Gyancity Journal of Electronics and Computer Science,
Vol.7, No.1, pp. 1-17, March 2022
ISSN: 2446-2918 DOI: 10.21058/gjecs.2022.71001

IMPLEMENTATION OF A MULTI-STANDARD INTEGRATED MANAGEMENT SYSTEM: ISO 27001, ISO 31000 AND ISO 22301 APPLIED TO SMES

Ulises Roman[1], Ulises Elguera[2], Luis Soto[3], José Piedra[4], Carlos Chávez[5]

[(1,3,4 y 5)] Teachers of the Department of Computer Science, Lima-Perú
[(2)] Graduate Student of the Faculty of Systems Engineering, Lima-Perú
nromanc@unmsm.edu.pe, ulises.elguera@unmsm.edu.pe, lsotos@unmsm.edu.pe ,
jpiedrasi@unmsm.edu.pe, cchavezh@unmsm.edu.pe

Abstract

In this article, it demonstrated research based on the implementation of an Integrated Management System (SIG) established in the ISO 27001 and ISO 22301 standards applied to SMEs. The main problem which is the aim to this study lies in the fact that, despite the measures adopted by the organizations in matters of information security or in the continuity of their commercial activities, the effective integration of the Information Security Management System (IIMS) and the Business Continuity Management System (SGCN) have not yet been established and, due to this, a SIG has been proposed that unifies these standards in a normative context through Annex SL and in a practical way based on the process of the Risk Management System (RMS) which is based on the ISO 31000 standard. Through the PDVA methodology (Plan - Do - Verify - Act), there is a mixture between qualitative and quantitative approach based on continuous improvement with which we can segment the requirements of each standard, avoiding duplication of documentation and guaranteeing the verification of its compliance. Likewise, the result was the integration of multi-standard management systems with the purpose to cover gaps related to information security and guarantee the recovery of SMEs in the event of incidents that could break down their activity through risk management for decreasing the impact for producing potential threats. Although it does no account with the certification, *there is a general compliance of approximately 45% in the implementation of its clauses.*

Keywords: *SMEs, integrated system, risk management, information security, business continuity.*

1. Introduction

Currently, companies carry out their activities in a context that has a constant change due to many factors ranging from the more traditional, such as competition, such as: resilience against to a pandemic. Consequently, the only way to survive and business success is to have a culture of innovation as the core of the business, with leaders with capacity for generating projects, initiatives and opportunities, which leads to add value to the organization's transformation process. In this sense, it is necessary to prioritize the interactions with customers through the digital channels which are directly related to taking advantage of new technologies. These constant efforts are the reasons for the sustainable development from company. Furthermore, the information and knowledge have been key factors for the evolution of companies despite having different concepts, these are related in the depth of their meaning since knowledge is formed by assimilated, information which is transformed and directed to the development of an activity or solving a problem, in conclusion, is a "know-how". Consequently, the constant dynamism of business, the evolution of products and / or services, technological advancement among other factors were the perfect combination to obtain a competitive advantage against the market because it reduced some barriers for doing business among them: improved processes, adapted new tools and thereby increased its income. However, today, the implementation of technology in organizations is a fundamental need for both small and large companies in their constant fight in the market. In the same way, the concept of technological surveillance was introduced like an organized process, constant in time whose purpose is to obtain internal and external information from the organization related with multidisciplinary issues and later, processing them with the purpose for producing knowledge, making decisions with lower risk and being able to anticipate changes, expanding a future proposal of the organization. Likewise, in parallel to all this evolution, standardization diferente organizations were formed which promotes the standardization of several approaches for the well-being of organizations and their objectives, among many approaches we have one key that involves information security, which involves aspects of confidentiality, integrity and availability, in addition, encompasses other properties, such as authenticity, non-repudiation, reliability and responsibility. Another standard approach is business continuity, which constitutes a conglomerate of strategies and plans that serve as a guide in response to any disruptive event which obtain a negative or catastrophic impact which affects the business continuity of the organization at a risk condition. Finally, another standardized approach is related to the risk management. according to this approach which gives an evidence the use of crucial components for the proper management: Principles, Framework and Process. Consequently, the organizational context was ideal for some companies to adopt competitive advantages because some organizations were able to provide products and / or services with unique and exclusive characteristics and which were permanent over time so they were also perceived and valued by their customers. As a result, there were several management systems, among of them: the information security management system, the business continuity management system, and the risk management system. At this point, the authors (Gomez & Fernández, 2015) affirmed which: “The information security management system (ISMS) is a set of processes that allow to establish, implement, maintain and continuously improve the information security, taking as a basis the risks that the organization faces”. (p.11). In addition, the (International Organization for Standardization - ISO 22301: 2012, 2012) stated that: “The business continuity management system is part of the general management system which establishes, implements, operates, monitors, reviews , maintains and improves business continuity ”. Therefore, it is correct to integrate management systems which strategically combine the processes of an organization in a complete framework, which allows the organization to operate as a unit through the cohesion of its objectives. In other words, an organization that has an integrated system will become a unified whole, possessing characteristics aligned with a single objective: optimizing the performance of the entire organization. In this sense, the authors (Karwowski & Salvendy, 2010) argued that, “integrated management is relevant for any organization, regardless of its size or sector, seeking to integrate two or more of its management systems in a cohesive system with a set holistic documentation, policies, procedures and processes ”(p.962).

2. State of the art

2.1. Information Security Management System (ISMS)

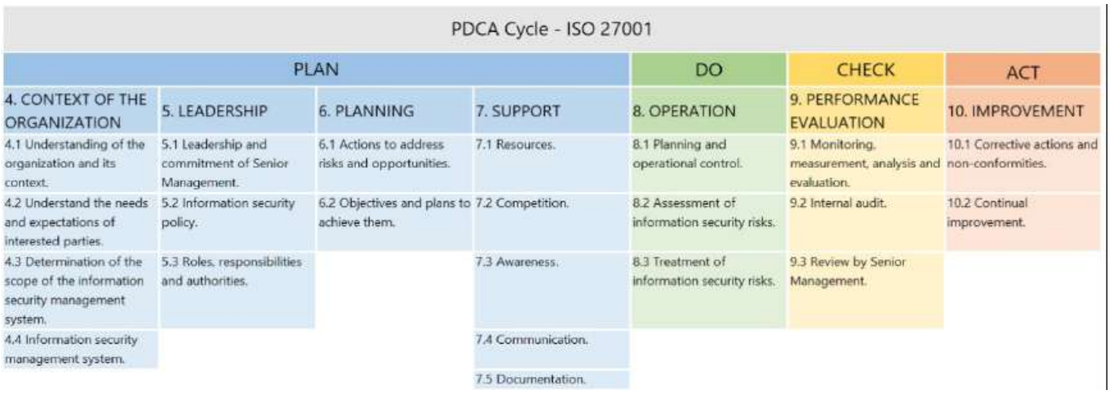
It is a systemic approach which is about the set of policies, procedures and guidelines to establish, implement, operate, monitor, review, maintain and improve the security of the information from an organization and achieve its commercial and/or service objectives.

According to the research "Establishment, implementation, maintenance and improvement of an information security management system, based on ISO / IEC 27001: 2013, for a software consulting company" by the author (Santos Llanos, 2016) which suggests the 27001 standard is complemented by other ISO standards which explain in greater detail how its requirements meet your goal, such as ISO 31000: 2009, which is referenced as a framework for context and risk management. In sum, ISO 27001 is an integrable standard with other ISO standards, the approach will depend on the type of organization and objectives that SMEs have.

In accordance with the normative structure from ISO 27001 and its relationship with the Plan - Do - Check - Act methodology, which demonstrates the structured Clauses and Sub-clauses from the Standard ISO 27001. As shown in Figure 1.

Figure 1

Structure of the Clauses of ISO 27001



PDCA Cycle - ISO 27001						
PLAN				DO	CHECK	ACT
4. CONTEXT OF THE ORGANIZATION	5. LEADERSHIP	6. PLANNING	7. SUPPORT	8. OPERATION	9. PERFORMANCE EVALUATION	10. IMPROVEMENT
4.1 Understanding of the organization and its context.	5.1 Leadership and commitment of Senior Management.	6.1 Actions to address risks and opportunities.	7.1 Resources.	8.1 Planning and operational control.	9.1 Monitoring, measurement, analysis and evaluation.	10.1 Corrective actions and non-conformities.
4.2 Understand the needs and expectations of interested parties.	5.2 Information security policy.	6.2 Objectives and plans to achieve them.	7.2 Competition.	8.2 Assessment of information security risks.	9.2 Internal audit.	10.2 Continual improvement.
4.3 Determination of the scope of the information security management system.	5.3 Roles, responsibilities and authorities.		7.3 Awareness.	8.3 Treatment of information security risks.	9.3 Review by Senior Management.	
4.4 Information security management system.			7.4 Communication.			
			7.5 Documentation.			

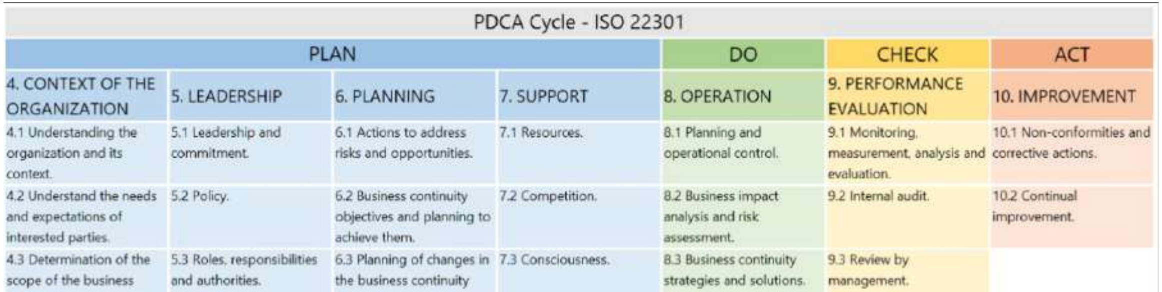
Note. The ISO standards document prioritizes a homogeneous structure in the standardized models.

2.2. Business Continuity Management System (BCMS)

Also, it is a systemic approach which is related to the group of policies, procedures and guidelines and aid to the torganizations to prepare for emergencies, to manage the crises and improve their operational recovery capacity, ensure the supply chain and protect themselves, for example, your reputation in a crisis. In addition, according to the author's research (Delgado Concha, 2015), he told us about the "Design and Proposal of a Methodology for the Implementation of a Business Continuity Management System based on the ISO / IEC 22301: 2012 Standard", regardless of the size of the company, sector or type of organization which they should implement a BCMS as a systematic and orderly process. Similarly, ISO 22301 is also an integrable standard with other ISOs, and this integration will depend on the measures and scope that SMEs approach to solve a problem or prepare for it. Likewise, through the relationship between ISO 22301 and the Plan-Do-Check - Act methodology, it is possible to illustrate the Clauses and Subclauses of the ISO 22301 Standard in a structured way. As shown in Figure 2.

Figure 2

Structure of the Clauses of ISO 22301



PDCA Cycle - ISO 22301						
PLAN				DO	CHECK	ACT
4. CONTEXT OF THE ORGANIZATION	5. LEADERSHIP	6. PLANNING	7. SUPPORT	8. OPERATION	9. PERFORMANCE EVALUATION	10. IMPROVEMENT
4.1 Understanding the organization and its context.	5.1 Leadership and commitment.	6.1 Actions to address risks and opportunities.	7.1 Resources.	8.1 Planning and operational control.	9.1 Monitoring, measurement, analysis and evaluation.	10.1 Non-conformities and corrective actions.
4.2 Understand the needs and expectations of interested parties.	5.2 Policy.	6.2 Business continuity objectives and planning to achieve them.	7.2 Competition.	8.2 Business impact analysis and risk assessment.	9.2 Internal audit.	10.2 Continual improvement.
4.3 Determination of the scope of the business	5.3 Roles, responsibilities and authorities.	6.3 Planning of changes in the business continuity	7.3 Consciousness.	8.3 Business continuity strategies and solutions.	9.3 Review by management.	

Note. The document prioritizes a homogeneous structure in standardized models.

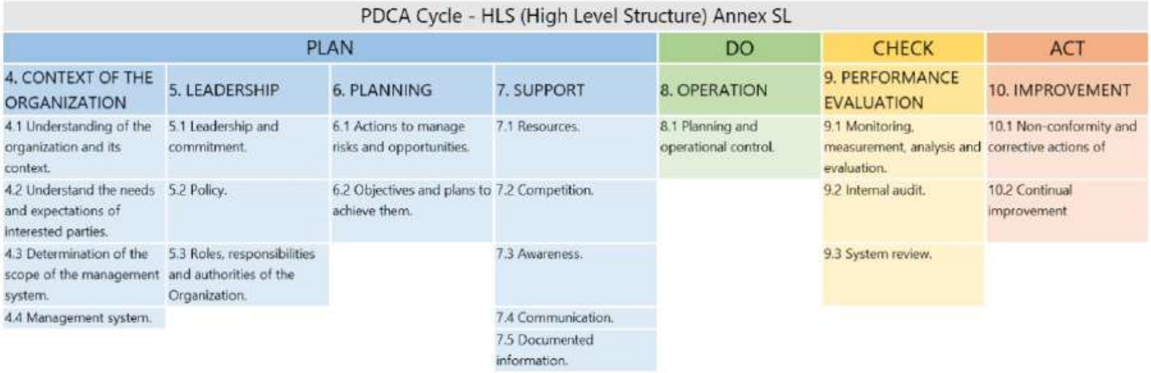
2.3. Risk Management System (SGR)

It is the consolidation of the risk management process through principles, reference framework and processes, which through a cyclical approach guarantee its application is repeatable and transversal for every processes from the organization. Furthermore, risks are managed not only at a global scale, but also at the scale of every area. This leads which every SMBs stop reacting to events or incidents, and start to opérate in proactively and predictively way faced all of them. Based on the proposal by the author (Martinez Torre-Enciso & Casares San José Martí, 2011) mentions that, “Risk management in a global environment is emerging as a financial and business strategy which provides an important competitive advantage to the companies with these tools". Therefore, risk management must be taken as a crucial factor for the improvement and permanence of the processes of SMEs.

2.4. Integrated Management System (IMS)

The global concept of a GIS is related to the interoperability of the systems which belongs to the organization, the degree of compatibility between these systems and the maturity of the organization's processes. On the other hand, it is possible to conceptualize it as a tool that makes possible the integration of data and the processes of an organization in a comprehensive system. According to the research of the authors (Navarro Monterroza, Pérez Extremor, & Estrada Muñoz, 2016) stated that: "The implementation of a SIG must meet the established requirements by current legal regulations, subsequently determines the importance of management related with the implementation of the program, which is vital in the creation of a quality and safety management process because this area will be attributed the responsibility of operating the integrated system”. In conclusion, it is possible to affirm that a GIS based on the ISMS, the SGCN and the SGR focuses on guaranteeing the confidentiality, integrity and availability of the information, ensuring the continuity of the services provided by SMEs. In conclusion, through the relationship between ISO 27001 and ISO 22301 with the Plan - Do - Verify - Act methodology, it is possible to showed a structured way, the cohesion of the Clauses and Sub-clauses of the ISO standards, likewise, the term " Annex SL ”which is responsible for optimizing matches and avoiding duplication in the use of resources, among other benefits. As shown in Figure 3.

Figure 3
Structure analyzed and proposed in accordance with Annex SL



PDCA Cycle - HLS (High Level Structure) Annex SL						
PLAN				DO	CHECK	ACT
4. CONTEXT OF THE ORGANIZATION	5. LEADERSHIP	6. PLANNING	7. SUPPORT	8. OPERATION	9. PERFORMANCE EVALUATION	10. IMPROVEMENT
4.1 Understanding of the organization and its context.	5.1 Leadership and commitment.	6.1 Actions to manage risks and opportunities.	7.1 Resources.	8.1 Planning and operational control.	9.1 Monitoring, measurement, analysis and evaluation.	10.1 Non-conformity and corrective actions of
4.2 Understand the needs and expectations of interested parties.	5.2 Policy.	6.2 Objectives and plans to achieve them.	7.2 Competition.		9.2 Internal audit.	10.2 Continual improvement
4.3 Determination of the scope of the management system.	5.3 Roles, responsibilities and authorities of the Organization.		7.3 Awareness.		9.3 System review.	
4.4 Management system.			7.4 Communication.			
			7.5 Documented information.			

Note. ISO document prioritizes a homogeneous structure in standardized models (SL)

2.5. Multi-standard systems in SMEs

The standardized systems applied to SMEs leads to the traceability and understanding of the processes, implementing models of information security, continuity, risk treatment, quality, among others. According to (Hallikas, Lintukangas, & Kahkonen, 2020), to ensure the sustainability of companies (SMEs) it is important to leads to the supply chain in purchasing management and the risks which generated, so it will be more likely to best performing in its purchasing and supply management. For (Rezaei Soufi, Esfahanipour, & Akbarpour Shirazi, 2020), through synergy and its possible reduction of the risks, the impact and the probability that it generates, it is important to prioritize the contingency plans, all the uncertainties of the problem must be considered with a comprehensive vision. (Taarup-Esbensen, 2021) points out that organizations such as SMEs must overcome events that affect security and critical value-added activities through business continuity plans and organizational capabilities and competencies.

3. Methodologies.

The methodology used in this research is based on a systemic and disciplinary sequence of steps which leads to the integration of the Information Security Management System-ISMS, the Business Continuity Management System-BCMS and the Risk Management System–RMS. Through the established methodology, can be focussed the guidelines with the aim of establishing and evaluating the unification process from the management systems, at the same time, prioritize the development of SMEs by integrating totally or partially the called systems with the purpose of a greater efficiency.

3.1. Plan - Do - Check - Act

According to the publication performed by the author (Deming, 1989), the PHVA is a: "Simple and iterative management approach to test changes in processes or solutions to solve problems, and promote their continuous optimization during the time". The approach, well-known in the present as the PDCA cycle, is designed to be completed and repeated over and over again.

3.2. Benchmarking

According to the analysis of the aforementioned methodologies and their relationship with respect to the concepts for integrating systems, maturity, information security, business continuity, risk management, among others, the following results are obtained:

Table 1

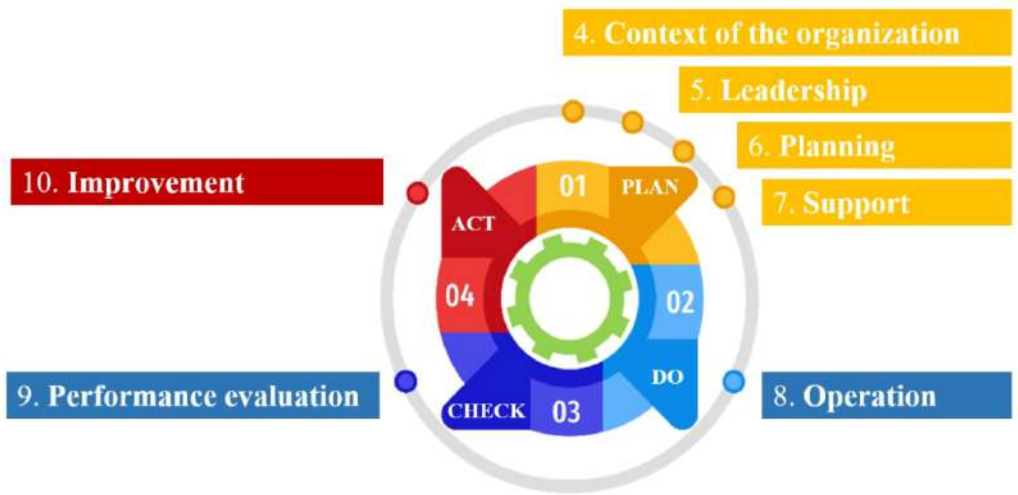
Quantitative evaluation of the main related methodologies.

	MATURITY	RISK	CONTINUITY	SECURITY
COBIT® 2019	4	3	4	4
MAGERIT V3	4	4	3	3
UNE 66177:2005	3	3	4	3
PHVA	4	4	4	4

It is appropriate to declare confidently through the risk management, there is congruence with ISO 27001 (information security), ISO 22301 (business continuity), cybersecurity and, consequently, the information technologies, being a key point for the integration based on similarity and standardization criteria´s, and as a result from the analysis performed for the methodologies related with the researching, it is concluded that the PDCA methodology is a holistic approach and is keeps consistent relationship with factors established in the integration. As shown in Figure 4.

Figure 4

Deming cycle applied to standards integration



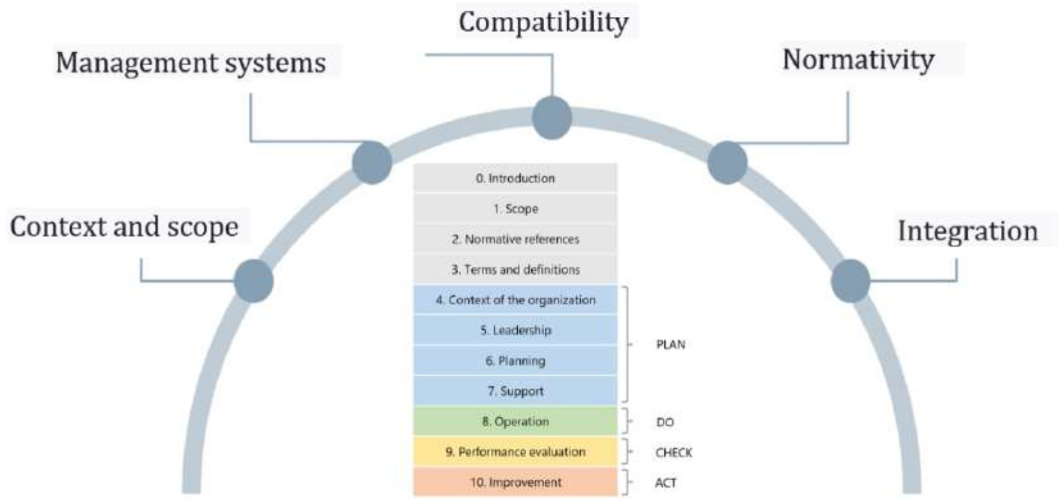
Note. The Deming cycle related with the improvement processes by restarting their continuous evaluation periodically

4. Results.

The integration of the management systems is materialized through the use of a High Level Structure or also called Annex SL, which includes the homogenized and standardized clauses from the information systems which influences this cohesion. The used integration´s architecture for the SIG is constituted by ISO 31000 (SGR), ISO 22301 (SGCN) and ISO 27001 (SGSI), where the 10 clauses in the High Level Structure are defined; also, in a complementary mode to the Annex SL is proposed to the use of Annex A, a document belonging to the ISO 27001 standard which contains a series of applicable controls according to the context and scope of the organization. As shown in Figure 5.

Figure 5

Factors involved in the integration of the GIS.



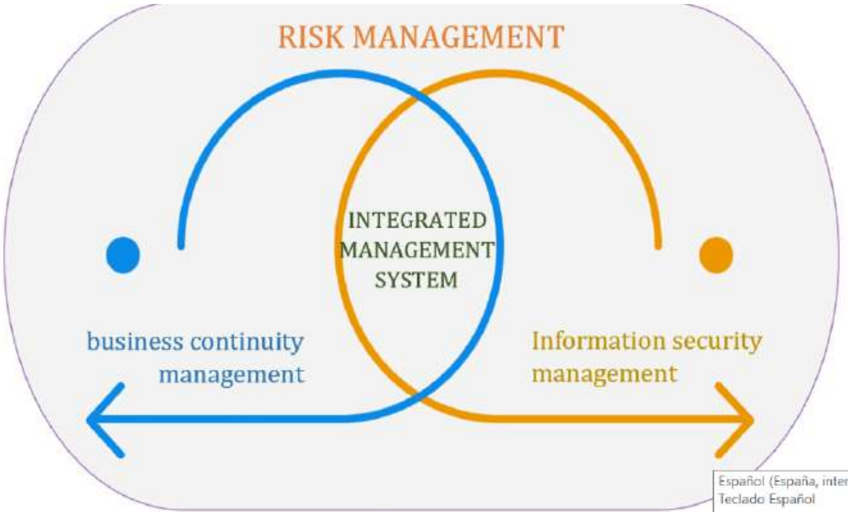
Note. The factors involved are related with the current regulations of the applied standards.

According to the normative form of integration, there are various deliverables are related to the GIS:

4. *Context*: (Identification of interested parties, Identification of applicable regulations and Scope of the S.I.G).
5. *Leadership*: (S.I.G Policy, S.I.G Roles and Responsibilities)
6. *Planning*: (Objective of the S.I.G, Methodology and risk treatment, Risk treatment plan and Statement of applicability - SOA).
7. *Support:* (S.I.G Training Plan, S.I.G Awareness Plan, S.I.G Communication Plan and S.I.G Documents).
8. *Operation*: (Measurement of the S.I.G, Management of changes in the S.I.G, Business Impact Analysis - BIA, Risk Assessment Matrix and Risk Treatment Plan).
9. *Performance Evaluation*: (S.I.G Audit Program, S.I.G Internal Audit Plan, Internal Audit Report and Management Review).
10. *Improvement*: Corrective Action Request.

In the same way as shown in Figure 6, the practical form of integration includes factors which contribute to the congruence of information systems, such is the case of risk management, which is valued in the Security Information Management System and in the Business Continuity Management System. According to the framework of the proposal, which should integrate standards based on safeguarding the information and guaranteeing the persistence of business activities and is necessary to establish convergence criteria, such is the case of Risk Management.

Figure 6
Practical factors involved in the cohesion of S.I.



Note. The practical factors directly identify risk management as a common factor in relation to the different standards.

Therefore, based on the proposed methodology of the PHVA is formed by a sequence of steps to follow which will be performed by cyclically mode each time it is necessary in search of continuous improvement.

4.1. Plan

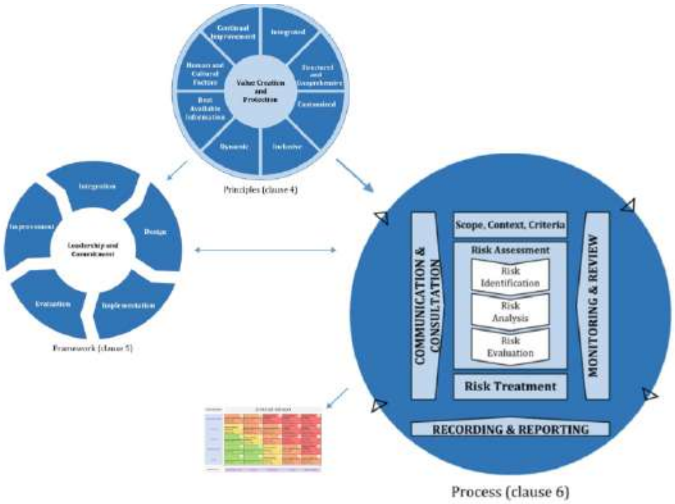
The organization analysis is carried out according to its context and its internal processes, determining the current state, the scope of the implementation and its similar regulatory requirements.

4.2. do

The process of integration of the ISO 27001 related with the standard of Information Security and ISO 22301 standard related to the Business Continuity which are achieved through an adequate risk management, in accordance with this premise, the effective risk management which is based on: Principles, Reference Framework and Process. All of these components belong to ISO 31000 related to the Risk Management.

Figure 7

Components of Risk Management. ISO 31000



ISO 31000, through the risk management process involves a systemic set of policies, procedures and practices in the 6 applications. Here are there are 6 applications integrated into the risk management process. In accordance with the scenario proposed by ISO 31000 Standard, it turns important in the organization, provides an effective and suitable risk management process which achieved through a proposal scheme by this standard which integrates 6 applications in a systemic set to risk management:

1. *Communication and consultation*:
According to this application, the organizations seek to gather information through the different means to publicize or exchange information based on the company's own facts, considering confidentiality and integrity of the information.

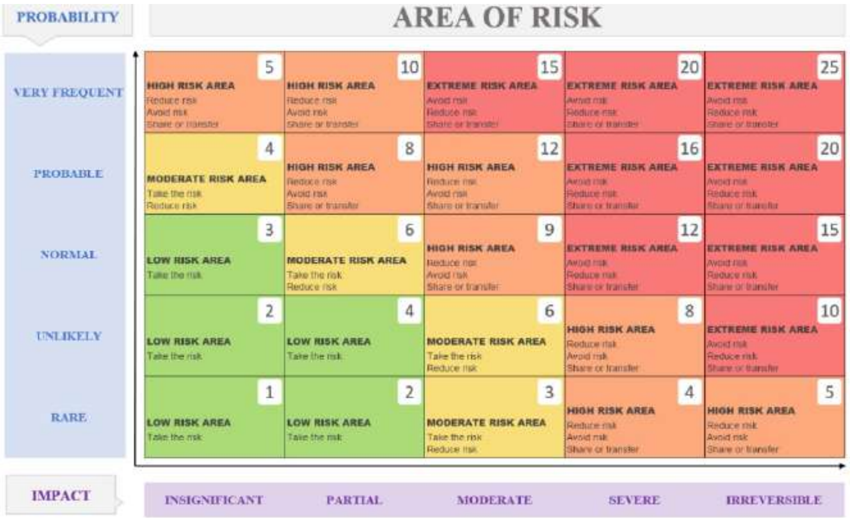
2. Scope, context, and criteria:
Regarding this application, the organization should define the edges that comprise the scope and evaluating its environment (internal and external), in order to achieve its objectives.

3. Risk assessment:
This application contains a set of processes which identify, analyze and value the risk, due to this, risk assessment has a systemic study.

- Risk Identification: For this process, it must be recognized which are the main risks for which the company is exposed; subsequently, secondary risks must be consider which could also cause possible damage to the company.

- Risk Analysis: after the identification of risks, in this process it must the nature of the risk and its characteristics containing the risk level must be understood; also, this implies considering factors such as: the effectiveness of the existing controls, the probability of the events and the consequences, as well as the nature and magnitude of the consequences, in the same way, the complexity and interconnection, in addition, the factors related to time and volatility, finally, the levels of sensitivity and trustworthy.

Figure 8
Segmented and valued Risk Matrix



PROBABILITY	AREA OF RISK				
VERY FREQUENT	5 HIGH RISK AREA Reduce risk Avoid risk Share or transfer	10 HIGH RISK AREA Reduce risk Avoid risk Share or transfer	15 EXTREME RISK AREA Avoid risk Reduce risk Share or transfer	20 EXTREME RISK AREA Avoid risk Reduce risk Share or transfer	25 EXTREME RISK AREA Avoid risk Reduce risk Share or transfer
PROBABLE	4 MODERATE RISK AREA Take the risk Reduce risk	8 HIGH RISK AREA Reduce risk Avoid risk Share or transfer	12 HIGH RISK AREA Reduce risk Avoid risk Share or transfer	16 EXTREME RISK AREA Avoid risk Reduce risk Share or transfer	20 EXTREME RISK AREA Avoid risk Reduce risk Share or transfer
NORMAL	3 LOW RISK AREA Take the risk	6 MODERATE RISK AREA Take the risk Reduce risk	9 HIGH RISK AREA Reduce risk Avoid risk Share or transfer	12 EXTREME RISK AREA Avoid risk Reduce risk Share or transfer	15 EXTREME RISK AREA Avoid risk Reduce risk Share or transfer
UNLIKELY	2 LOW RISK AREA Take the risk	4 LOW RISK AREA Take the risk	6 MODERATE RISK AREA Take the risk Reduce risk	8 HIGH RISK AREA Reduce risk Avoid risk Share or transfer	10 EXTREME RISK AREA Avoid risk Reduce risk Share or transfer
RARE	1 LOW RISK AREA Take the risk	2 LOW RISK AREA Take the risk	3 MODERATE RISK AREA Take the risk Reduce risk	4 HIGH RISK AREA Reduce risk Avoid risk Share or transfer	5 HIGH RISK AREA Reduce risk Avoid risk Share or transfer
IMPACT	INSIGNIFICANT	PARTIAL	MODERATE	SEVERE	IRREVERSIBLE

At the same time, the degree of impact must be estimaded which an organization could suffer as a result of the unexpected occurrence of an incident or disaster. The BIA analysis allows to estimate possible necessary resources to identify the organization's processes, especially which represents greater sensitivity in relation to time and impact.

- *Risk assessment*: in this process, the results obtained are benchmarked in order to determine the actions to be taken. The decisions resulting from the risk assessment must take into account the context, consequences and perception of the interested parts.

4. Risk treatment

Risk treatment focuses primarily on the selection and subsequent implementation of the options chosen to address risk.

This implies which:

(1) Expectations are formulated for the risk treatment
(2) The most suitable alternative is selected
(3) Risk treatment is properly planned and implemented
(4) The effectiveness of the implemented actions is evaluated.
(5) The residual risk is quantified and qualified according to its acceptable and unacceptable result and
(6) The residual risk treatment has not been accepted.

5. Monitoring and review

The purpose of monitoring and reviewing the risk management whose aim is progressively guarantee the quality and effectiveness of the design, as well as the implementation and results obtained from the process.

6. Record and report

In accordance with the foregoing, it must evidenced the raised and executed, as well as reported the positive and negative results through the appropriate mechanisms.

4.3. Check

According to this stage, the development of the implementation of an Integrated Management System is based on conducting audits and reviews by management. Monitoring and follow-up elements are also integrated in this phase, such as the progress achieved in accordance with the objectives or indicators that have been determined.

4.4. Act

Finally, in this stage of 'taking action', the organization decides on the application of the concepts of corrective and preventive action to be taken, or the adoption of agreements based on the analysis, as given in the reviews carried out by the direction. Likewise, the completion of this stage leads the company to rethink what was planned and the cycle continues without end, which causes continuous improvement.

5. Discussion

According to the research, different aspects are considered for the development of an integrated management system in SMEs which has main factors of integration of standards based on information security, business continuity and risk management, it also has information on interviews, surveys and the results of the implementation of ISOs in the integration, then we proceed to describe the results obtained according to the following analyzes:

- Analysis of results on the ISMS.

Regarding the results obtained, the implementation of an ISMS would have a beneficial impact on the company, taking into account which Peru has started a culture of standardization in several areas, information security being a crucial axis when digitizing services that the company delivers internally as well as externally.

The initiative to implement an ISMS brings with its several benefits, the most important of which is to minimize the risks in terms of confidentiality, integrity and availability, identifying threats, vulnerabilities and impacts on information assets, guaranteeing the continuous improvement of the security information in the organization. Similarly, the implementation of the ISMS is adaptable to the other standards, including Annex A, which contains the controls that will be supported according to their use in the Statement of Applicability.

- Analysis of results on the SGCN.

According to the obtained results, the implementation of a SGCN would also have a positive impact on the company, considering which Peru has initiated a culture of standardization in several areas, with business continuity being an underdeveloped sector. The initiative to implement a BCMS brings with it several benefits, the most important of which is to guarantee the continuity of your business by protecting it from various events that could jeopardize the company's commercial activities, as well as helping to prepare for emergencies, manage crisis, improving recovery capacity, maintaining reputation against risks or for example secure the supply chain.

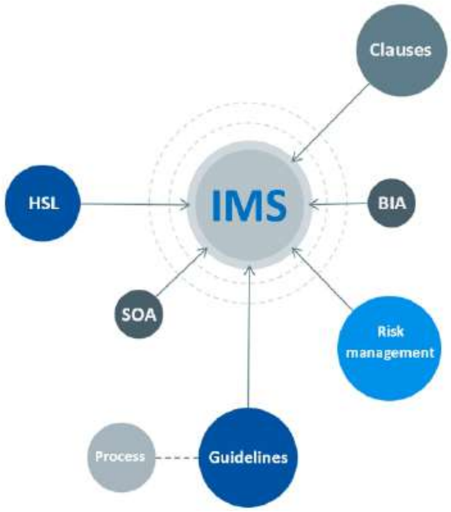
- Analysis of results on the SGR.

According to the obtained results, the implementation of an SGR would also have a positive impact on the company, considering that risk management systems which are designed for doing more than just identify the risk; in this sense, ISO 31000 standard based on 3 guidelines : Principles, Reference Framework and process, provides a continuous scheme for risk management which creates and protects value in the company, in accordance with the process of these 3 guidelines.

- Analysis of results on the integration architecture.

The architecture proposed for the integration of the management systems will strategically understand the benefits of the ISOs involved, guaranteeing the security information and the continuity of the commercial activities from the organization through the adequate risk management, a general map of the structure proposed for the GIS and the main requirements for its implementation is showed:

Figure 7
GIS integration model proposal



6. Conclusions.

A GIS model applied to SMEs was designed and implemented, through which different standards were effectively involved, based on the ISOs, 27001, 22301 and 31000 standards. The performed integration of promoting the use of strategies based on protection and Information security; also, provides competencies in the resumption of business activities and finally provided control in the adequate management of risk. The integration of the 22301, ISO 27001 and ISO 31000 management systems were performed through the High Level Structure (HLS), which unifies and considerably reduces the use of resources, since many of the requirements demanded for each one of these standards are similar and only vary in focus; likewise, it has been possible to use the common documentation which require to protect the information and ensure the recovery of the organization faced for incidents which may interrupt its activity through risk management trying to minimize the impact of possible threats. As part of the integration, the ISMS contributed to the unification process through of a set of measures and requirements aimed at guaranteeing the protection of information against any threat, such as: cyber attacks, bad practices by the employees themselves, intruders or natural disasters; through the application of controls and the establishment of security procedures. Similarly, through the SGCN, a strategy was applied focused on ensuring the company's activities, avoiding cessation or interruptions due to certain incidents, thus reducing possible losses that could occur. Likewise, in relation to this management system is essential to perpetuate an educational strategy focused on exploiting the capacities of the company's workers, with the aim of strengthening their degree of response to the potential risk situations, proceeding based on the plans established, thus mitigating the interruption time. Under the application of the Plan - Do - Verify - Act (PDVA) methodology, it was possible to avoid duplication of requirements and regulations related to the integration of multistandard systems, since through these 4 stages allowed us to re-evaluate the processes and suitable management of risks in several times, in a cyclical way, thus ensuring continuous improvement, increased productivity and its unlimited applicability in the organization's processes. Finally, through the adequate risk management based on ISO 31000 standard, the integration of the SGR in the SIG considered the collection of requirements with the purpose to mitigate the risks that could threaten the organization. Likewise, through this management system the potential risks that could generate problems in the performance of the company, through the economic consequences or which affect the image of the organization. In addition, the Risk Management based on the ISO 31000 standard establishes “the principles, the frame of reference and the process”, precisely in the processhas been developed: the evaluation, identification, analysis, assessment and treatment of risks according to the performed study with a common factor of the aforementioned standards is the performance of risk management, reason which it has been taken as a link between the ISO 27001 and ISO 22301 standards.

References

Delgado Concha, K. (2015). *Diseño y propuesta de una metodología para la implementación de un sistema de gestión de continuidad del negocio, basado en la norma ISO/IEC 22301:2012.* Universidad Católica de Santa María, Arequipa, Perú. Obtenido de http://tesis.ucsm.edu.pe/repositorio/bitstream/handle/UCSM/2236/44.0386.II.pdf?sequen

Deming, W. (1989). *Calidad, productividad y competitividad: la salida de la crisis.* Obtenido de https://dialnet.unirioja.es/servlet/libro?codigo=123126

Gomez, L., & Fernández, P. (2015). *Cómo implentar un SGSI según UNE-ISO/IEC 27001:2004 y su aplicación en el Esquema Nacional de Seguridad (.* Madrid, España: AENOR.

Hallikas, J., Lintukangas, K., & Kahkonen, A.-K. (2020). The effects of sustainability practices on the performance of risk management and purchasing. *Science Direct*. Obtenido de https://www.sciencedirect.com/science/article/abs/pii/S0959652620316267

International Organization for Standarization - ISO 22301:2012. (2012). *Societal Security - Business Continuity Management System - Requierements.* Suiza. Obtenido de http://www.smv.gob.pe/Biblioteca/temp/catalogacion/ISO22301_2012.pdf

Karwowski, W., & Salvendy, G. (2010). *Advances inhuman Factors Ergonomics and Safety in Manufacturing and Service Industries.* Taylor & Francis Group. Obtenido de https://www.routledge.com/Advances-in-Human-Factors-Ergonomics-and-Safety-in-Manufacturing-and/Karwowski-Salvendy/p/book/9781439834992#googlePreviewContainer

Martinez Torre-Enciso, M., & Casares San José Martí, I. (2011). *Dialnet*. Obtenido de El proceso de gestión de riesgos como componente integral de la gestión empresarial: https://dialnet.unirioja.es/servlet/articulo?codigo=3636068

Ministerio de Hacienda y Administraciones Públicas. (octubre de 2012). *Protal de Administración Electrónica*. Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Navarro Monterroza, C., Pérez Extremor, J., & Estrada Muñoz, J. (2016). *Guía de implementación del Sistema Integrado de ISO 9001:2008 - ISO 22000:2005, para* *empresas de producción de leche entera pasteurizada y queso fresco.* Universidad Pontificia Bolivariana. Obtenido de https://repository.upb.edu.co/handle/20.500.11912/6589

Rezaei Soufi, H., Esfahanipour, A., & Akbarpour Shirazi, M. (2020). Risk reduction through enhancing risk management by resilience. *Science Direct*. Obtenido de https://www.sciencedirect.com/science/article/abs/pii/S2212420921004581

Santos Llanos, D. (2016). *Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información basado en la ISO/IEC 27001:2013, para una empresa de consultoria de software.* Pontificia Universidad Católica del Perú, Lima, Perú. Obtenido de https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/7616

Taarup-Esbensen, J. (2021). Business continuity management in the Arctic mining industry. *Science Direct*. Obtenido de https://www.sciencedirect.com/science/article/abs/pii/S0925753521000333