International Journal on Advanced Science Engineering Information Technology

Vol.12 (2022) No. 3
ISSN: 2088-5334

Implementation of Information Security Audit for the Sales System in a Peruvian Company

Leoncio Cueva Ruiz [a,*], Misael Lazo Amado [a], Jeremy Rodrigez Carrasco [a], Laberiano Andrade-Arenas [a]

[a] *Department of Systems Engineering and Informatics, Universidad de Ciencias y Humanidades, Los Olivos, Lima, 15314, Peru*
*Corresponding author: *leocuevar@uch.pe*

Abstract— **Technology has been updated over the last few years, and this has been generating a worldwide impact as currently, in this pandemic, several companies have been victims of information theft through hacks, as some companies do not have audits so that they can protect their information. The management of computer security audits in companies is very important to detect possible risks and manage business control by applying continuity management in each disaster. The article's main objective is to implement an audit plan and information security through ISO 27001 for a sales system to improve computer security. The literature review is on the definition of several processes that are part of our implementation development. Our methodology employed five stages of project management (Start, Planning, Execution, Monitoring and control, and closure), explaining the procedure and definition of each stage. The case study is the development of each stage that identifies the risks and obtains a solution to any threat. The results are the treatments of the risks carried out in the company, explaining the compliance with the clause and controls of ISO 27001 in the company. Finally, the analysis of the indicators of each policy of the company to know the improvement the company Domingez.**

Keywords— **Audit; continuity management; information security; ISO 27001; project management.**

Manuscript received 11 Dec. 2020; revised 28 Apr. 2021; accepted 26 Nov. 2021. Date of publication 30 Jun. 2022.

I. Introduction

Lately, technology is increasingly important in our lives, especially in these pandemic times. However, the information we keep on our computers, cell phones, or devices with the Internet is not always safe. In some ways, we were the victims of a computer attack, and these types of attacks are critical to businesses when their information disappears, is damaged, or distributed; that is why in order to mitigate these cases, there are audits.

The ISO 27001 is considered a standard of information security. This helps avoid data loss in the company [1], thus having a standard certification ISO 27001 reflecting the information processes to develop attitudes toward security management [2]. Currently, issues related to computer auditing are becoming increasingly relevant, both nationally and internationally, because the training has become the most important asset of companies, representing their main strategic advantage, so they invest large amounts of money and time in creating information systems in order to obtain the highest possible productivity and quality [3]. The audit methods are based on identifying risks and analyzing the company or area of focus [4]. Information in organizations has become a very important asset that must be safeguarded and protected by different security tools [5]. Computer security is very important to help avoid some threats and vulnerabilities. The main problem that has been found is the lack of specialized personnel, as infiltrations or security flaws can be found that expose information to computer intruders [6]. In recent years, technological advances in Peru have made internal auditing a force to be reckoned with among management risks. In the government, according to the model of the government through the Institute of Internal Auditors (IIA), auditing fulfills three cornerstones for business management [7]. This includes the auditing of the board of directors, executive management, and external auditing. This determines the internal audit department responsible for adding strategic benefits to the organization where the sales system is implemented [8]. It is crucial for an application development professional to have full knowledge of IT auditing. All procedures should be obeyed and generate all documentation and product planning to be successful in external audit processes band.

The main objective is to implement an audit plan through the ISO 27001 standard to identify the problems found in the sales system of the Domingez company, allowing the improvement of the computer security of this process of the organization.

II. Materials and Method

Information security is important for both users and organizations [9], as they currently have security policies [10]. Information security is to defend information from unauthorized access, disclosure, and use, such as modifications, disruption, and inspection for confidentiality, integrity, and reliability, as seen in Fig. 1. Currently, with this coronavirus pandemic, there have been many cyber security attacks, such as data theft from people and organizations, generating concern at the global level. Information security has three important pillars (Confidentiality, Integrity, and Availability). Confidentiality ensures that the information is only accessible to the organization's authorized personnel. Integrity maintains the data accurately. It is not allowed to change or modify unless you have permission, and availability ensures that the data is available when needed [11].

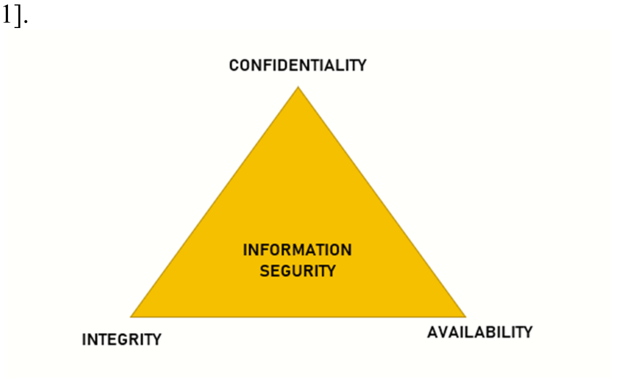


Fig. 1 Information Security

Information security risks help those involved make good decisions by assessing and understanding the risks. Organizations apply information security risks because they ensure they have a business strategy [12]. To identify these risks in organizations, it is necessary to analyze the critical assets in order to make plans to manage the risks. There are different methods for risk management, standards, guidelines, and specifications that remain available for risk assessment and management [13].

Compliance with information security policies is essential in organizations because it reduces the minimum of information security incidents [14]. However, the organization's employees who do not follow information security policies become internal threats [15]. Continuity management is a risk management process that allows counteracting the negative impacts of future threats (fires, earthquakes, pandemics, among others) to the continuity of the organization's activities [16].

The information security provides different types of security management in charge of studying by means of the 27000 series, allowing us to obtain all the technical requirements to reduce the risks of an infraction. This way, the ISO 27001 can examine the security risks that can threaten organizations' security to achieve their functional and strategic objectives. In the companies, it is applied to order, execute, elaborate, supervise, review, and administer information security management [17] to maintain the integrity, confidentiality, and availability of information. Another type of operation of ISO 27001 can be applied with the PDA (plan, do, check). This allows accelerating their processes for the time to perform a management [18].

Companies currently use the cloud server to store their information in case of computer problems or data loss. This helps to have better control when managing the ISO, allowing to adapt to the policies and objectives of the company [19]. These risks can be specified by theories, settings, principles, rules, and models [20].

It is important to have the controls to guarantee the security of the services and processes [21]. This has to be applied efficiently to take the importance of integrity, confidentiality, and availability, including all the stakeholders who participated in the company. Prioritizing security controls so that vulnerabilities and threats are not found [22].

Moreover, a widely used yet standardized project management framework was realized and grew over 30 years. This framework aims to standardize any project that is very focused on the managers of that work so that there is a greater likelihood of success in the project and is more reliable and more stable. When rejecting planning and rigid processes, try to increase the project's flexibility. In both cases, the objectives are the same: the success of the project and the client's maximum satisfaction [23]. The PMBOK management framework has as a standard to identify the good methodology of work and, at the same time to specify the common paths that exist in project management for structuring. In this way, in PMBOK the standard is similar to the aptitude for the one project in structuring concerning the development of the knowledge, tools, techniques, and skills needed for their correct use [24].

It consists of a plan which serves to recover from the disasters that are about to happen or that are already happening. It is a group of processes with which they could defend themselves and also obtain technical support again. Therefore, a company counts on different cases for its development if any type of natural disaster occurs that affects the organization [25]. This part of the method explains the five stages of the project management activities (Initiation, Planning, Execution, Control, and Closing) in which it served for the development of the work.

A. Start-up Stage

In this first stage, it is in charge of realizing the company's mission and vision to finally finish the process map.

1) Mission: The mission states the reasons for the organization's existence, including its services in the present [26]. Mission Domingez: The company Dominguez's mission is to distribute excellent quality wholesale and retail groceries to different customers with the best price and through a good service that provide a friendly treatment.

2) Vision: The vision is for the future and describes your position in the market in about 5 to 20 years [27]. Vision Domingez: The company Dominguez's vision is to be the first option for all customers when they are planning to get some groceries and strengthen the relationship through trust, transparency, and respect.

3) Process Map: It represents an organization that manages its processes; it can immediately identify its main characteristics, strategic processes, business processes, and support processes [28]. As shown in Fig. 2, the company's process map is shown, which has three fundamental processes. The strategic process (planning, customer service, marketing, and merchandise management), operational processes (purchase management, reception and product control, order management, sales management, delivery management), and finally, the support process (IT, HR, accounting and finance).

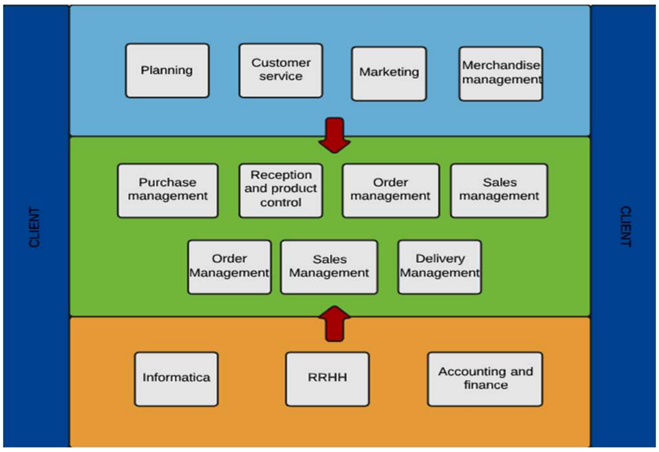


Fig. 2 Process Map of the Organization

B. Planning Stage

1) Schedule: Chronogram is a tool in charge of planning the schedule or time to carry out or complete a project's activities.

2) Information security policies Information security: It oversees obtaining information through the organization's objective. This allows the implementation of information security that would allow the evaluation [29] of risks, threats, and vulnerabilities to control any failure or inconvenience found in the company [30].

- Backup and recovery systems: To have a backup system and recovery procedure, you must have a storage protection medium for access control to the libraries.
- Risk Management: It is necessary to have a risk methodology that identifies, observes, and evaluates.
- Database creation: The IT area is in charge of the database's physical and logical design, using the company's information.
- Database installation: For any database, installation is required by technical support personnel who are trained in the IT area. Usually, it can be a staff of third-party companies to perform supervision and installation.
- Database security: The DOMINGUEZ database has a sophisticated mechanism that guarantees security, integrity, and confidentiality when storing any company information.
- Physical and environmental security: To obtain a physical access control to any installation, it is protected against any internal or external threat.
- Policies on the use of software licenses: The IT area supervise that all the computers work correctly.
- General access security policies: If an employee is dismissed, access must be deactivated and blocked with prior notification to the person. The person in charge of the area must notify the IT area to close or disable the access to that employee.
- Management of networks and computer systems: All networks connected to any computer in the company, mobile devices, and others. It must have supervision and protection against cybernetic attacks to protect the information of data of the company.
- Disaster recovery plans: A contingency plan should be in place in case of any type of natural disaster. All plans must be approved and verified by the company's manager.

C. Execution stage

1) Information Asset Inventory: Information asset inventories are identified, qualifying the assets according to their type. In the first part of the stage, the company's available assets were made, as shown in Table 1.

TABLE I
INVENTORY OF INFORMATION ASSETS

Active Type	Description
Data and Information	Database
Software	Applications, Operating Systems
Hardware	Servers, Desktop, Computers, Storage, Tape library, entre outros.
Communication networks	Routers, Switch, Videoconference communication
Information media	Backup tapes
Auxiliary Equipment	Air Conditioning, Generator, Alarms, Smoke Detectors, Fire Extinguishers, Temperature Meters, entre outros.
Facilities	Headquarters, offices, warehouses.
Staff	Internal staff, External staff, Suppliers, Customers

2) Valuation of the information asset: It is in charge of carrying out a valuation according to confidentiality, integrity, and impact. According to the three pillars of information, a 5-level valuation is performed for each pillar, as shown in Table 2.

- Confidentiality: The failure or loss of an asset leads to the unauthorized disclosure of information; producing an impact that affects the organization’s interests (prestige, economic, legal, competition, among others.).
- Integrity: The failure or loss of an asset originates the alteration of information (ceasing to be accurate and complete); producing an impact that affects the organization’s interests (prestige, economic, legal, and competition, among others.).
- Availability: The failure or loss of an asset causes the interruption of the access and availability of the information; producing an impact that affects the organization’s interests (prestige, economic, legal, competition, among others).

TABLE II
VALUATION OF THE INFORMATION ASSET.

Level	Criteria for the valuation of information assets		
	Confidentiality	Integrity	Availability
Very High (5)	Irreversible impact	Irreversible impact	Irreversible impact
High (4)	Severe impact	Severe impact	Severe impact
Medium (3)	Moderate impact	Moderate impact	Moderate impact
Low (2)	Partial impact	Partial impact	Partial impact
Very Low (1)	No impact	No impact	No impact

3) Probability of Occurrence: Identifies the levels that have a probability of occurrence. As shown in Table 3, the probability of occurrence has a value from 1 to 5 with corresponding frequencies.

TABLE III
PROBABILITY OF OCCURRENCE

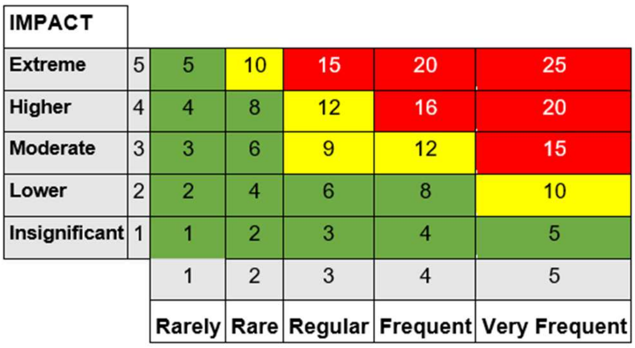
Value	Frequency
5	Very Frequent
4	Frequent
3	Regular
2	Rare
1	Rarely

4) Impact Level: The Impact Level is responsible for measuring and calculating the impact that risk could have when it begins to materialize, according to the information's confidentiality, availability, and integrity. In Table 4, the level of impact of the organization was identified through confidentiality, integrity, and availability. The impact value is the maximum value of the three dimensions.

TABLE IV
LEVEL OF IMPACT

Level of impact
Confidentiality
Integrity
Integrity
VALUE OF IMPACT

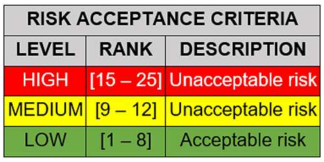
5) Risk Calculation: The risk calculation serves to identify the impact (extreme, major, moderate, moderate, minor, negligible) and the probabilities (rarely, rare, normal, frequent, very frequent) that the risk would give us. Fig. 3 identifies the impact level of the organization through confidentiality, integrity, and availability.



IMPACT						
Extreme	5	5	10	15	20	25
Higher	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Lower	2	2	4	6	8	10
Insignificant	1	1	2	3	4	5
		1	2	3	4	5
		Rarely	Rare	Regular	Frequent	Very Frequent

Fig. 3 Risk Calculation

In Fig. 4, we identify the risk acceptance criteria, which have three levels, high has red color where it has a range of 15 to 25, while the medium has had yellow color 9 to 12, which is an unacceptable risk, low which would be from 1 to 8 this risk is acceptable as they are minimal errors that can be solved.



RISK ACCEPTANCE CRITERIA		
LEVEL	RANK	DESCRIPTION
HIGH	[15 – 25]	Unacceptable risk
MEDIUM	[9 – 12]	Unacceptable risk
LOW	[1 – 8]	Acceptable risk

Fig. 4 Risk Acceptance Criteria

6) Risk Treatment: For the treatment of the risk is used the mitigation which is carried out by means of the use of the controls for the security, the transference, which is made concrete by means of the obtaining some cybernetic insurance and finally, the avoidance, which is carried out by means of the denial of the asset that could have been affected. In Table 5, the risk treatment is made, counting on four treatments (Avoid, mitigate, share, accept), allowing to an evaluation of the realized risks.

TABLE V
RISK TREATMENT

Treatment	Description
Avoid	This treatment is about not performing or continuing with a process or activity which aggravates the risk.
Mitigate	This treatment is about being able to initiate actions that help reduce the probability of impact or occurrence of a risk.
Share	It consists of splitting up the possible impact that the risk may have on an external agent or rather a third party, while at the same time having all the responsibility that the response may have.
Accept	In this treatment, all the consequences of the risk are simply assumed and accepted. For this treatment, none of the previous measures are carried out unless the risk materializes. This treatment is about being able to initiate actions that help reduce the probability of impact or occurrence of a risk.

7) Calculation of the Residual Risk: It allows to use of the respective controls. This allows the average of the risks can be calculated to take out the calculation of residual risk.

$$Residual\ Risk = Risk - Risk * Control\ Effectiveness \qquad (1)$$

D. Monitoring and Control Stage

Risk Assessment: Generally, risk assessment is known for identifying, prioritizing, and estimating all possible risks that may affect the entire organization. It is, above all, a critical activity for all risk management, and this is because all the specifications are given so that the risks that have been identified can be correctly managed [31].

E. Closing Stage

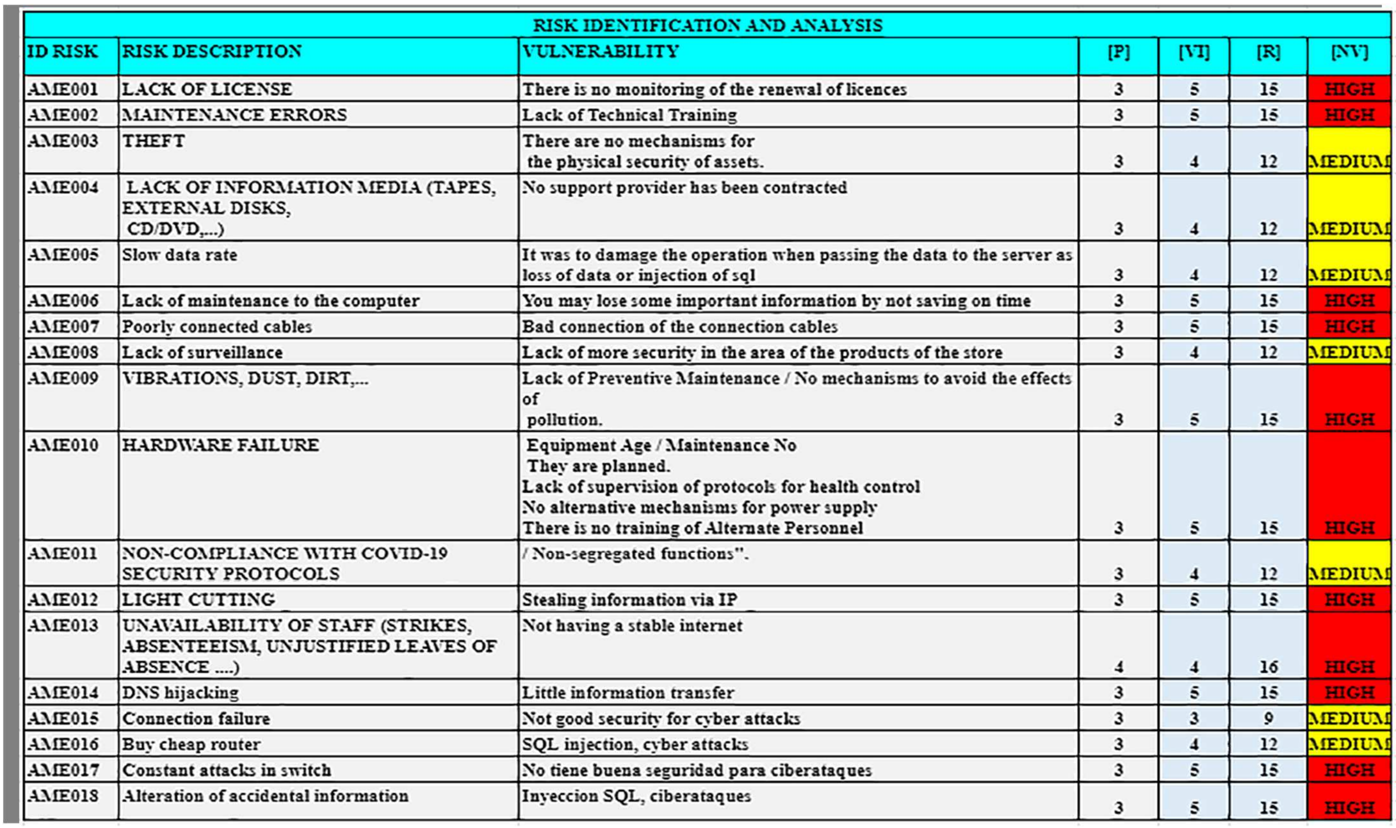
Closing Act: This process is a document describing all completed and signed deliverables. It is reviewed by the sponsors, thus accepting the stakeholders, leaving formal evidence of the conclusion and completion of the project. If the project has any canceled deliverables, this should be specified in the document regarding the situation, explaining why the deliverable was not completed.

III. Results and Discussion

These results and the discussion section show two final stages of our method. The first stage is Monitoring and Control, which deals with the risk assessment. The last stage is the Closing Act, in which a risk treatment plan, gap analysis, and final diagnosis are the results of the ISO 27001 compliance.

A. Monitoring and Control Stage

Risk Assessment: The risk assessment is explained in Fig. 5. According to the identification of the assets in Table I, the risks and vulnerability of each asset were observed. After estimating the Probability (P) and the Impact Value (VI), it is multiplied, resulting in the Risk (R). The Risk Levels (NV) are the risk acceptance criteria as explained in Fig. 3 and Fig. 4.



RISK IDENTIFICATION AND ANALYSIS						
ID RISK	RISK DESCRIPTION	VULNERABILITY	[P]	[VI]	[R]	[NV]
AME001	LACK OF LICENSE	There is no monitoring of the renewal of licences	3	5	15	HIGH
AME002	MAINTENANCE ERRORS	Lack of Technical Training	3	5	15	HIGH
AME003	THEFT	There are no mechanisms for the physical security of assets.	3	4	12	MEDIUM
AME004	LACK OF INFORMATION MEDIA (TAPES, EXTERNAL DISKS, CD/DVD,...)	No support provider has been contracted	3	4	12	MEDIUM
AME005	Slow data rate	It was to damage the operation when passing the data to the server as loss of data or injection of sql	3	4	12	MEDIUM
AME006	Lack of maintenance to the computer	You may lose some important information by not saving on time	3	5	15	HIGH
AME007	Poorly connected cables	Bad connection of the connection cables	3	5	15	HIGH
AME008	Lack of surveillance	Lack of more security in the area of the products of the store	3	4	12	MEDIUM
AME009	VIBRATIONS, DUST, DIRT,...	Lack of Preventive Maintenance / No mechanisms to avoid the effects of pollution.	3	5	15	HIGH
AME010	HARDWARE FAILURE	Equipment Age / Maintenance No They are planned. Lack of supervision of protocols for health control No alternative mechanisms for power supply There is no training of Alternate Personnel	3	5	15	HIGH
AME011	NON-COMPLIANCE WITH COVID-19 SECURITY PROTOCOLS	/ Non-segregated functions".	3	4	12	MEDIUM
AME012	LIGHT CUTTING	Stealing information via IP	3	5	15	HIGH
AME013	UNAVAILABILITY OF STAFF (STRIKES, ABSENTEEISM, UNJUSTIFIED LEAVES OF ABSENCE ....)	Not having a stable internet	4	4	16	HIGH
AME014	DNS hijacking	Little information transfer	3	5	15	HIGH
AME015	Connection failure	Not good security for cyber attacks	3	3	9	MEDIUM
AME016	Buy cheap router	SQL injection, cyber attacks	3	4	12	MEDIUM
AME017	Constant attacks in switch	No tiene buena seguridad para ciberataques	3	5	15	HIGH
AME018	Alteration of accidental information	Inyeccion SQL, ciberataques	3	5	15	HIGH

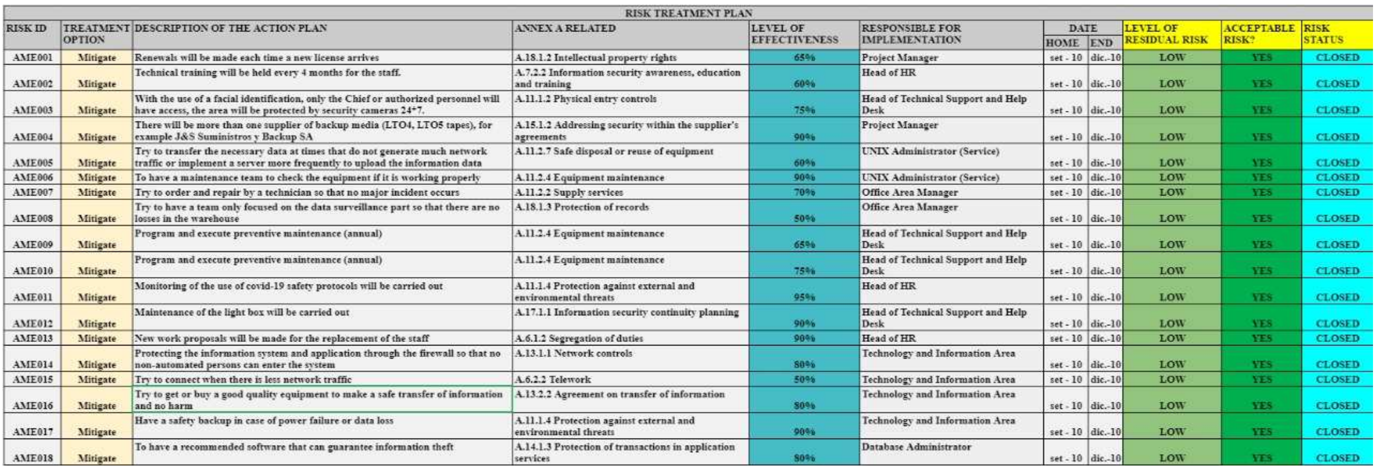
Fig. 5 Risk Assessment

B. Closing Stage

Closing act: In this last stage, we proceeded to make the closing act whereby the company's work team and owner conclude the project.

C. Risk Treatment Plan

Based on the risk assessment in Fig. 4, a plan was made that help address the risks that exist in the Domingez Company, as shown in Fig. 6.



RISK TREATMENT PLAN										
RISK ID	TREATMENT OPTION	DESCRIPTION OF THE ACTION PLAN	ANNEX A RELATED	LEVEL OF EFFECTIVENESS	RESPONSIBLE FOR IMPLEMENTATION	DATE		LEVEL OF RESIDUAL RISK	ACCEPTABLE RISK?	RISK STATUS
						HOME	END			
AME001	Mitigate	Renewals will be made each time a new license arrives	A.18.1.2 Intellectual property rights	65%	Project Manager	set - 10	dic.-10	LOW	YES	CLOSED
AME002	Mitigate	Technical training will be held every 4 months for the staff.	A.7.2.2 Information security awareness, education and training	60%	Head of HR	set - 10	dic.-10	LOW	YES	CLOSED
AME003	Mitigate	With the use of a facial identification, only the Chief or authorized personnel will have access, the area will be protected by security cameras 24*7.	A.11.1.2 Physical entry controls	75%	Head of Technical Support and Help Desk	set - 10	dic.-10	LOW	YES	CLOSED
AME004	Mitigate	There will be more than one supplier of backup media (LTO4, LTO5 tapes), for example J&S Suministros y Backup SA	A.15.1.2 Addressing security within the supplier's agreements	90%	Project Manager	set - 10	dic.-10	LOW	YES	CLOSED
AME005	Mitigate	Try to transfer the necessary data at times that do not generate much network traffic or implement a server more frequently to upload the information data	A.11.2.7 Safe disposal or reuse of equipment	60%	UNIX Administrator (Service)	set - 10	dic.-10	LOW	YES	CLOSED
AME006	Mitigate	To have a maintenance team to check the equipment if it is working properly	A.11.2.4 Equipment maintenance	90%	UNIX Administrator (Service)	set - 10	dic.-10	LOW	YES	CLOSED
AME007	Mitigate	Try to order and repair by a technician so that no major incident occurs	A.11.2.2 Supply services	70%	Office Area Manager	set - 10	dic.-10	LOW	YES	CLOSED
AME008	Mitigate	Try to have a team only focused on the data surveillance part so that there are no losses in the warehouse	A.18.1.3 Protection of records	50%	Office Area Manager	set - 10	dic.-10	LOW	YES	CLOSED
AME009	Mitigate	Program and execute preventive maintenance (annual)	A.11.2.4 Equipment maintenance	65%	Head of Technical Support and Help Desk	set - 10	dic.-10	LOW	YES	CLOSED
AME010	Mitigate	Program and execute preventive maintenance (annual)	A.11.2.4 Equipment maintenance	75%	Head of Technical Support and Help Desk	set - 10	dic.-10	LOW	YES	CLOSED
AME011	Mitigate	Monitoring of the use of covid-19 safety protocols will be carried out	A.11.1.4 Protection against external and environmental threats	95%	Head of HR	set - 10	dic.-10	LOW	YES	CLOSED
AME012	Mitigate	Maintenance of the light box will be carried out	A.17.1.1 Information security continuity planning	90%	Head of Technical Support and Help Desk	set - 10	dic.-10	LOW	YES	CLOSED
AME013	Mitigate	New work proposals will be made for the replacement of the staff	A.6.1.2 Segregation of duties	90%	Head of HR	set - 10	dic.-10	LOW	YES	CLOSED
AME014	Mitigate	Protecting the information system and application through the firewall so that no non-automated persons can enter the system	A.13.1.1 Network controls	80%	Technology and Information Area	set - 10	dic.-10	LOW	YES	CLOSED
AME015	Mitigate	Try to connect when there is less network traffic	A.6.2.2 Telework	50%	Technology and Information Area	set - 10	dic.-10	LOW	YES	CLOSED
AME016	Mitigate	Try to get or buy a good quality equipment to make a safe transfer of information and no harm	A.13.2.2 Agreement on transfer of information	80%	Technology and Information Area	set - 10	dic.-10	LOW	YES	CLOSED
AME017	Mitigate	Have a safety backup in case of power failure or data loss	A.11.1.4 Protection against external and environmental threats	90%	Technology and Information Area	set - 10	dic.-10	LOW	YES	CLOSED
AME018	Mitigate	To have a recommended software that can guarantee information theft	A.14.1.3 Protection of transactions in application services	80%	Database Administrator	set - 10	dic.-10	LOW	YES	CLOSED

Fig. 6 Risk Treatment Plan

D. Gap Analysis

Table 6 shows the estimation of ISO 27001:2014, identifying the beginning of the article clauses are observed in 40% and ending in 84%.

TABLE VI
GAP ANALYSIS

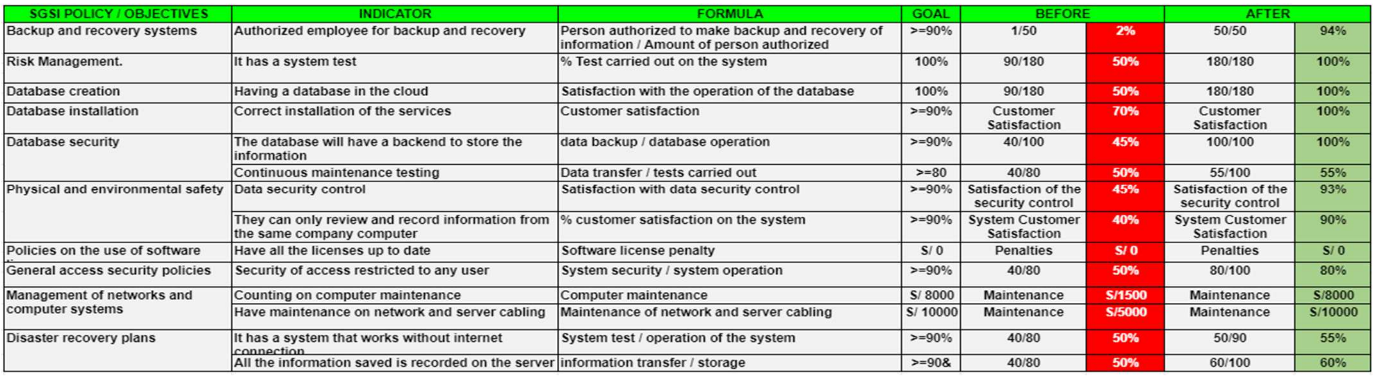
Clause	Start	Final
4. Context of the Organization	28%	69%
5. Leadership	50%	86%
6. Planning	69%	93%
7. Support	37%	93%
8. Operation	30%	83%
9. Performance evaluation	44%	75%
10. Improve	21%	89%
Compliance	**40%**	**84%**

E. Final diagnosis – controls

Table 7 shows the estimate of ISO 27001:2014, identifying the start of the article controls are observed at 48% and ending at 73%.

TABLE VII
FINAL DIAGNOSIS

Description of Controls	Start	Final
A.5 - IS Policies	50%	65%
A.6 - Organization of the IS	50%	65%
A.7 - Security linked to HR	50%	73%
A.8 - Asset management	45%	79%
A.9 - Access control	50%	79%
A.11 - Physical and environmental safety	45%	77%
A.12 - Security of operations	50%	79%
A.13 - Security of communications	45%	75%
A.14 - Acquisition, development, and maintenance of the system	40%	68%
A.15 - Relationship with the supplier	50%	75%
A.16 - IS Incident Management	50%	72%
A.17 - IS aspects in GCN	50%	71%
A.18 - Compliance	50%	75%
Compliance	**48%**	**73%**



SGSI POLICY / OBJECTIVES	INDICATOR	FORMULA	GOAL	BEFORE		AFTER	
Backup and recovery systems	Authorized employee for backup and recovery	Person authorized to make backup and recovery of information / Amount of person authorized	>=90%	1/50	2%	50/50	94%
Risk Management.	It has a system test	% Test carried out on the system	100%	90/180	50%	180/180	100%
Database creation	Having a database in the cloud	Satisfaction with the operation of the database	100%	90/180	50%	180/180	100%
Database installation	Correct installation of the services	Customer satisfaction	>=90%	Customer Satisfaction	70%	Customer Satisfaction	100%
Database security	The database will have a backend to store the information	data backup / database operation	>=90%	40/100	45%	100/100	100%
	Continuous maintenance testing	Data transfer / tests carried out	>=80	40/80	50%	55/100	55%
Physical and environmental safety	Data security control	Satisfaction with data security control	>=90%	Satisfaction of the security control	45%	Satisfaction of the security control	93%
	They can only review and record information from the same company computer	% customer satisfaction on the system	>=90%	System Customer Satisfaction	40%	System Customer Satisfaction	90%
Policies on the use of software	Have all the licenses up to date	Software license penalty	S/ 0	Penalties	S/ 0	Penalties	S/ 0
General access security policies	Security of access restricted to any user	System security / system operation	>=90%	40/80	50%	80/100	80%
Management of networks and computer systems	Counting on computer maintenance	Computer maintenance	S/ 8000	Maintenance	S/1500	Maintenance	S/8000
	Have maintenance on network and server cabling	Maintenance of network and server cabling	S/ 10000	Maintenance	S/5000	Maintenance	S/10000
Disaster recovery plans	It has a system that works without internet connection	System test / operation of the system	>=90%	40/80	50%	50/90	55%
	All the information saved is recorded on the server	information transfer / storage	>=90&	40/80	50%	60/100	60%

Fig. 7 Analysis of indicators

F. Analysis of indicators

In Fig. 7, we obtained the indicators analysis table, which indicates the information security policies and the company's objectives. This helped to identify the indicator, the formula, the goal, and it is before and after. There was a growth in some indicators, this served so that the company currently has to reach its goal and have a better performance in its policies.

IV. CONCLUSIONS

Analysis and design based on the ISO27001 of the Peruvian technical norms 2014 was made, making the corresponding comparisons, the conclusion was reached to have a great improvement which implies a great advance in the company. The objective has been successfully fulfilled since the goal was to implement an audit plan through the ISO 27001 standard while also identifying the information security problems found in the company Dominguez. Developing an information security strategy is disseminated and known by all employees, giving the organization a vision of how to perform daily activities and how these activities can help improve the management system. If risk management methods are applied correctly, important business information assets and risks and their impact can be identified, and appropriate control measures can be used to formulate work plans to mitigate and reduce risks. The risk level has reached an acceptable level. Future work suggests that an information security system be implemented through software where all controls can be entered through the software.

REFERENCES

[1] W. Boehmer, "Appraisal of the effectiveness and efficiency of an information security management system based on iso 27001," in 2008 Second International Conference on Emerging Security Information, Systems and Technologies, IEEE, 2008, pp. 224-231.

[2] R. Almeida, R. Lourinho, M. Mira da Silva, and R. Pereira, "A model for assessing cobit 5 and iso 27001 simultaneously," in 2018 IEEE 20th Conference on Business Informatics (CBI), vol. 01, 2018, pp. 60-69.

[3] T. Suryanto, "Audit delay and its implication for fraudulent financial reporting: A study of companies listed in the indonesian stock exchange," 2016.

[4] S. Nurizzati, "Effect of accounting information systemsfor credit sales and trade receivables on cash receipts,"JASa (Jurnal Akuntansi, Audit dan Sistem InformasiAkuntansi), vol. 4, no. 1, pp. 126–131, 2020.

[5] E. G. Vorobiev, S. A. Petrenko, I. V. Kovaleva, and I. K. Abrosimov, "Analysis of computer security incidents using fuzzy logic," in 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM), 2017, pp. 369-371.

[6] D. C. Villagran-Vizcarra, D. D. Ram'irezochoa, C. Barbamart'inez, and A. J. Barroso-Barajas, "Importancia de la capacitacion' del personal a traves de una cultura de seguridad ' informatica importance of staff training through a ' culture of computer security," lio-Septiembre-2018, p. 11, 2018.

[7] B. Hartadi, "Pengaruh fee audit, rotasi kap, dan reputasi auditor terhadap kualitas audit di bursa efek indonesia," *EKUITAS (Jurnal Ekonomi dan Keuangan)*, vol. 16, no. 1, pp. 84-104, 2018.

[8] W.-H. Tsai, H.-C. Chen, J.-C. Chang, J.-D. Leu, D. C. Chen, and Y. Purbokusumo, "Performance of the internal audit department under erp systems: Empirical evidence from taiwanese firms," Enterprise Information Systems, vol. 9, no. 7, pp. 725-742, 2015. DOI: 10 . 1080/17517575.2013.830341. eprint: https://doi.org/ 10.1080/17517575.2013.830341. [Online]. Available: https://doi.org/10.1080/17517575.2013.830341.

[9] Y. Chen, K. Ramamurthy, and K.-W. Wen, "Impacts of comprehensive information security programs on information security culture," Journal of Computer Information Systems, vol. 55, no. 3, pp. 11-19, 2015.

[10] W. A. Cram, J. G. Proudfoot, and J. D'arcy, "Organizational information security policies: A review and research framework," European Journal of Information Systems, vol. 26, no. 6, pp. 605-641, 2017.

[11] D. Achmadi, Y. Suryanto, and K. Ramli, "On developing information security management system (isms) framework for iso 27001-based data center," in 2018 International Workshop on Big Data and Information Security (IWBIS), IEEE, 2018, pp. 149-157.

[12] C. Schmitz and S. Pape, "Lisra: Lightweight security risk assessment for decision support in information security," Computers & Security, vol. 90, p. 101 656, 2020.

[13] P. Shamala, R. Ahmad, A. Zolait, and M. Sedek, "Integrating information quality dimensions into information security risk management (isrm)," Journal of Information Security and Applications, vol. 36, pp. 1-10, 2017.

[14] S. Bauer, E. W. Bernroider, and K. Chudzikowski, "Prevention is better than cure! designing information security awareness programs to overcome users' noncompliance with information security policies in banks," computers & security, vol. 68, pp. 145-159, 2017

[15] A. Brown, "Why are non-malicious employees noncompliant: Guidance for identifying employee negligence and implementing information security policies to reduce employees inadvertently becoming insider threats," PhD thesis, Utica College, 2020.

[16] S. Mishra, R. D. Raut, B. E. Narkhede, B. B. Gardas, and P. Priyadarshinee, "To investigate the critical risk criteria of business continuity management by using analytical hierarchy process," International Journal of Management Concepts and Philosophy, vol. 11, no. 1, pp. 94-115, 2018.

[17] I. M. Lopes, T. Guarda, and P. Oliveira, "Implementation of iso 27001 standards as gdpr compliance facilitator," Journal of Information Systems Engineering & Management, vol. 2, no. 4, pp. 1-8, 2019.

[18] C. Carvalho and E. Marques, "Adapting iso 27001 to a public institution," in 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), 2019, pp. 1-6. DOI: 10.23919/CISTI.2019.8760870.

[19] B. Barafort, A.-L. Mesquida, and A. Mas, "Integrating risk management in it settings from iso standards and management systems perspectives," Computer Standards & Interfaces, vol. 54, pp. 176-185, 2017.

[20] T. Aven, "Risk assessment and risk management: Review of recent advances on their foundation," European Journal of Operational Research, vol. 253, no. 1, pp. 1- 13, 2016.

[21] L. Almeida and A. Respıcio, "Decision support for selecting information security controls," Journal of Decision Systems, vol. 27, no. sup1, pp. 173-180, 2018.

[22] R. Kalaiprasath, R. Elankavi, D. R. Udayakumar, et al., "Cloud. security and compliance-a semantic approach in end to end security," International Journal Of Mechanical Engineering And Technology (Ijmet), vol. 8, no. 5, pp. 987-994, 2017.

[23] P. Rosenberger and J. Tick, "Suitability of pmbok 6th edition for agile-developed it projects," in 2018 IEEE 18th International Symposium on Computational Intelligence and Informatics (CINTI), 2018, pp. 000 241- 000 246. DOI: 10.1109/CINTI.2018.8928226.

[24] M. Huda and S. Azizah, "Implementation of pmbok 5th standard to improve the performance and competitiveness of contractor companies," International Journal of Civil Engineering and Technology, vol. 9, no. 6, pp. 1256-1266, 2018.

[25] J. J. Chamba Mera et al., "Development of a disaster recovery plan (drp) for the ti ' unit of the amco corporation," Master's thesis, Espol, 2017.

[26] A. A. Taiwo, F. A. Lawal, and P. E. Agwu, "Vision and mission in organization: Myth or heuristic device?" The International Journal of Business & Management, vol. 4, no. 3, 2016.

[27] S. A. Bowen, "Mission and vision," The international encyclopedia of strategic communication, pp. 1- 9, 2018.

[28] P. Navarro, P. Cronemyr, and M. Huge-Brodin, "Greening logistics by introducing process management-a viable tool for freight transport companies going green," in Supply Chain Forum: An International Journal, Taylor & Francis, vol. 19, 2018, pp. 204-218.

[29] W. A. Cram, J. G. Proudfoot, and J. D'arcy, "Organizational information security policies: A review and research framework," European Journal of Information Systems, vol. 26, no. 6, pp. 605-641, 2017.

[30] K. Hone and J. H. P. Eloff, "Information security ¨ policy-what do international information security standards say?" Computers & security, vol. 21, no. 5, pp. 402-409, 2002.

[31] J. R. C. Nurse, S. Creese, and D. De Roure, "Security risk assessment in internet of things systems," IT Professional, vol. 19, no. 5, pp. 20-26, 2017. DOI: 10.1109/ MITP.2017.3680959.