Maturity Model for Information Access Management of Peruvian IT Service Providers based on ISO/IEC 27001 and CMMI Security Controls

Sergio Huamán, Luis Ponce, Lenis Wong
Universidad Peruana de Ciencias Aplicadas
Lima, Perú
u201816393, u201916220, pcsilewo @upc.edu.pe

***Abstract*—In the current context of increasing cyber threats to Latin American IT service providers, the cost of data breaches is expected to increase 31% by 2023, which highlights the urgency of strengthening security practices. Therefore, it is proposed to improve maturity in access management, with the development of a model based on ISO/IEC 27001:2022 designed for Peruvian IT service providers. The study consists of three stages: analysis, design, and validation. In the first stage, a comparative analysis is made between success factors, cybersecurity aspects, maturity models and access management mechanisms. The second and third stages cover the model building phases according to De Bruin's methodology. In the second stage, the evaluation scope, and the level structure according to CMMI are defined as well as the criteria of the model where the evaluation is based on a user life cycle, type of access and regulatory compliance. Finally, in the third stage, the model is validated by experts in the field and deployed in an enterprise in the sector. The results obtained from the validation showed that "understandability", "usefulness and practicality", "accuracy", "comprehensiveness", "sufficiency", "relevance", "usability" and "accuracy" obtained an average rating of 4.6 (agree). Finally, with respect to the implementation of the proposed model, the elimination phase had a maturity index of 0.14, which placed it at an initial maturity level. On the other hand, the other phases exceeded an index of 0.55, placing them in the three highest levels of maturity achievable. In this way, an improvement proposal for the enterprise was made and accepted.**

I. INTRODUCTION

As IT evolves and the value of information increases, so do the threats, vulnerabilities and risks that beset organizations. Attackers that constitute a form of threat seek to exploit vulnerabilities with diverse objectives, which can range from affecting technological infrastructure to accessing organizational information or data for various malicious purposes. During 2023 the cost of data breaches in Latin America has increased 31% over the previous year, representing a warning of great negative impact for all companies. Such incidents occur when attackers use various methods to exploit vulnerabilities and gain access to confidential information. Among the most common external attack vectors are those that generate unauthorized access, such as phishing (16%) and credential theft (15%). In contrast, the least frequent attack vectors were those of internal origin (6%); however, these generated the most significant losses for the companies [1]. Although there are several standardized sources of good security and cybersecurity practices, there is significant difficulty in interpreting them due to their very general and non-prescriptive nature that seeks to cover a wide range of business contexts [2]. Similarly, maturity models, being ideal tools for measuring process performance, have been criticized for their lack of clarity and consistency in defining maturity levels and assessment criteria, which limits their usefulness and effectiveness [3]. Also, the organizational uniqueness and technological complexity of each enterprise can make it difficult to implement authorized access controls because the adoption of these controls requires changes in the operation and new learning for employees, which can generate resistance to change [4].

This is how several studies through different proposals try to improve the mitigation of existing gaps in security controls, such as proposing maturity models for each context of the organization and thus be able to detect weaknesses and establish future improvements [3]. Also, the identification of success factors in the organization that allow the good performance of security controls and the establishment of strategies based on them [5]. However, these studies expand on the generality of all the controls that make up an organization's information security (IS) and cybersecurity, which limits the improvement of each control and management process.

For this reason, this study proposes a maturity model for information access management in Peruvian IT service providers based on ISO/IEC 27001 security controls [6]. The model will consist of phases such as: Scope (i), Design (ii), Populate (iii), Test (iv), Deploy (v) and Maintain (vi).

II. RELATED WORK

For the analysis of the related works, we performed a systematic review of the literature based on the following steps [7]: planning, development, and analysis.

In the "planning" phase, research categories were defined based on the following questions: What organizational factors are determinant for the success of controls focused on information security? (Q1) What cybersecurity aspects impact the performance of controls focused on information security? (Q2) What maturity models currently exist for the evaluation of information security oriented to access management and what deficiencies do they present? (Q3) What mechanisms exist for access management in an organization? (Q4). In the "development" phase, keywords such as "maturity model", "security information", "access management", "access control" were defined. Also, the scientific database engines consulted were Scopus, Web of Science and IEEE considering articles after 2019. In the "analysis" phase, a taxonomy was elaborated

where the literature obtained was classified according to its contribution to the questions posed in the first phase (see Table ITABLE I).

TABLE I. TAXONOMY OF ARTICLE DISTRIBUTION BY CATEGORY

Taxonomy	References
Organizational success factors (Q1)	[8] [9] [10] [5] [11] [12] [13] [14] [15] [16] [17] [18]
Cybersecurity aspects (Q2)	[11] [13] [12] [14] [16] [18]
Maturity Models (Q3)	[2] [3] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28]
Access Management Mechanisms (Q4)	[29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39]

A. Organizational success factors

We identified five organizational success factors that influence information security: human resources, technological complexity, organizational complexity, risk management and vulnerability management. In [5], [10] they argue that the "human resource" is the main factor responsible for executing security controls from start to finish and its performance can be optimized through training and awareness-raising, strengthening the most vulnerable link in the organization. Regarding the "technological complexity" factor, in [12] mentions the variability of technological infrastructures among organizations and emphasizes the need to implement technical controls, previously analyzed by a specialized area under a risk perspective, and to have technically specialized personnel. Regarding the "organizational complexity" factor, several authors argue that it is important to consider some characteristics of an organization, such as organizational size [13] and industry [10], for the design of controls, since there is no possibility of changing them from the security position [5]. With respect to the "Risk Management" factor, several authors argue that it is a process present in many organizations where different methodologies are used to address risk through prevention, tolerance and exposure by means of the ISO/IEC 27001 and NIST CSF standards [40]. According to the factor "Vulnerability Management", in [18] organizations usually deal with vulnerabilities by associating them with technical aspects. Such management can only be highly efficient if the organization is aware of all its assets and infrastructure.

B. Cybersecurity aspects

On the other hand, four aspects of cybersecurity have been identified that are highly related to the performance of information security controls: technological controls, cybercrime legislation, organizational and specialized equipment. Referring to "technological controls" in [11], [18] technical security measures in emerging technologies such as IoT were analyzed for risk mitigation. Regarding "cybercrime legislations" in [12], [18] addressed the need for a local regulatory body to promote a cybersecurity capacity assessment guide in organizations. For the "organizational" aspect, in [14] it is argued that cybersecurity measures should include the participation of all areas of an organization and ensure coordination in the event of incidents. Also, regarding "specialized teams", in [13], [16] argues that organizations must have specialized areas for the execution of security and cybersecurity controls, as well as be continuously trained and capable of responding to incidents and emergencies.

C. Maturity models

We have identified the use of three maturity models published by international institutions and associations for the evaluation of the performance of information security controls in different small and medium-sized organizations: C2M2, COBIT and CMMI. Regarding "C2M2" studies such as [2] analyze the application of the cybersecurity capability maturity model to evaluate security technology controls where it was highlighted for its use with other cybersecurity frameworks. Similarly, regarding "COBIT", research by [25] analyzed the application of the maturity model proposed by the framework, based on its information technology (IT)-related governance essence, and its usefulness in highlighting areas for improvement in critical processes was appreciated. In addition, regarding "CMMI", in [26], [27], [28] analyzed the use of the model for process improvement and recognized the flexibility in its application, adapting better to the different requirements and contexts of each organization.

D. Access Management Mechanisms

We identified three mechanisms used by companies to define their access management process for the systems that are part of their organization: access control model, access and identity management, and privileged user management. With regard to "Access Control Models" in organizations, according to their organizational aspects, models such as Role-Based Access Control (RBAC) [29], [31], [34], Mandatory Access Control (MAC) [30] and Discretionary Access Control (DAC) [29]. Complementing the use of the different models of access control management, organizations employ cybersecurity capabilities such as the practice of "Access and Identity Management" in that [36], [37], [38] study the controls and mechanisms for the correct use of applications and data. Likewise, in [39] he controls and risks present in the "Privileged User Management" were analyzed, where the criticality of handling superusers and privilege management in the systems of the organizations is highlighted.

III. PROPOSED MODEL

This section presents the maturity model oriented to the access management of Peruvian IT service provider companies based on ISO/IEC 27001:2022 and CMMI.

According to [41], for the development of a maturity model, it is important to consider the maturity levels of the model. For this purpose, there are two variations: the fixed-level model and the focus area model. The former is a model with linear stages that results in a maturity level according to the average of the assessment. The second is built by capabilities and can include any number of levels. Since the present study aims to develop a maturity model to serve as a basis for the assessment of access management in organizations, a fixed-level model is chosen.

For this purpose, the De Bruin methodology [42] will be applied, which consists of 6 phases: (i) Scope, (ii) Design, (iii) Populate, (iv) Test, (v) Deploy and (vi) Maintain. Phase I delimits the process in which the maturity level assessment will be carried out. The security frameworks are defined, as well as the structure of the maturity model on which the proposal will be based in phase II. In phase III, the evaluation criteria for each

maturity level are defined. The model will be validated under expert judgment in phase IV. In phase V, the model will be deployed in a proposed case study. Finally, in phase VI, the results obtained will be evaluated by validating it in accordance with the case study (see Fig. 1).

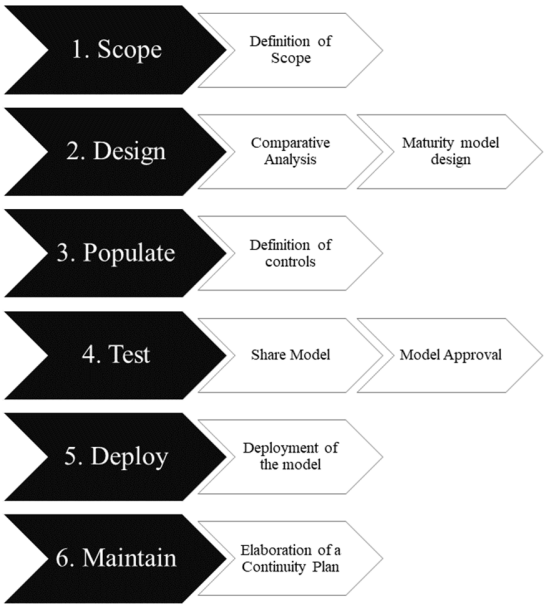


Fig. 1 Phases of the De Bruin methodology [42]

A. Phase I: scope

The proposed maturity model will be focused on Peruvian IT services companies, whose main scope is to evaluate their information access management process using different security frameworks.

As a result of the literature review conducted in section II of this study, three information security frameworks were selected. As the first framework, ISO/IEC 27001:2022 was selected because of its certifiable international status and its ability to establish information security controls. Likewise, NIST CSF will be used as it has a risk and incident assessment clearly focused on cybersecurity, in addition to the fact that the use of the framework is customizable for each enterprise. Finally, COBIT [43] will be used because it focuses on Information Technology (IT) governance and control.

B. Phase II: design

For the design of the maturity model, the levels are defined according to CMMI [44], highlighting its structure designed by stages and flexibility for the evaluation of access management; Table II shows the five maturity levels with their description, in which each level represents a key milestone in the development of access management, providing a clear framework of compliance identified in the current state of the enterprise.

C. Phase III: populate

This phase establishes the criteria to be measured to determine the organization's access management maturity level. The criteria will be defined based on the relationship between the following components: (i) ISO/IEC 27001:2022 requirements regarding access control, (ii) access lifecycle and (iii) types of access.

1) ISO/IEC 27001:2022 requirements: As a first component, an analysis and interpretation of Annex A of the standard was carried out and the following requirements related to access control were selected (see Table III).

2) Lyfe cycle of an access: In this section an access lifecycle will be established based on the study of [35] and the Oracle Cloud Infrastructure documentation [45], in Table IV the Lifecycle for Managing Users (LMU) phases are shown.

3) Types of access: It is important to define and segregate the evaluation for the different recurring accesses in an organization because they contain different criteria. In the present section the types of access are determined based on the concepts provided by the COBIT framework and ISO/IEC 27001:2022 resulting in the following (see Table V).

TABLE II. CMMI MATURITY LEVELS [44]

Level	Description
Initial (L1)	The organization's processes are AD HOC, so it may have access management processes that are poorly structured or non-existent. Likewise, they do not follow a clear methodology on the life cycle of an access, which can lead to a risk of greater vulnerability in information security
Managed (L2)	The organization is aware of the aspects of information access management and establishes systematic processes
Defined (L3)	The organization has clearly defined and documented its processes related to access management
Quantitatively Managed (L4)	The organization manages the potential risks of the process related to access management and evaluates according to the impact on privacy. In addition, they establish monitoring that is used to detect suspicious behavior in access management
Optimizing (L5)	The enterprise has a high level of maturity in access management and information security and is constantly looking for ways to strengthen security controls. Regular tests are conducted to evaluate the effective protection of security controls

TABLE III. ISO/IEC 27001:2022 REQUIREMENTS [6]

Domain	Control
Organizational controls	Policies for information security (5.1)
	Information security roles and responsibilities (5.2)
	Segregation of duties (5.3)
	Access control (5.15)
	Identity management (5.16)
	Authentication information (5.17)
	Access rights (5.18)
People Controls	Confidentiality or non-disclosure agreements (6.6)
	Remote working (6.7)
Physical controls	Physical entry (7.2)
	Physical security monitoring (7.4)
	Security of assets off-premises (7.9)
	Storage media (7.10)
Technological controls	User end point devices (8.1)
	Privileged access rights (8.2)
	Information access restriction (8.3)
	Access to source code (8.4)
	Secure authentication (8.5)
	Data leakage prevention (8.12)
	Segregation of networks (8.22)
	Separation of development, test and production environments (8.31)

TABLE IV. PHASES OF LIFECYCLE FOR MANAGING USERS [35] [45]

Phase	Description
Create (P1)	In this phase, user records are created and collected. User identification and authentication data are also stored in a centralized system [35] [45]
Activate (P2)	In this phase, access rights are assigned to registered users. Specific permissions are configured so that users can access the resources required for their roles or tasks [35] [45]
Assign (P3)	In this phase, security policies and controls are implemented to ensure that users access only those resources and data to which they are authorized. This involves the implementation of security and authentication measures [35] [45]
Review (P4)	In this phase, continuous monitoring of user access is performed. Access activities are monitored and audited to detect strange behavior or possible security threats [35]
Modify/ Deactivate (P5)	This phase establishes the activities to be carried out when a user is no longer authorized, or their roles change. Access permissions are revoked, either delete or adjust existing ones as necessary [35]
Delete (P6)	In this phase, the user is removed from the system, however, a detailed log of all access activities is maintained, including who accessed which resources and when [35] [45]

TABLE V. TYPES OF ACCESS [6] [43]

Access	Description
Physical	Ability of a user to enter the organization's physical facilities, such as offices, data centers, warehouses, others
Logical	The ability of a user or system to access digital resources, such as computer systems, networks, applications, and databases
Privileged	A user's capacity to access digital resources by means of certain special privileges that go beyond normal access parameters

TABLE VI. CRITERIA OF MATURITY LEVELS FOR THE PHASE "CREATE" (P1) OF LMU

L1	L2	L3	L4	L5
Type: Physical				
Responsible not assigned. No registry	Responsible defined for registering	Documented policy and procedure for managing	Technological controls to register access	Advanced technologies Biometric identification systems, facial recognition, and behavioral analysis
Type: Logical				
Responsible for user creation not defined. No nomenclature	Responsible and approver for user creation. Generic nomenclature	Documented policy and procedure for the creation of users. Centralized in a specialized area. Nomenclature for each type of user	Data accuracy is measured. Compliance with established policies and procedures is evaluated.	Metrics are periodically analyzed to identify opportunities for improvement
Type: Privileged				
Not inventoried superusers	Inventoried superusers	Documented policy and procedure for: "acceptable use of superuser accounts" and "creation of privileged users"	Risk assessment. Personnel authorized to use superuser accounts. Generation of privileged users	Regularly analyze metrics data to identify opportunities for improvement in the superuser usage process

With the components established and detailed, we proceeded to draw up the list of ISO/IEC 27001:2022 compliance criteria according to the six phases of the LMU: P1 (Table VI), P2, P3, P4, P5 and P6 (Table IX). For example, Table VI shows the defined criteria of the "Create" (P1) phase and classified by five levels (L1, L2, L3, L4 and L5), by the three types of access: physical, logical, and privileged.

D. Phase IV: test

The study is validated in a Peruvian IT service provider enterprise through the participation of a group of experts who occupy different positions in the Information Security Management System (ISMS), in order to obtain an integral validation of access management, approaching the evaluation from different perspectives of the process. The group of experts, belonging to the enterprise, is made up of a Security Officer, an information security analyst, and IT security analyst.

For the validation process with the experts, the design developed in the "Design" phase is presented and shared with them in order to obtain their appreciation of the proposal by means of a questionnaire based on the survey structure proposed in Salah's study [46]. In Table VII shows the questionnaire made up of 14 questions classified by category to be validated. The closed questions will be evaluated on a Likert scale (1 = Strongly Disagree, 2 = Disagree, 3 = Neither Disagree Nor Agree, 4 = Agree and 5 = Strongly Agree).

TABLE VII. QUESTIONNAIRE FOR EXPERTS

Category		Question	Type
Sufficiency	Q1	Does the model allow you to evaluate all aspects of the processes that make up access management?	Close-ended
Accuracy	Q2	Are there no overlaps/redundancies between maturity level criteria and descriptions?	Close-ended
	Q5	Are processes and practices clearly differentiated?	Close-ended
	Q6	Are processes and practices correctly assigned to their respective maturity level?	Close-ended
Relevance	Q3	Are the processes and practices relevant to access management?	Close-ended
Comprehensiveness	Q4	Do the processes and practices cover all aspects affecting or involved in access management?	Close-ended
Understandability	Q7	Are the maturity levels understandable?	Close-ended
	Q8	Are the evaluation guidelines understandable?	Close-ended
	Q9	Is the documentation understandable?	Close-ended
Usability	Q10	Is the scoring system easy to use?	Close-ended
	Q11	Are the evaluation guidelines easy to use?	Close-ended
	Q12	Is the documentation easy to use?	Close-ended
Usefulness and practicality	Q13	Is the maturity model useful for conducting assessments for the access management process?	Close-ended
	Q14	Is the maturity model practical for use in the IT services industry?	Close-ended

In Fig. 2, the results obtained from the validation questionnaire completed by the three case study experts are shown. According to this definition, the results are broken down into several categories: "sufficiency" with an average score of 4.3, "accuracy" with an average of 4.5, "completeness" with an average of 4.6, "comprehensibility" of 4.4, "usability" with an average of 5, and "usefulness and practicality" with a total of 4.8. These scores indicate that the experts are satisfied with the maturity model, which validates its usefulness in real environments.

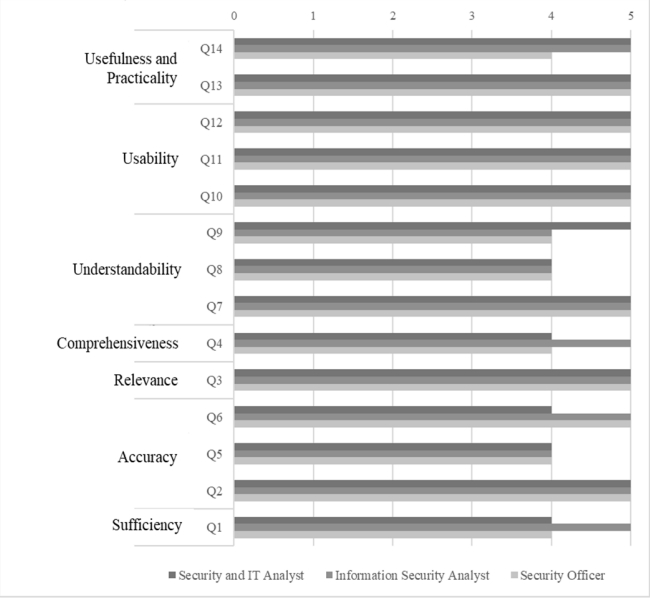


Fig. 2. Expert Satisfaction Level per question

E. Phase V: deploy

The validated model was implemented in the enterprise, having as scope the access management process under the applications and physical facilities defined in its scope of the Information Security Management System (ISMS).

With the purpose of carrying out the implementation, a diagnostic tool was built that includes all the defined and validated criteria of the "Design" phase.

The diagnostic tool developed will be used for two purposes. The first purpose of use will be to obtain the degree of compliance with ISO/IEC 27001:2022 according to its controls related to access management. Also, the second purpose of use will be to calculate: the overall maturity level of the access management process, the maturity by LMU phase and the maturity by access type. The two purposes of use will be presented by the tool through a graphical report for a better visualization of results for the user.

For the implementation of the maturity model in the enterprise, the diagnostic tool was used in collaboration with the parties involved in the access management of the enterprise, where all the LMU phases were evaluated with their respective criteria. The diagnostic tool calculates maturity using a scale of scores according to the status of compliance with each criterion (0 = Not met, 1 = Partially met and 2 = Compliant). It should be emphasized that the compliance status is recorded in the 'Status' column of the diagnostic tool in coordination with the members of the enterprise's ISMS. As an example, Table VIII shows how to fill in the compliance status of the P6 evaluation criteria.

TABLE VIII. EVALUATION OF THE PHASE P6 OF LMU

Type	Criteria	Domain	Status
Logical	There is an operational responsible for the elimination of access rights	5.2	Not comply
Logical	There is specialized area for the elimination of access rights	5.2	Not comply
Logical	The elimination of user accounts is supported in a policy and procedure	5.15	Not comply
Logical	The elimination of "identities" is carried out if the applicant and approving	5.16	Not comply
Logical	Period of time for the elimination of users based on regulatory compliance applicable to the organization is established	5.18	Not comply
Logical	Auditable registration of eliminated users is maintained	5.18	Partially complies
Physical	There is a procedure or instruction for the elimination and insurance deletion corporate identification cards.	7.2	Not comply
Physical	The insurance erase of technological identification controls information is carried out for reuse	8.1	Not comply
Physical	Advanced elimination techniques are used, such as safe survey and detailed verification, to ensure that no trace of confidential data is exposed.	8.1	Not comply
Privileged	There is operational responsible for the elimination of privileged users	5.2	Not comply
Privileged	There is specialized area for the elimination of privileged users	5.2	Not comply
Privileged	There is a procedure or instruction for the elimination of users with privileged functions.	8.2	Not comply
Privileged	Responsible personnel inventory for the use of superusers are updated	8.2	Complies
Privileged	The custody flow of superusers is updated	8.2	Complies
Privileged	Auditable record of privileged users eliminated is maintained	5.18	Not comply

Once the diagnostic tool has been completed, it calculates the maturity of each type of access, each phase of the LMU and the regulatory compliance of access management using the formula (1):

$$M = \frac{\sum_{i=1}^{n} \beta_i \times w_i}{n \times W_i} \quad (1)$$

Where:

- *n:* Is the total number of factors evaluated.
- β_i: Is the degree of relative importance with respect to maturity determination.
- w_i: Are the weights assigned to each factor, reflecting their relative importance in determining maturity.
- W_i is the maximum relative weight in determining maturity.

The results obtained from the calculation are shown graphically in the final report (Fig. 3), where the following is detailed: the overall "Maturity level" of the access management process (Fig. 3a), the "Maturity by life cycle phase" (Fig. 3b) and "Maturity level by type of access" (Fig. 3c).

A based on the analysis of the results and the report in Fig. 3, an improvement proposal covering phase P6 was presented to enterprise A, since a maturity level L1 was identified, representing an information security gap for the enterprise, as shown in Fig. 4. This improvement proposal was presented to the case study through its Information Security Committee, contributing to the decision making of senior management and the security team, obtaining their approval for the implementation of the proposal, and thus improving the maturity of the access management of its applications, considering in the future to evaluate areas of improvement in other types and phases of access.

TABLE IX. OPTIMIZED MATURITY LEVEL FOR THE STAGES P2, P3, P4, P5 AND P6 OF LMU

Activate (P2)	Assign (P3)	Review (P4)	Modify / Deactivate (P5)	Delete (P6)
Type: Physical				
Maintenance plans are in place for identification technology controls and physical security for all physical facilities including critical areas	Automatic communication by official means	Preventive maintenance plans for technological controls Measurement of personnel access to critical areas to improve and restrict access dynamically	Accurate, real-time tracking of physical assets	Advanced deletion techniques, such as secure overwriting and detailed verification, are employed to ensure that no trace of sensitive data is exposed
Type: Logical				
The activation of user accounts is fully automated and without significant manual intervention	Authentication requirements are based on risk analysis and continuously improved. Role-based access with real-time visibility into active usage	Ongoing, automated and comprehensive assessment of access rights in relation to roles, duties and positions held. Self-learning analysis tools	Automatic abandoned account detection system at all access levels	Advanced auditing system that records and retains logs after user deletion
Type: Privileged				
The request for superuser use is automatically communicated to the custodians	Activities are measured under the use of privileged functions in the accounts to guarantee minimum accesses	Continuous superuser usage analysis and alerts Automatic report creation	Automatically updates under a period Changes in privileged user are communicated to custodians	Thorough verification that all associated data and accounts have been completely and effectively deleted

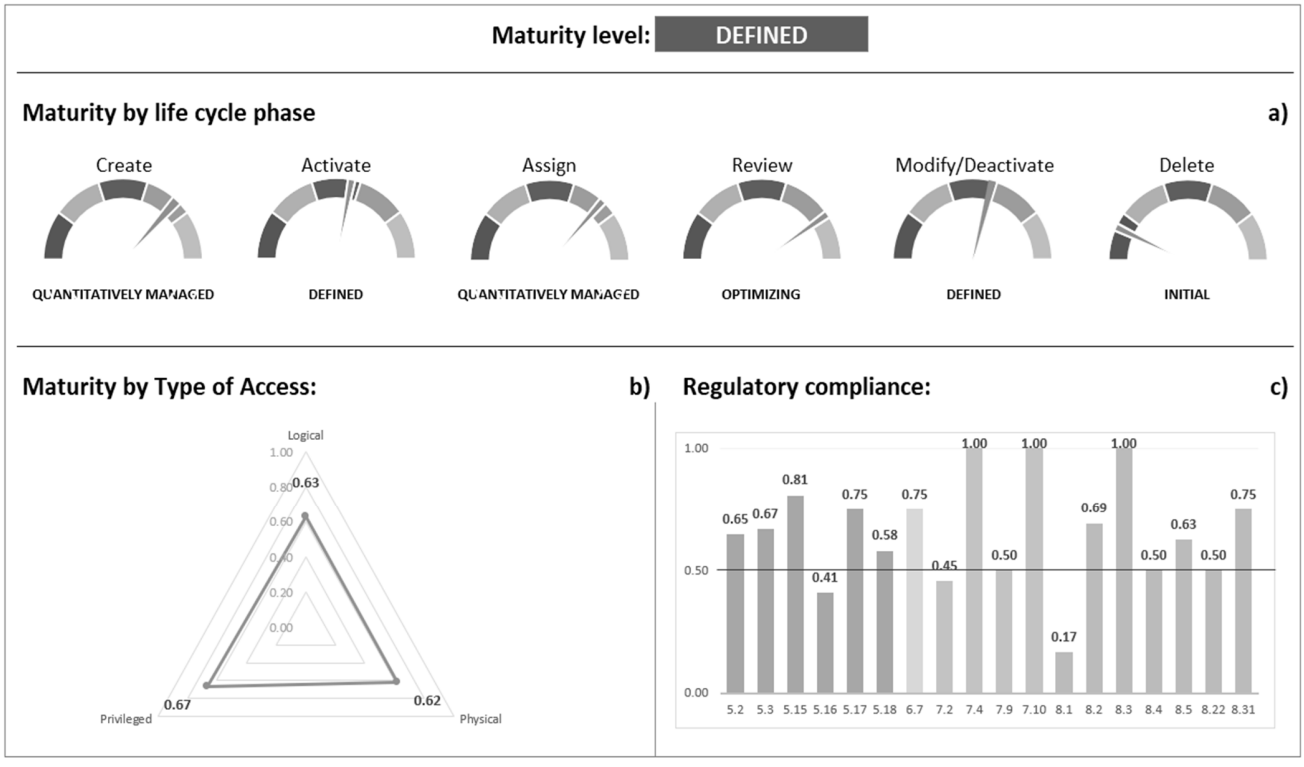
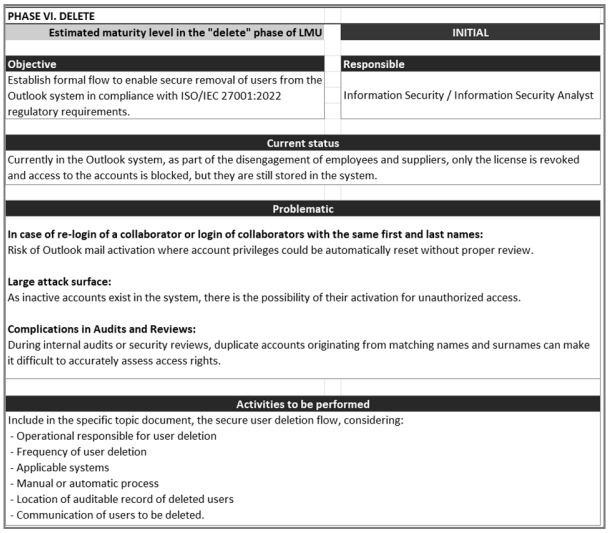


Fig. 3 Report on the results of the enterprise's implementation



PHASE VI. DELETE	
Estimated maturity level in the "delete" phase of LMU	INITIAL
Objective	**Responsible**
Establish formal flow to enable secure removal of users from the Outlook system in compliance with ISO/IEC 27001:2022 regulatory requirements.	Information Security / Information Security Analyst
Current status	
Currently in the Outlook system, as part of the disengagement of employees and suppliers, only the license is revoked and access to the accounts is blocked, but they are still stored in the system.	
Problematic	
In case of re-login of a collaborator or login of collaborators with the same first and last names: Risk of Outlook mail activation where account privileges could be automatically reset without proper review. **Large attack surface:** As inactive accounts exist in the system, there is the possibility of their activation for unauthorized access. **Complications in Audits and Reviews:** During internal audits or security reviews, duplicate accounts originating from matching names and surnames can make it difficult to accurately assess access rights.	
Activities to be performed	
Include in the specific topic document, the secure user deletion flow, considering: - Operational responsible for user deletion - Frequency of user deletion - Applicable systems - Manual or automatic process - Location of auditable record of deleted users - Communication of users to be deleted.	

Fig. 4. Improvement proposal for the case study

IV. CONCLUSION AND FUTURE WORKS

In this study, the construction of a maturity model based on the methodology proposed by De Bruin, composed of 6 phases, was carried out. For this reason, the proposal was developed under the structure of 5 maturity levels (L1, L2, L3, L4 and L5) according to the CMMI model, detailing a set of criteria based on the controls established by the ISO/IEC 27001:2022 standard distributed in 6 phases of the life cycle for 3 types of accesses.

To validate the maturity model, the proposal was exposed to the evaluation of three experts who occupy different positions in the Information Security Management System (ISMS) of the case study. This made it possible to evaluate 6 aspects of the proposal from different perspectives linked to the access management process.

In the same way, the validated model was deployed to an enterprise in order to corroborate the performance and usefulness of the proposal for the evaluation of the access management process.

The results obtained showed that the construction of the maturity model based on a standard accepted by the industry, such as ISO/IEC 27001:2022, facilitated acceptance and reliability in its implementation for the case study. In the same way, the diagnosis of the maturity level based on an access lifecycle contributed to the understanding of the evaluation criteria, consequently, it was possible to clearly identify an area of improvement for the case study. Finally, based on the identification of the improvement area, an improvement proposal was developed and presented, which was promptly accepted by the case study for implementation.

As future work, it is proposed to complete the last phase of the methodology used in this study so that the model can strengthen compliance with security controls related to access management by considering the integration of other information security standards and regulations applicable to the IT services industry.

ACKNOWLEDGMENT

We thank the professors who participated in the study. We also thank the Research Department of the Universidad Peruana de Ciencias Aplicadas for their support.

REFERENCES

[1] IBM. (s/f). ¿Qué son los controles de seguridad?. [Online]. Available: https://www.ibm.com/mx-es/topics/security-controls

[2] M. Zammani, R. Razali & D. Singh, "Organisational Information Security Management Maturity Model," (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 12, no. 9, pp. 668-678, January 2021.

[3] S. Assoul, A. Rabii, K. Ouzzani & O. Roudies, "Information and cyber security maturity models: a systematic literature review," Information and Computer Security, vol. 28, no. 4, pp. 627-644, October 2020.

[4] D. Aponte & G. Maestre, "Dataset about information technology governance: A survey in Colombian enterprises," ISSN 2352-3409, vol. 50, p. 109480, October 2023.

[5] R. Diesch, M. Pfaff & H. Krmar, "A comprehensive model of information security factors for decision-makers," Computers and Security, no. 92, p. 101747, May 2020.

[6] ISO, "Information security, cybersecurity and privacy protection", 27001, October, 2022

[7] L. Wong, D. Rodriguez & D. Mauricio, "A systematic literature review about software requirements elicitation," Journal of Engineering Science and Technology, vol. 12, no. 2, pp. 296-317, February 2017.

[8] B. Barnes & T. Daim, "Information Security Maturity Model for Healthcare Organizations in the United States," IEEE Transactions on Engineering Management, vol. 71, pp. 928-939, January 2022.

[9] K. Wehrle, V. Tozzi, S. Braune, F. Robnagel, H. Dikow, S. Paddock, A. Bergmann & P. Van, "Implementation of a data control framework to ensure confidentiality, integrity, and availability of high-quality real-world data (RWD) in the NeuroTransData (NTD) registry," JAMIA Open, vol. 5, no. 1, pp. 1-9, April 2022.

[10] A. Chu & M. So, "Organizational Information Security Management for Sustainable Information Systems: An Unethical Employee Information Security Behavior Perspective," Sustainability (Switzerland), vol. 12, no. 8, pp. 1-25, April 2020.

[11] A. Alagappan, L. Andrews, S. Venkatachary, D. Sarathkumar & R. Raj, "Cybersecurity Risks Mitigation in the Internet of Things," in Proceedings - 2022 2nd International Conference on Innovative Sustainable Computational Technologies, CISCT 2022, Dehradun, December 2022.

[12] S. AlDaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger & K. Raymond, "The role of national cybersecurity strategies on the improvement of cybersecurity education," Computers & Security, vol. 119, August 2022.

[13] A. Jamal, G. Amjad & E. Sanaa, "GoSafe: On the practical characterization of the overall security posture," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 6, pp. 3079-3095, June 2022.

[14] T. Callari, F. Chiarugi, D. Guerri, A. Pollini, A. Tedeschi, D. Ruscio & L. Save, "Leveraging human factors in cybersecurity: an integrated methodological approach," Cognition, Technology and Work, vol. 24, no. 2, pp. 371-390, May 2022.

[15] A. Reyana, S. Kautish, S. Juneja, K. Mohiuddin, F. Karim, H. Elmannai, S. Ghorashi & Y. Hamid, "Enhanced Cloud Storage

Encryption Standard for Security in Distributed Environments," Electronics (Switzerland), vol. 12, no. 3, February 2023.
[16] I. Skarga, I. Kotsiuba & E. Velasco, "Cyber Hygiene Maturity Assessment Framework for Smart Grid Scenarios," Frontiers in Computer Science, vol. 3, March 2021.
[17] J. Yang, G. Lan, S. Xiao, Y. Li, J. Wen & Y. Zhu, "Enriching Facial Anti-Spoofing Datasets via an Effective Face Swapping Framework," Sensors, vol. 22, no. 13, July 2022.
[18] A. Georgiadou, S. Mouzakitis & D. Askounis, "Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework," Sensors, vol. 21, no. 9, May 2021.
[19] O. Al-Matari, I. Helal, S. Mazen & S. Elhennawy, "Adopting security maturity model to the organizations capability model," Egyptian Informatics Journal, vol. 22, no. 2, pp. 193-199, July 2021.
[20] T. Shimels & L. Lessa, "Maturity of information systems security in selected private Banks in Ethiopia," in 2021 International Conference on Information and Communication Technology for Development for Africa, ICT4DA 2021, Bahir Dar, November 2021.
[21] H. Berrada, J. Boutahar & S. Houssaini, "Simplified IT Risk Management Maturity Audit System based on "COBIT 5 for Risk"," International Journal of Advanced Computer Science and Applications, vol. 12, no. 8, pp. 641-652, January 2021.
[22] K. Razikin & A. Widodo, "General Cybersecurity Maturity Assessment Model: Best Practice to Achieve Payment Card Industry-Data Security Standard (PCI-DSS) Compliance," CommIT Journal, vol. 15, no. 2, pp. 91-104, August 2021.
[23] I. Riadi, I. Yanto & E. Handoyo, "Analysis of academic service cybersecurity in university based on framework COBIT 5 using CMMI," in IOP Conference Series: Materials Science and Engineering, Sorong, October 2019.
[24] D. Sulistyowati, F. Handayani & Y. Suryanto, "Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS," International Journal on Informatics Visualization, vol. 4, no. 4, pp. 225-230, December 2020.
[25] B. Yigit & M. Spruit, "Adaptable Security Maturity Assessment and Standardization for Digital SMEs," Journal of Computer Information Systems, vol. 63, no. 4, pp. 965-987, September 2022.
[26] D. Romero, M. Baldassarre, M. Rodriguez & M. Piattini, "Maturity model based on CMMI for governance and management of Green IT," IET Software, vol. 13, no. 6, pp. 555-563, December 2019.
[27] A. Hassan, S. Mahmood, A. Mohammad & N. Mahmood, "A Maturity Model for Secure Software Design: A Multivocal Study," IEEE Access, vol. 8, pp. 215758-215776, January 2020.
[28] M. Jami, F. Abbasi & B. Sohrabi, "Toward a Maturity Model for Big Data Analytics: A Roadmap for Complex Data Processing," International Journal of Information Technology and Decision Making, vol. 22, no. 1, pp. 377-419, January 2023.
[29] Z. Wang, Y. Li, G. Liu & D. Zhang, "A Multi-User Collaborative Access Control Scheme Based on New Hash Chain," Electronics (Switzerland), vol. 12, no. 8, p. 1792, April 2023.
[30] B. Brimhall, J. Garrard, C. De La Garza & J. Coffman, "A Comparative Analysis of Linux Mandatory Access Control Policy Enforcement Mechanisms," in EUROSEC 2023 - Proceedings of the 2023 European Workshop on System Security, Rome, May 2023.
[31] Z. Han, X. Li, G. Xu, N. Xiong, E. Merlo & E. Stroulia, "An Effective Evolutionary Analysis Scheme for Industrial Software Access Control Models," IEEE Transactions on Industrial Informatics, vol. 16, no. 2, pp. 1024-1034, February 2020.
[32] L. Zhang, B. Li, H. Fang, G. Zhang & C. Liu, "An Internet of Things Access Control Scheme Based on Permissioned Blockchain and Edge Computing," Applied Sciences (Switzerland), vol. 13, no. 7, April 2023.
[33] A. K. Malik, N. Emmanuel, S. Zafar, H. Khattak, B. Raza, S. Khan, A. Al-Bayatti, M. Alassafi, A. Alfakeeh & M. Alqarni, "From Conventional to State-of-the-Art IoT Access Control Models," Electronics (Switzerland), vol. 9, no. 10, pp. 1-34, October 2020.
[34] S. Alshammari, A. Albeshri & K. Alsubhi, "Integrating a High-Reliability Multicriteria Trust Evaluation Model with Task Role-Based Access Control for Cloud Services," Symmetry, vol. 13, no. 3, March 2021.
[35] A. Schrimpf, A. Drechsler & K. Dagianis, "Assessing Identity and Access Management Process Maturity: First Insights from the German Financial Sector," Information Systems Management, vol. 38, no. 2, pp. 94-115, April 2021.
[36] M. Abdul, S. Mishra, A. Mansour & R. Mohammed, "Identity Governance Framework for Privileged Users," Computer Systems Science and Engineering, vol. 40, no. 3, pp. 995-1005, September 2021.
[37] A. Alsirhani, M. Ezz & M. Mostafa, "Advanced authentication mechanisms for identity and access management in cloud computing," Computer Systems Science and Engineering, vol. 43, no. 3, pp. 967-984, January 2022.
[38] S. Fugkeaw, "Achieving Decentralized and Dynamic SSO-Identity Access Management System for Multi-Application Outsourced in Cloud," IEEE Access, vol. 11, pp. 25480-25491, March 2023.
[39] E. Sindiren & B. Ciylan, "Application model for privileged account access control system in enterprise networks," Computers & Security, vol. 83, pp. 52-67, June 2019.
[40] NIST. (2023, August 15). NIST Cybersecurity Framework (CSF) 2.0 Reference Tool. [Online]. Available: https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters
[41] J. B. Santos-Neto & A. P. Costa, "Enterprise maturity models: a systematic literature review," Enterprise Information Systems, vol. 13, no. 5, pp. 719-769, May 2019.
[42] T. De Bruin, R. Freeze, U. Kulkarni & M. Rosemann, "Understanding the Main Phases of Developing a Maturity Assessment Model," in ACIS 2005 Proceedings - 16th Australasian Conference on Information Systems, Australasian, December 2005.
[43] ISACA *COBIT 2019 Framework: Governance and Management Objectives.* Schaumburg: ISACA, 2019
[44] R. Waina. (2018, December 04). Intro to CMMI-SVC Module 1.1. [Online]. Available: https://static.spacecrafted.com/eff8f1444ff547dc97bb98fe24e32d2d/r/bcadbce7d8524899a4eeeba71308c14c/1/CMMI%20V2.0%20Overview.pdf
[45] Oracle. (2023, April 27). Lifecycle for Managing Users. [Online]. Available: https://docs.oracle.com/en-us/iaas/Content/Identity/users/lifecycle-managing-users.htm
[46] D. Salah, R. Paige & P. Cairns, "An Evaluation Template for Expert Review of Maturity Models," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 8892, pp. 318-321, December 2014.