Journal of Contemporary Issues in Business and Government Vol. 27, No. 2,2021
https://cibg.org.au/

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.487

Systems Audit for the Tourism Sector

Nestor Cuba[1], Rosario Pariona[2,] Alex Pacheco[3], Elizabeth Mendoza[4], Consuelo Espino[5], Bertha Larico[6]
[1,3,6]Universidad Nacional de Cañete, [2] Universidad Nacional Autonoma de Huanta, [4]Universidad Peruana Union, [5]Universidad Nacional Federico Villareal
ncuba@undc.edu.pe, rpariona@unah.edu.pe, apacheco@undc.edu.pe, estherma@upeu.edu.pe, coeespino@gmail.com, blarico@undc.edu.pe

Abstract

It is essential to have a Systems Audit process to determine the conformity of the products, processes, plans, agreements and monitoring that may be generated in the Tourism Sector. The objective of the article is to describe a procedure to carry out computer audits, evaluate, determine the level of compliance with the processes and propose improvement actions. For this, we rely on observation sheets, survey format and checklist format of the Peruvian Technical Standard NTP ISO / IEC 27001: 2014, NTP ISO / IEC 12207: 2016 and ISO / IEC 27004: 2016. The results show that having a defined process saves management costs, identifies threats and reduces risks while safeguarding the integrity of the data. Highlighting the importance of improvement plans to prevent crime, increase the profitability of operations and scale the business strategy. Likewise, know the non-conformities of the processes so that through corrective and preventive actions they become compliant processes.

Keywords: Computer Audit, Tourism Sector, NTP-ISO / IEC 27001, NTP-ISO / IEC 12207: 2016, ISO / IEC 27004: 2016.

1. Introduction

The Tourism sector is an activity that has had considerable growth, becoming a key factor in socioeconomic progress worldwide. The vast majority of companies in the tourism sector do not have a well-defined process for computer audits, in the absence of these processes profitability and competitive advantage can be affected by having a high percentage of deficiencies in data management such as elements that stores, processes and distributes.

The success of the tourism sector has been related to its ability to manage risks. The importance of computer audits lies in their ability to determine the strengths and weaknesses of the company's information system (Arcentales-

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.487

Fernández & Caycedo-Casas, 2017). Some aspects must be taken into account: Cunning to identify key aspects to find inconsistencies in the processes being audited, Creativity for the fulfillment of its activities, Intelligence for proper decision-making, Honesty for the development of its activities, Confidentiality in the management of the information to which he has access (Proaño et al., 2017).

On the other hand, auditing is the exhaustive analysis of computer systems in order to detect, identify and describe different vulnerabilities that may arise. When performing the audit functions in an information system, auditors must comply with a series of regulations and ethical (Chicano, 2014). Companies must conduct internal and external audits at planned intervals to provide information on information security, define the criteria and scope of each audit, the results must be reported to the indicated personnel. (Peruvian Technical Standard, 2018).

With reference to computer audits, they must ensure: the acceptance review and the test requirements prescribed in the documentation are adequate for the acceptance of software products (Peruvian Technical Standard, 2018, test data meets specification; computer systems are successfully tested and meet their specifications (Mendoza et al., 2020); User documentation meets specific standards; Costs and schedule meet established plans

(International Organization for Standardization, 2016), The information security management system will help us to evaluate and identify those ineffective processes or regulations in our information security system, as well as the controls and priorities of the associated actions.

2. Materials and methods

2.1 Research techniques and instruments:

Techniques:

Observation, Surveys, Interview, Checklist, Evaluation, Inspection, Comparison, Document Review, Evaluation Matrix.

Instruments:

Observation Sheet, Survey Format, Checklist Formats.

2.2 Analysis of data

Logical content techniques or quantitative analysis, to draw conclusions. The results will be represented graphically to obtain accurate and visual information that will allow us to study them later.

2.3 Referential Review

The study of the Peruvian Technical Standard NTP-ISO / IEC 12207: 2016 Software and Systems Engineering, software life cycle process; NTP-ISO / IEC 27001; ISO / IEC 27004: 2016 Information technology - Security

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.487

techniques - Information security management - Monitoring, measurement, analysis and evaluation.

2.4 Proposed model:

The computerized audit in the tourism sector must comply with established standards, norms and policies of the company to achieve a good level of data security (Tamayo, 2015), development of systems with an established testing process (Mendoza et al., 2020) and with a control of the elements of the system before going to production (Mendoza et al., 2019). For internal and external audits, the auditors must sign a confidentiality statement on the company's information.

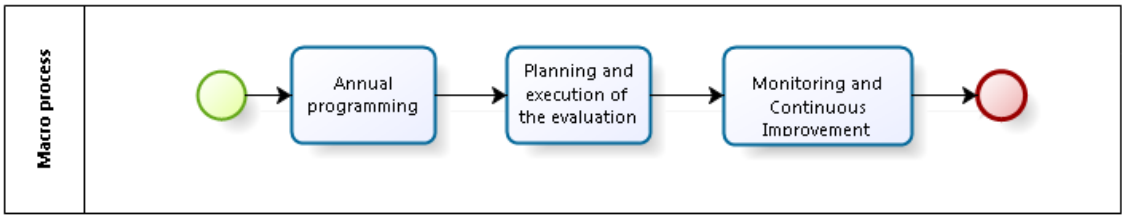

Figure 1. Proposal process (own source)

Figure 1, describes the proposal processes, which are detailed below:

Annual Computer Audit Schedule

The annual Computer Audit schedule must be planned, approved and disseminated to the competent areas. Likewise, the programming risks that may be affected by the objective must be taken into account. For internal audits, some of the risks are: planning, resources and selection of the evaluation team. For the External audit, one of the risks is the collaboration of the Computer Management. Once the annual program has been tested, its execution planning must be carried out. The annual program must take into account the following information: The Objective, scope, approval date, version, year, date of evaluation, date of approval, the plan must be signed by the general management.

Planning the Execution of the Annual Plan

For internal audits, the quality management must be in charge of appointing the evaluator team, informing the scope and criteria of the audit. The evaluation team must prepare the evaluation plan for the audit and must have the following information: the objective, scope, criteria and requirements for the audit, date, time and place of the areas to be evaluated. The quality management must approve said plan and communicate it to the areas involved.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.487

The evaluation team must have certain skills and abilities, for example leadership, manager, mediator, facilitator, experience in computer auditing.
In the case of the external audit, the certifying company has its execution process, in which it must respect the company's policies.
In both cases, meetings must be held: opening, intermediate (if necessary) and closing.

Execution of the Evaluation

For the execution of the evaluation of the internal or external audits, the following should be considered:

- In the opening meeting, the objective and the scope of the evaluation in which it will be reflected in an opening / closing minutes must be clearly explained. The start / closing time and list of attendees must be included with their title and signature.
- In the review and collection of evidence, the team of evaluators must prepare a checklist which must include the following information: name of the auditor, date, name / role of the evaluated, standards / clauses, team comment evaluator and the finding found.
- Identification and appreciation of the findings, the findings are communicated verbally during the evaluation to the IT Manager so that he can have a better understanding at the closing meeting.
- Closing meeting, all the findings found in the evaluation must be known by means of a closing act, at this meeting there should be a representative of the General Directorate, Quality Management, Evaluation Team and the Computer Management as appropriate.

Evaluation Report

The audit report is a document containing all the findings of the evaluation of the evaluation team, in which the report will be forwarded to the General Directorate, Quality Directorate and the IT Management within a specified period.

Monitoring and Continuous Improvement

The Computing Management is responsible for managing the findings, identifying the cause and effect for the survey and implementing opportunities for improvement.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.487

Figure 2, details the activities of the proposed model.

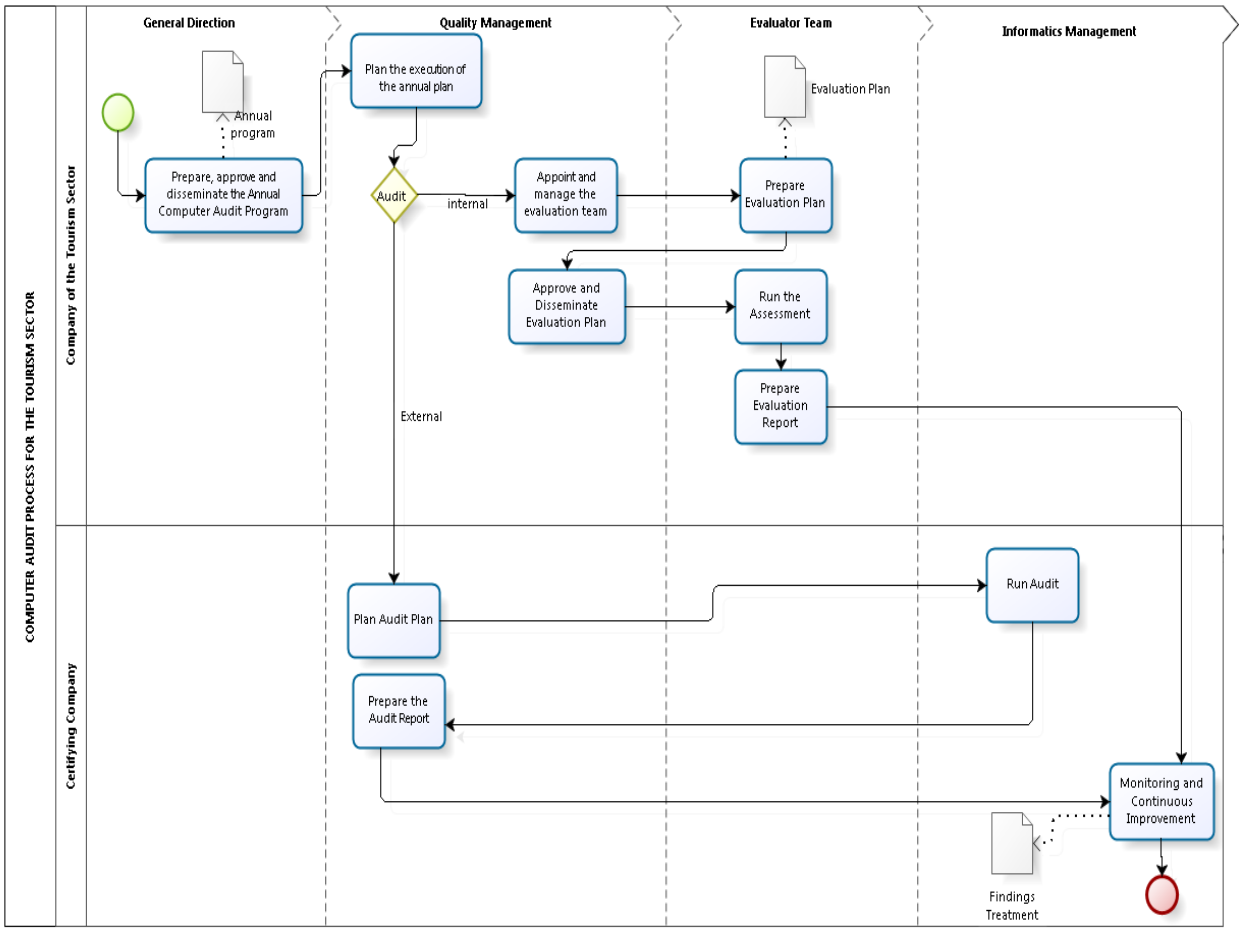

Figure 2: Activities of the Proposed Computer Audit Model (Own elaboration)

3. Results

For the systems audit in the tourism sector, techniques and instruments were applied where technological advances that are relevant and efficient applied to this sector were identified.

3.1 Survey: One of the techniques that was applied were surveys of sixty (60) workers in the tourism sector:

Application Security

Table 1: Installed Programs

Question 01: Are the programs installed on your station necessary for your work?		
Response	Frequency	Percentage
Yes	18	30%
No	42	70%

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.487

Total	60	100%

Source: own elaboration

Table 1, shows that 30% of workers in the tourism sector indicate that they DO agree with the programs installed at their workstation, while 70% indicate that they do not agree why they need other accesses and also report that the installed programs do not work correctly.

Table 2: Database Security

Question 02: Is the database of the tourism company secure?		
Response	Frequency	Percentage
Always	5	8.3%
Sometimes	45	75%
Hardly ever	10	16.7%
Never	0	0%
Total	60	100%

Source: own elaboration

In Table 2, it is shown that 8.3% of workers in the tourism sector indicate that the database is always safe, 75% of those mention that the database is sometimes secure, 16.7% declare that almost the database is never secure, because there were many falls as a consequence, they did not have the availability of the service, 0% state that the database is never secure.

Table 3: Monitoring and control of programs

Question 03: Are the installed programs monitored and controlled?		
Response	Frequency	Percentage
Yes	5	8.3%
No	55	91.7%
Total	60	100%

Source: own elaboration

Table 3 shows that 8.3% of workers in the tourism sector indicate that the installed programs are monitored and controlled, while 91.7% indicate that the installed programs are NOT monitored and controlled.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.487

Table 4: Antivirus updates

Question 04: Do the workstations have updated antivirus?		
Response	Frequency	Percentage
Always	0	0%
Sometimes	45	75%
Hardly ever	15	25%
Never	0	0%
Total	60	100%

Source: own elaboration

In table 4, it is shown that 0% of workers in the tourism sector indicate that their workstations have updated antivirus, 75% of them mention that sometimes their antivirus is updated on their workstation, 25 % declare that they hardly ever update the antivirus, 0% state that they never update the antivirus on their workstation.

Logical Security

Table 5: Access credentials

Question 05: Do users have credentials to access workstations?		
Response	Frequency	Percentage
Yes	15	25%
No	45	75%
Total	60	100%

Source: own elaboration

Table 5, shows that 25% of workers in the tourism sector DO have access credentials to their work station while 75% indicate that they DO NOT have access credentials to their work station.

3.2 Process execution

02 computer audits were carried out, we can see the following results:

Table 6: Execution of the audit process

Systems Audit in the Tourism Sector				
Period	No. Non-conformity Major	Major non-conformity	Observations	Observations
First semester	0	3	15	4

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.487

Second semester	0	0	5	2

Source: own elaboration

By having a defined process of auditing systems in the tourism sector, we can save management costs, identify any threat, reduce risks, and information would be accessible, safeguarded, and data integrity would be safe.

4. Discussion

This research proposes a Systems Audit process, this is an evaluation to verify if they comply with its procedures, standards that organizations establish, as it agrees (Blanco, 1982), the systems audit is a set of working methods and techniques, linked to the problem of adequately conserving the information resources of the entities and guaranteeing the authenticity, correctness and integrity of their information. According to (Alfonso et al., 2012), with the intervention of computer auditing, it can achieve the efficiency of other systems.

The Systems Audit for the Tourism Sector can improve its services. Instruments and techniques were applied to obtain a diagnosis of the current situation, thanks to the results obtained, a systems audit process was defined. The Tourism Sector should promote a computer culture in the follow-up of controls as agreed (Salgado et al., 2017), by not carrying out this culture in the company it would lead to not safeguarding the assets, not maintaining the integrity of the data. Having a systems audit could identify threats and reduce risks, achieve data integrity and information efficiency, as well as comply with standards, norms to increase competitiveness.

5. Conclusions

It is important to implement improvement plans as a result of the computer audit, which allow the company to have security in computer processes, prevent crimes, increase the profitability of operations and scale the business strategy. All this hand in hand with a computer security policy that saves the information, which is a very important asset of the entire organization, ensuring the sustainability of the business. In this way, the unauthorized use of the information that would lead to a bad institutional image is avoided.

Likewise, the audit made it possible to know the non-conformities of the processes, giving the organizations the opportunity to take advantage of the information received, taking corrective and preventive actions so that the processes were classified as compliant, achieving continuous improvement of the processes.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.487

References

Alfonso, Y., Blanco, B., & Loy, L. (2012). Information Systems Audit of Financial Statements. Revista de Arquitectura e Ingeniería, 6(2), 1–14. https://www.redalyc.org/pdf/1939/193924743004.pdf

Arcentales-Fernández, D., & Caycedo-Casas, X. (2017). Auditoría informática: un enfoque efectivo. Dominio de Las Ciencias, 157–173. https://dx.doi.org/10.23857/dom.cien.pocaip.2017.3.mono1.ago.157-173

Blanco, L. (1982). La auditoria de los sistemas automatizados : una introduccion a su estudio. Economia y Desarrollo, 67(Mar-Abr), 20–45. https://biblat.unam.mx/es/revista/economia-y-desarrollo/articulo/la-auditoria-de-los-sistemas-automatizados-una-introduccion-a-su-estudio

Chicano, E. (2014). Auditoria de seguridad informática. IC Editorial.

International Organization for Standardization. (2016). Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and Evaluation. (ISO/IEC 27004: 2016). https://www.iso.org/standard/64120.html

Mendoza, E., Espino, C., Rodriguez, C., & Pacheco, A. (2020). Software Testing of Information Systems in Peruvian Public Organizations. TEST Engineering & Management, 83(March-April), 13428–13433. https://testmagzine.biz/index.php/testmagzine/article/view/6045/4778

Mendoza, E., Rodriguez, C., & Esenarro, D. (2019). Configuration Management of Information Systems in Peruvian Goverment Organizations. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(12S2), 31–36. https://doi.org/10.35940/ijitee.L1007.10812S219

Peruvian Technical Standard. (2018). Information Technology. Security techniques Information security management systems. Requirements 2nd. Edition. (NTP ISO/IEC 27001:2014). https://cdn.www.gob.pe/uploads/document/file/357224/Resoluci%C3%B3n_Ministerial_N__004-2016-PCM20190902-25578-19siyuu.pdf

Peruvian Technical Standard. (2016). Systems and Software Engineering, Software life cycle processes 3rd, Edition. (NTP ISO/IEC 12207:2016).

https://cdn.www.gob.pe/uploads/document/file/313911/Resoluci%C3%B3n_de_Secretar%C3%ADa_General_N__020-2019-PRODUCESG20190515-27906-1x5ijoj.pdf

Proaño Escalante, R. A., Saguay Chafla, C. N., Jácome Canchig, S. B., & Sandoval Zambrano, F. (2017). Knowledge based systems as an aid in information systems audit. Enfoque UTE, 8(1), pp. 148-159. https://doi.org/10.29019/enfoqueute.v8n1.122

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.02.487

Tamayo, D. (2015). Modelo de Auditoría Informática orientada a procesos de seguridad en redes computacionales. [Tesis de Pregrado, Universidad Andina Néstor Cáceres Velásquez]. http://repositorio.uancv.edu.pe/handle/UANCV/475

Salgado, M. del C., Osuna, N., Caro, M., & Morales, J. (2017). La Auditoría Informática en las organizaciones. Revista Electrónica Sobre Cuerpos Académicos y Grupos de Investigación, 4(8), 1–14. https://www.cagi.org.mx/index.php/CAGI/article/view/165