5	There are system processes that must have a continuous process
AVERAGE	**4.57**	**High risk**

TABLE 3. SITUATIONAL ANALYSIS RESULTS OF SMES

VI. DISCUSSION OF RESULTS AND FUTURE WORK

In **Table 3**, applying the simple assessment technique, it can be deduced that the company is participating in a high-risk process management. Safety measures and protection to equipment are not applied, there is no adequate performance, and even more, they do not comply with formal procedures that act in the processes of the area.

This is why it is identified that the participation of an IT specialist is of great importance in companies where they mitigate the high risk that causes the company to fluctuate.

Innovation and development are fundamental aspects that must be coordinated with senior management; without an IT specialist, the company would be resulting in manual processes accompanied by technological obsolescence.

In the practical case, if the company does not establish control and monitoring of its systems and applications, we would indicate that in the future, this would affect production operations and regulatory entity validations.

It is of great importance that companies understand and know a new 3AC concept. That is, with a basic assessment, they have risk indicators and understand that digital transformation must go hand in hand with the company's senior management.

If, even after a brief assessment scheme, the company decides to continue with its digital operations in the cloud without IT control, the company could have service interruptions and loss of valuable information for the company. It is important to understand that we should always see how to protect the company's data. It is also important to maintain a culture of cybersecurity in the company, where its members are aware of the risks that may occur if, for example, they send mass emails from business accounts or click on advertising emails. Having a systems specialist is crucial to guaranteeing the operational efficiency of executing all processes and ensuring the security and availability of information.After applying the first initial step in the R3ACC technique, the second step must be hiring an IT specialist who can establish an IT Governance structure. As a third step, there must be a vision of applying a technique

of good IT governance based on COBIT or ISO 38500 **Error! Reference source not found.**.It is important to highlight that the control entities, current regulations, and frequent audits by the state towards companies are giving rise to evaluating the companies' behaviour. Being punctual with the pharmaceutical company, the current regulations of ARSA report 37 of good manufacturing practices require assessing everything regarding the validation of computer systems and their leadership.Likewise, the Ecuadorian Standardization Service INEN, in charge of promoting innovation, carries out assessments in companies so that companies establish standards and promote responsible practices in the quality of information management.Applying the initial valuation technique, the company does not have innovation, productivity and transformation value. Even when the company, in the practical case, justifies maintaining professional IT services, the assessment results do not change and remain high marks, which undoubtedly results in the company not working for its objectives and goals, giving, as a result, a very strong weakness in IT governance.

A consultation was carried out with SME companies with more than fifteen years in the market and as can be seen in **Figure 6**, the three companies focus their criteria on maintaining an IT expert who can ensure correct IT governance, reliability of the information and problem solving.

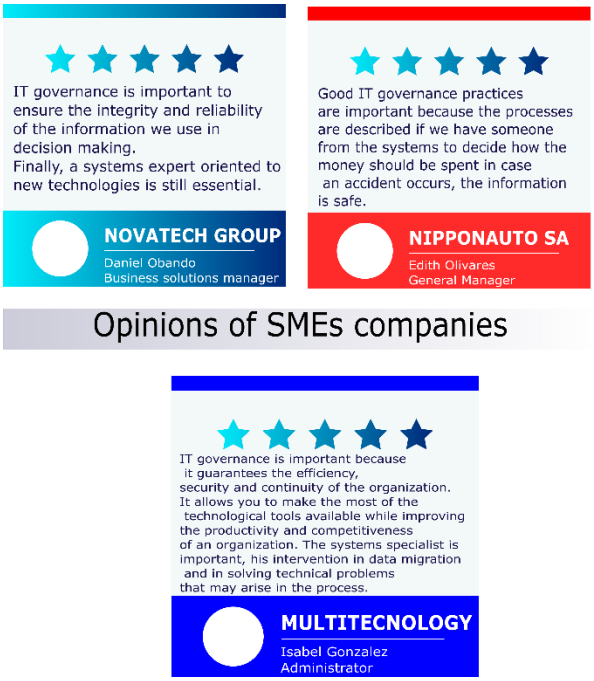

Figure 6. Critical thoughts of SME companies

If the critical thoughts of several authors and SMEs are collected, the balance would have to lean towards the importance of the IT systems specialist. There may be formal methodologies, but if no specialist governs them, they cannot be applied successfully.

That is why companies must evaluate whether they need to apply a series of formal methods or want to develop informal methods that contribute more to information security and reliability. See **Figure** *7*

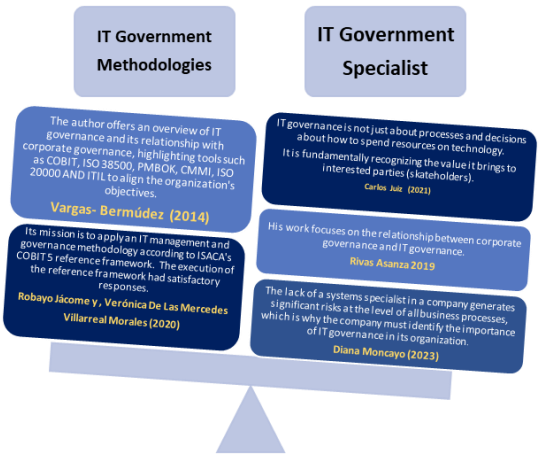

Figure 7. Critical balance

VII. CONCLUSIONS AND FUTURE LINES

No one denies the importance of IT governance, but new information technologies, cloud services, and artificial intelligence are undeniably transforming the current landscape. More and more organizations are adopting these solutions to improve their efficiency and competitiveness.

Senior management must support optimizing technological assets to drive the company's success and growth. It is recommended that methodologies such as COBIT be explored, which facilitate the establishment of clear processes and an adequate structure to effectively manage technology resources, including data, software, hardware, and architecture.

Companies must prioritize information security by implementing good project management practice models, which propose essential and adaptable regulations for an optimal process management environment. They must also consider addressing risks to guarantee potential business development.

There is a diversity of opinions regarding the need to incorporate a systems specialist into the company; external consultancies may exist, but they are not directly integrated with the business.

A consultation was conducted with companies in the market for over ten years. Their thinking is focused on the need for an IT specialist in their companies, given that they guarantee the reliability of the information and problem resolution becomes more effective.

With this technique, the general manager of a company is intended to acquire the essential knowledge of assessing the current situation of the systems area. This can lead to making decisions that can mitigate risks and thus safeguard the organization's information in its system.

In the future, this research will focus on a deeper analysis, where it will address how to eliminate that dependency on the IT role in the company and how to replace it with operational artificial intelligence; it is most likely that over time, a hybrid model will be created where there is IT management through two roles, one of the AI robots to create automation programs and the role of the IT specialist who will be in charge of making strategic decisions where his management intervenes in innovation and development.

In the upcoming time, advanced cyber threats are likely to increase, requiring the presence of on-site systems experts to implement and monitor security measures and safeguard cloud services against data vulnerabilities. Regular audits and rapid response to security incidents will be essential for IT specialists to ensure the security and confidentiality of business information.

The contracting of cloud services will have a series of higher characteristics and developments according to technological advances. In this context, systems specialists who understand the company's specific needs will optimize the performance and efficiency of cloud resources to ensure alignment with strategic objectives.

With time, artificial intelligence will likely execute the tasks of a systems specialist through programmed instructions, which ensure the reliability of computer systems and services. However, it is important to highlight that the role of the systems specialist will be essential to guarantee strategic decision-making for the organization. Even when the tasks are executed by a robot, the IT specialist oversees leading, managing, supervising, and innovating new solutions and IT Governance policies that are aligned with the correct management business.

REFERENCES

[1] V. Claudia, M. Mirna y M. Jezreel, «Characterization of Software Processes Improvement Needs in SMEs,» in International Conference on Mechatronics, Electronics and Automotive Engineering (ICMEAE), 2013.

[2] NU-CEPAL, Manual de la Micro, Pequeña y Mediana Empresa, San Salvador, 2009.

[3] World Bank/IFC, «Micro, Small, and Medium Enterprises Around the World: How Many Are There, and What Affects the Count?,» 2010.

[4] Parlamento Europeo, "La inteligencia artificial en la vida cotidiana," [En línea]. Disponible en: https://www.europarl.europa.eu/news/es/headlines/society/20180831STO10923/la-inteligencia-artificial-en-la-vida-cotidiana. [Accedido: 21-Mar-2024].

[5] National Geographic, "¿Qué es la inteligencia artificial?," [En línea]. Disponible en: https://www.nationalgeographic.es/ciencia/que-es-la-inteligencia-artificial. [Accedido: 21-Mar-2024].

[6] M. J. Schwartz, "La crisis de la ciberseguridad en tiempos de COVID-19," en *Reporte de Ciberseguridad 2020*, Banco Interamericano de Desarrollo y Organización de los Estados Americanos, 2020.

[7] J. P. Amón-Salinas y M. G. Zhindón-Mora, "Modelo de Gobierno y Gestión de TI, basado en COBIT 2019 e ITIL 4, para la Universidad Católica de Cuenca," FIPCAEC (Federación Iberoamericana de Asociaciones Científicas y Académicas de la Comunicación), vol. 5, no. 14, 2023. [Online]. Disponible en: https://doi.org/10.23857/fipcaec.v5i14.168. [Accedido: 24-10-2024].

[8] I. A. Alonso, J. C. Verdún, y E. T. Caro, "Case Study of Strategic IT Demand Management in Organizations - Exploratory Results," en CENTERIS 2013 - Conference on ENTERprise Information Systems / PRojMAN 2013 - International Conference on Project MANagement / HCIST 2013 - International Conference on Health and Social Care Information Systems and Technologies, Boadilla del Monte (Madrid), 2013.

[9] C. Juiz, 2021, "Secretos de un buen Gobierno TIC," Universidad de las Islas Baleares, disponible en: https://www.youtube.com/watch?v=2QUogGZoz40

[10] Martínez Estébanes, E., García Cano, J.C. (2011). "Gobierno de TI a través de COBIT 4.1 y cambios esperados en COBIT 5.0". Revista ECORFAN, enviado el 27 de Octubre, aceptado el 26 de Diciembre, pp. 6-8.

[11] ISO/IEC 38500, 2008. International Standard for Corporate Governance of Information Technology, First edition.

[12] F. A. Vargas-Bermúdez, "Marcos de control y estándares para el gobierno de tecnologías de información (TI) Control frameworks and standards for information technology governance (ITG)," Universidad de Boyacá, Colombia, 2014, pp. [número de página inicial]-[número de página final].

[13] D. J. Robayo Jácome y V. D. L. M. Villarreal Morales, "Convergencia de COBIT e ISO 38500 en el Gobierno de Tecnologías de la Información," Pontificia Universidad Católica del Ecuador, Ecuador; Universidad Estatal Amazónica, Ecuador, Autor por correspondencia: drobayo@pucesa.edu.ec; vvillarreal@uea.edu.ec, recibido el 20 de agosto de 2019, aceptado el 24 de enero de 2020. [En línea]. Disponible: https://orcid.org/0000-0002-0661-6573, https://orcid.org/0000-0002-6401-3404

[14] NU-CEPAL, Manual de la Micro, Pequeña y Mediana Empresa, San Salvador, 2009.

[15] World Bank/IFC, «Micro, Small, and Medium Enterprises Around the World: How Many Are There, and What Affects the Count?,» 2010.

[16] Price Waterhouse Coopers, IFRS for small and medium-sized entities, 2009.

[17] "Conócenos,"Laboratorios LIRA. [En línea]. Disponible: www.laboratorioslira.com. [Accedido: 10 10 2023].

[18] Feltus, C. (2023). "ISO/IEC 38500: Corporate Governance in ICT", Public Research Centre Henri Tudor, 29, Rue John F. Kennedy L-1855 Luxembourg, p. 20.

[19] I. Bartesaghi y W. Weck, "Los efectos de la digitalización, inteligencia artificial, big data e industria 4.0 en el trabajo de las PYMES en Latinoamérica," p. 59. [Online]. Disponible: [5]. [Accedido: dd-mm-aaaa].

[20] García, M. "Gobierno de TI: ¿qué es la ISO/IEC 38500 y para qué sirve?", Coding or Not, vol. 1, no. 1, pp. 1-1, Sept. 2018.

[21] Rivas Asanza, W.B. "Marco de Trabajo de Gobierno de Tecnologías de la Información Sostenible". Tesis Doctoral, Universidad de A Coruña, Programa de Doctorado en Tecnologías de la Información y Comunicaciones, 2019/20, dirigida por J. Andrade Garda y S. Rodríguez Yáñez, p. 41.

[22] Diana Moncayo y Carlos Montenegro, "Information security risk in SMEs: A hybrid model compatible with IFRS: Evaluation in two Ecuadorian SMEs of automotive sector," en Proceedings of the 2016 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), pp. 29-31, October 29-31, 2016.

[23] ESED - IT & Cybersecurity, "Razones por las que debes contar con un IT en tu empresa," en ESED - IT & Cybersecurity Blog, [fecha de acceso], disponible en: https://www.esedsl.com/blog/razones-por-las-que-debes-contar-con-un-it-en-tu-empresa

[24] EY Consulting y Revista IT ahora, "Tendencias Tecnológicas de Mayor Impacto en el Ecuador 2020 - Evolucionando Digitalmente los Negocios," EY,

[10-12-2023], disponible en: https://www.ey.com/es_ec/consulting/tendencias-tecnologicas-de-mayor-impacto-en-el-ecuador-para-el-a

[25] EY Consulting, “Tendencias Tecnológicas de Mayor Impacto en el Ecuador para el Año 2022: Evolucionando Digitalmente los Negocios,” EY, [12-03-2024], disponible en: https://www.ey.com/es_ec/consulting/tendencias-tecnologicas-de-mayor-impacto-en-el-ecuador-para-el-a1