An InfoSec GRC Maturity Model Proposal for a Secure Information Systems Usage on Brazilian Small Organizations

Caio Steglich[1], **Ildevana Poltronieri Rodrigues**[2], **Avelino Francisco Zorzo**[1], **Daniel Dalalana Bertoglio**[1]

[1]Escola Politécnica - Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)

[2]Universidade Federal do Pampa (UNIPAMPA)

caio.steglichb@gmail.com, ildevanarodrigues@unipampa.edu.br

avelino.zorzo@pucrs.br, daniel.bertoglio@edu.pucrs.br

Abstract. *On one hand, Small organizations are highly dependent on Information Systems. On the other hand, small organizations have limited resources, including a lack of specialized professionals and insufficient budgets to invest in Information Security (InfoSec). The objective of this paper is to propose a preliminary Maturity Model focused on Governance, Risk Management, and Compliance (GRC) in the usage of Information Systems in small organizations. The model's levels are designed to enable small organizations to implement several security mechanisms without requiring an expert on the team in the initial stages. This research aims to support small organizations in developing information security (InfoSec) practices for the use of information systems.*

1. Introduction

Several small organizations rely heavily on Information Systems; in this context, Information Security (InfoSec) has become a major challenge, especially in protecting sensitive data [Almubayedh et al. 2018]. Studies indicate that approximately 72% of organizations that suffer cyberattacks are small, and that 50% of them believe they will not be targeted by this type of attack due to their small size [Jahankhani et al. 2022].

Small organizations are defined as those with up to 50 employees [Heidenreich 2017]. Despite their heavy reliance on Information Systems, these organizations face several barriers to achieving adequate security, including limited financial resources for InfoSec investments, a scarcity of readily accessible specialized knowledge, and a limited understanding of the risks they face [Alahmari and Duncan 2021].

In this context, the effective adoption of consolidated InfoSec practices requires managerial actions across governance, risk management, and compliance (GRC). However, hiring InfoSec specialists poses a significant challenge for small organizations, which, unlike large organizations, lack the resources to maintain dedicated teams [Kwong and Pearlson 2024]. This scenario is aggravated by the growing demand for cybersecurity professionals, resulting in a shortage of qualified labor in the field [Ponsard and Grandclaudon 2019].

Therefore, this research aims to develop a maturity model to support the adoption of defensive practices in small organizations' use of Information Systems. The model proposes a set of simplified practices that allow non-expert professionals to develop GRC

practices in the context of InfoSec. Furthermore, the model supports the assessment of the organization's current state relative to its defensive mechanisms and recommends evolutionary actions aligned with its maturity level.

The remainder of the paper is organized as follows: Section 2 describes the theoretical foundations of this work. Section 3 presents the first version of the Proposed Maturity Model, developed with consideration of the literature. Section 4 introduces our initial validation process with InfoSec experts. Section 5 explains the Maturity Model updates based on these experts' recommendations, and Section 6 concludes the paper with considerations and future work.

2. Background

People in small organizations are particularly susceptible to the consequences of cybercrime because employees are often not trained to use information systems in accordance with security strategies. On the other hand, several small organizations, including InfoSec, lack GRC and focus solely on their business operations. Therefore, it may lead to unforeseen consequences, as the organization often expands its business while its infrastructure usually does not evolve at the same rate [Cartwright et al. 2023].

These small organizations have relatively limited budgets, which often leads to a lack of interest in investing in infrastructure improvements or employee training [Harsch et al. 2014]. Additionally, small organizations rarely have formal task assignments for InfoSec responsibilities, resulting in a lack of monitoring and preventive threat identification in their use of information systems [Harsch et al. 2014].

Several factors may influence InfoSec GRC in small organizations, including a lack of specialized expertise, non-technical management, inadequate strategic planning, and the costs of specialized solutions [Alharbi et al. 2021]. Often, small organizations focus on short-term planning, including for their business operations, leading to limited knowledge of local InfoSec legislation and limited prior experience with risks [Jain et al. 2023]. Moreover, the organizational culture tends to be informal, and perceived risk is low [Alharbi et al. 2021].

InfoSec must account for the social model within which the organization operates. In this regard, other countries, through government agencies or non-governmental organizations (NGOs), have developed models, standards, or frameworks to support organizations within their territories. However, some are not specifically tailored to small or micro organizations [Ponsard and Grandclaudon 2019].

3. Proposed Maturity Model

In a previous study, we conducted a systematic mapping of InfoSec GRC literature in small organizations and identified a set of elements to compose a maturity model. This previous mapping presented 28 practices, 5 processes, 6 standards, 23 frameworks, 9 tools, and 6 guidelines, distributed across the levels of the proposed model [1].

The proposed model consists of 8 levels, ranging from 0 to 7, as shown in Figure 1, progressing from non-existent or almost-occasional security to an organization that exports well-established practices. Progression through levels occurs when an organization

[1]Data available at https://zenodo.org/records/19301267 — Accessed on Mar, 28, 2026 at 09:15 PM.

implements all the practices of a given level, thereby enabling it to advance to the next. It is common for some practices from higher levels to be present in the organization, but advancement to the next level occurs only when the complete set of practices is achieved.

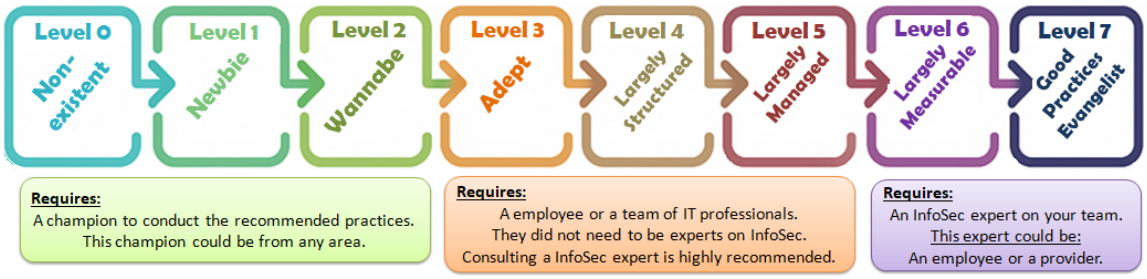

Figure 1. Proposed levels for this Maturity Model

All recommended elements (standards, processes, frameworks, tools, guidelines) are also presented in Figure 2 and can be used by organizations. This model considers the levels at which each element is distributed, since some require greater organizational maturity than others.

3.1. Level 0 - Non-existent

As the title suggests, countless small organizations are at this level, lacking security management and knowledge of the risks to their Information Systems. There is no dedicated person to handle security. Additionally, governance is lacking, as the focus is generally short-term and entirely on the organization's core business. Risk management is performed ad hoc only when risks are imminent. Compliance is limited to the business area, and the organization is unaware of the laws and regulations to which it should adhere.

3.2. Level 1 - Newbie

At this level, we can take initial steps by applying Information Systems practices that require less advanced technical knowledge. Someone within the organization should assume the role of security champion, even if they have other responsibilities. GRC has a short-term vision and has trivial controls. The recommended practices are: 1) Use of strong passwords, 2) Use of antivirus software, 3) Update passwords regularly, and 4) Perimeter security. We can use the Federal Trade Commission (FTC) Guideline at this level [Kwong and Pearlson 2024].

3.3. Level 2 - Wannabe

This level marks the point at which the organization begins to recognize the importance of InfoSec. It requires a technology agent, even if they are not an InfoSec specialist. Governance is generic; all IT and InfoSec decisions are made by non-technical managers who are beginning to understand the importance of the area. Compliance encompasses adherence to InfoSec legal requirements (e.g., General Data Protection Regulation - GDPR). Recommended practices at this level are: 1) regular software updates, 2) an IT asset catalog, 3) removing unused applications, 4) removing unused user accounts, and 5) ensuring that systems are configured correctly. We can use the ENISA Guideline at this level [Ponsard and Grandclaudon 2019].

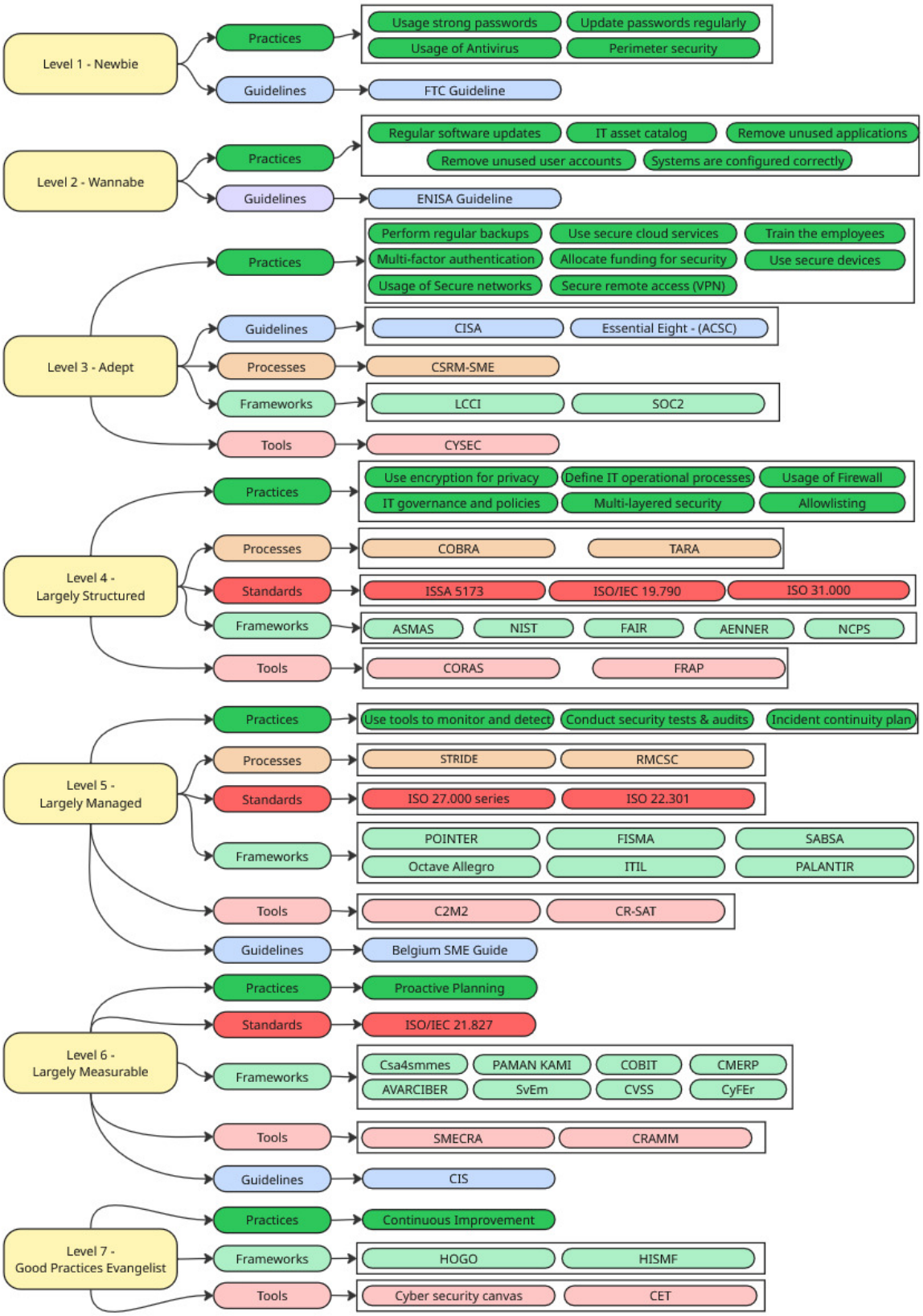

Figure 2. Initial Proposed Maturity Model Resources

3.4. Level 3 - Adept

This is the first level at which high managers recognize InfoSec as important to the organization and begin to structure key InfoSec processes. Furthermore, awareness campaigns for the initial security policies begin. It can be led by a general IT team, which may occasionally rely on expert mentoring (but there is no need for a permanent one in the organization at this level). GRC advances by exposing the organization to InfoSec risks, managing the most likely risks, and complying with applicable legislation (e.g., GDPR).

The recommended practices at this level are: 1) Train the employees, 2) Multi-factor authentication, 3) Perform regular backups, 4) Use secure networks and connections, 5) Ensure secure remote access (VPN), 6) Use secure devices, 7) Use secure cloud services, and 8) Allocate financial support for security implementation. The recommended process is: CyberSecurity Readiness Model for SMEs (CSRM-SME) [Benjamin et al. 2024].

The recommended frameworks are 1) Least Cybersecurity Controls Implementation (LCCI) [Benjamin et al. 2024], and 2) Service Organization Control Type 2 (SOC2) [Kwong and Pearlson 2024]. The recommended tool is: CYSEC [Benjamin et al. 2024] and the recommended guidelines are: 1) Cyber Guidance for Small Businesses (CISA) [Kwong and Pearlson 2024], and 2) Essential Eight (ACSC) [Chidukwani et al. 2022].

3.5. Level 4 - Largely Structured

At this level, InfoSec processes are documented as standard operating procedures (SOPs), and the flows and efforts adopt a more proactive approach, with an established/structured area. At this stage, a general IT team could be supported by an InfoSec expert (but there is no need for a permanent InfoSec team in the organization at this level). InfoSec governance has designed and institutionalized processes. Risk management employs probability and impact analyses, whereas compliance focuses on adherence to standards and legal requirements.

The recommended practices are: 1) Use encryption for sensitive data, 2) Implement IT Governance and security policies, 3) Use a Firewall, 4) Define InfoSec operational processes, 5) Implement multi-layered security measures (e.g., demilitarized zone), and 6) Allowlisting. The recommended processes are: 1) Consultative, objective, and bifunctional risk analysis (COBRA) [Javaid and Iqbal 2017], and 2) Threat Analysis and Risk Assessment (TARA) [AL-Dosari and Fetais 2023]. The recommended tools are: 1) Coordinated Risk Analysis of Security-critical Systems (CORAS); 2) Facilitated Risk Analysis Process (FRAP) [Javaid and Iqbal 2017].

The recommended standards are: 1) Information Security for Small and Medium-Sized Enterprises (ISSA 5173 - UK) [Jahankhani et al. 2022], 2) ISO 31000 (risk management) [Javaid and Iqbal 2017], and 3) ISO/IEC 19.790 (security for cryptographic modules) [Ozkan and Spruit 2019]. The recommended frameworks are: 1) NIST Cybersecurity Framework (CSF) [Ponsard and Grandclaudon 2019], 2) Factor Analysis of Information Risk (FAIR) [AL-Dosari and Fetais 2023], 3) Adaptable Security Maturity Assessment and Standardization (ASMAS) [Yigit Ozkan and Spruit 2023], 4) AENNER [Pérez et al. 2023], and 5) National Cyber Security Policy and Strategy (NCPS) [Ogbeide et al. 2024].

3.6. Level 5 - Largely Managed

The structuring of InfoSec processes enables management based on indicators and implementation goals, allowing the assigned team to make proactive and sometimes predictive moves. An InfoSec specialist at this level is highly recommended for the organization. Governance begins to design indicators. Risk Management Plans for Business Continuity Following Incidents. The recommended practices are: 1) Use tools to monitor and detect threats, 2) Develop business continuity plans for InfoSec incidents, and 3) Conduct tests (pentests), audits, and periodic security assessments.

The recommended processes are: 1) Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) [AL-Dosari and Fetais 2023], and 2) Roadmap for Minimum Cybersecurity Capabilities (RMCSC) [Azinheira et al. 2023]. The recommended standards are: 1) ISO 27.000 (Family: 27.000 - 27.032 - InfoSec Management) [AL-Dosari and Fetais 2023], and 2) ISO 22.301 (Business Continuity) [AL-Dosari and Fetais 2023]. The recommended guideline is: Belgium SME Guide [Ponsard and Grandclaudon 2019].

The recommended frameworks are: 1) Information Technology Infrastructure Library (ITIL) [Javaid and Iqbal 2017], 2) Operationally Critical Threat, Asset, and Vulnerability Evaluation (Octave Allegro) [Javaid and Iqbal 2017], 3) Federal Information Security Modernization Act (FISMA) [Ogbeide et al. 2024], 4) Sherwood Applied Business Security Architecture (SABSA) [AL-Dosari and Fetais 2023], 5) PALANTIR [Mlakar et al. 2021], and 6) POINTER [Archibald and Renaud 2018]. The recommended tools are: 1) Cybersecurity Capability Maturity Model (C2M2) [AL-Dosari and Fetais 2023], and 2) Cyber Resilience Self-Assessment Tool (CR-SAT) [Carías et al. 2021].

3.7. Level 6 - Largely Measurable

At Level 6, all implemented InfoSec processes and controls are measurable and quantifiable. Data is collected, and it can be measured whether a policy, strategy, or process is working as intended or failing for some reason. The team must be trained to implement and manage InfoSec controls, and the data generated should support informed decision-making. Risks are generally contained through preventive procedures. Compliance hires external experts for regular audits.

The recommended practice is to develop a dashboard for monitoring InfoSec data. The recommended standard is: ISO/IEC 21.827 (Systems Security Engineering) [Anass et al. 2020]. The recommended tools are: 1) SME Cyber Risk Assessment (SME-CRA) [AL-Dosari and Fetais 2023], or 2) CCTA Risk Analysis and Management Method (CRAMM) [AL-Dosari and Fetais 2023]. The recommended guideline is: The Center for Internet Security (CIS) Critical Security Controls [Jahankhani et al. 2022].

The recommended frameworks are: 1) Control Objectives for Information and Related Technology (COBIT) [Javaid and Iqbal 2017], 2) Common Vulnerability Scoring System (CVSS) [Pérez et al. 2023], 3) Csa4Smmes [Lejaka et al. 2023], 4) AVARCIBER [Jayathilaka and Wijayanayake 2025], 5) Coordinated Malware Eradication and Remediation Platform (CMERP) [Mutalib et al. 2021], 6) Cybersecurity Vulnerability Mitigation Framework Through Empirical Paradigm (CyFEr) [AL-Dosari and Fetais 2023], 7) Peni-

laian Mandiri Keamanan Informasi (PAMAN KAMI) [Wardana and Suryani 2021], and 8) Security visualization effectiveness measurement (SvEm) [Ahmed and Nanath 2021].

3.8. Level 7 - Good Practices Evangelist

At this final level, the organization has become a benchmark for good InfoSec practices, sharing knowledge with the community of practice and entering a process of refining and continuously improving its controls, processes, and policies. GRC is exemplary because corporate governance recognizes the need for InfoSec, risk management is preventive and data-driven, and compliance aligns with laws and quality standards. It is worth noting that a company at level 7 is not immune to security threats, but is considerably better protected than at other levels.

The recommended frameworks are: 1) HOGO [Cruzado et al. 2022], or 2) High-level self-sustaining information security management framework (HISMF) [Kaušpadienė et al. 2019]. The recommended tools are: 1) Cyber security canvas [Scholl and Schuktomow 2021], and 2) SME cybersecurity evaluation tool (CET) [Ponsard and Grandclaudon 2019].

4. Insights from Initial Validation

Flick explains that interviews with experts can be used for the following purposes [Flick 2014]: i) to explore a new field; ii) to collect information that complements insights gained from the application of other methods; or iii) to generate theories to develop a typology or a theory about an issue based on the reconstruction of knowledge from various experts. We decided to invite some InfoSec experts on order to evaluate the initial version of this Maturity Model. The interviews were conducted on the Zoom platform[2], and, in each interview, we obtained the interviewee's consent through a clarification and free consent form, which was signed by the researcher and the interviewee.

After that, three preliminary interviews were conducted with experts to validate the proposed model, which was developed based on a prior literature review. The first interviewee (E1) holds a degree in Computer Science and has 8 years of experience in the security field, currently serving as a Consultant and InfoSec Manager. The second interviewee (E2) also holds a degree in Computer Science and 8 years of experience in the security field, and currently serves as an Operational InfoSec Manager. The third interviewee (E3) holds a degree in Information Systems and an MBA in cybersecurity, and has 15 years of experience in cybersecurity. All interviewees were Brazilians and worked mainly for Brazilian organizations.

Figure 3 presents the new model version based on experts' perceptions, taking into account the Brazilian national context.

5. Second Version of the Maturity Model - Updates

At the first level, experts only recommended changing "perimeter security" to "Device with screen locking", as other perimeter security measures could be too complex for small organizations at this level. At level 2, Specialist E1 recommended adding the practice:

[2]https://www.zoom.com/pt — Accessed on Jan. 28, 2026 at 11:20 AM.

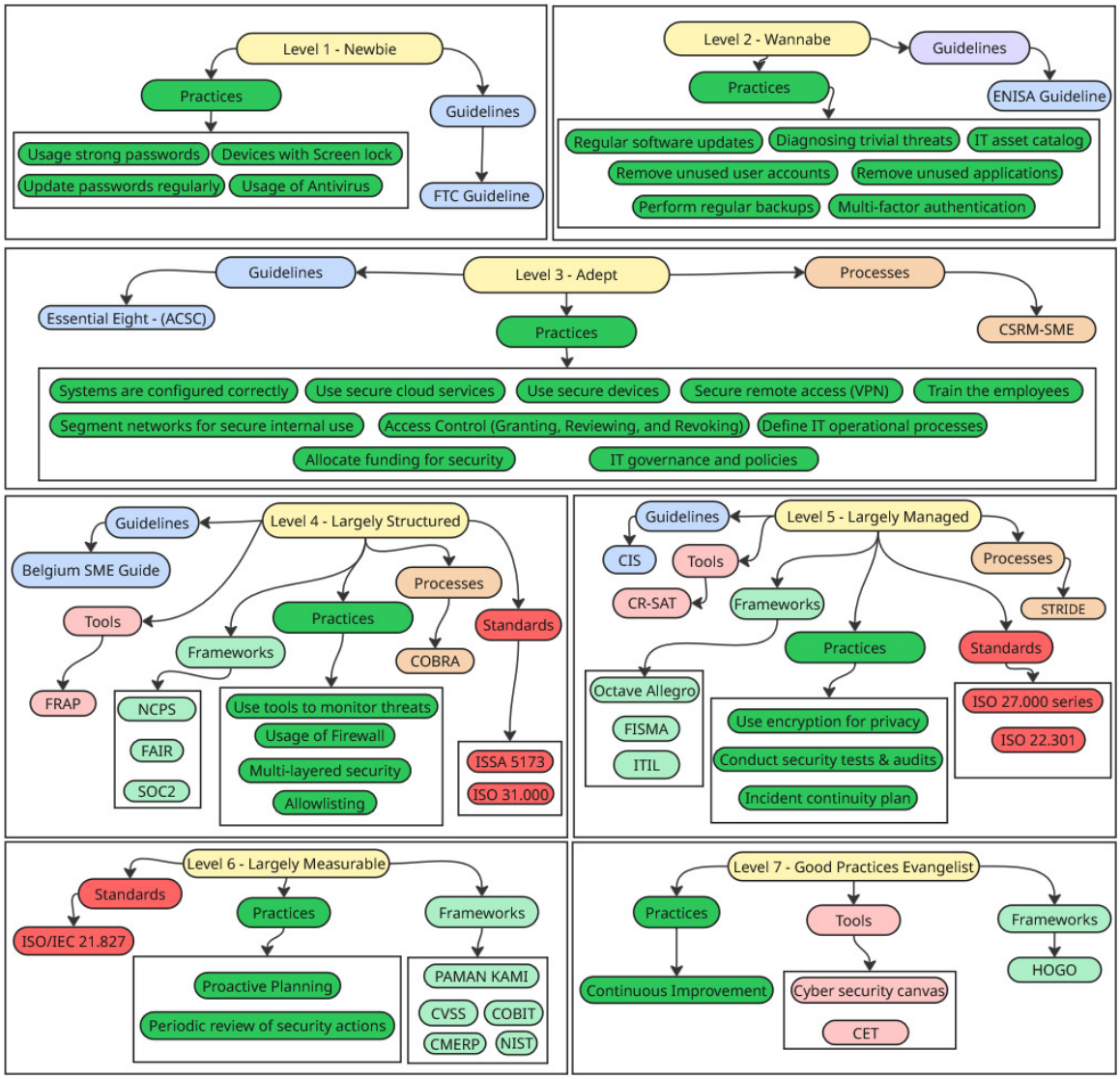

Figure 3. Proposed Maturity Model Resources - New Version

"Diagnose trivial threats", while E2 recommended bringing forward the practices "Multifactor authentication" and "Perform regular backups", considering them simple enough to be performed at this level.

At level 3, experts recommend adding "Systems are configured correctly" to the practices, which was previously at level 2. Additionally, the practices "Define IT operational processes" and "IT Governance and policies" were brought forward. E2 also added the practice titled "Access Control (Granting, Reviewing, and Revoking)". Experts believe that some levels contain too many elements, which can hinder the model's usability. E3 recommends the CISA guideline, as it is redundant with other models and the CYSEC tool at this level, given the national context.

At level 4, experts recommended that the practice "Use tools to monitor and detect", originally at level 5, be moved to this level. Also, the practice "Use encryption for privacy" was moved to level 5. The SOC2 framework was recommended to be upgraded from level 3 to level 4. The "Belgium SME Guide" was recommended for level 4, and

the elements of ISO 19790, LCCI, ASMAS, AENNER, and CORAS are pointed out by experts as being too complex to implement without a dedicated security specialist within the company.

At level 5, experts recommend including the CIS guideline. Experts describe the elements of SABSA, C2M2, and POINTER as overly complex for small businesses. Experts recommend removing the RMCSC because it is specific to software development, and PALANTIR because it is exclusive to outsourcing.

At level 6, experts recommended incorporating the practice: "periodic review of security actions", and the NIST framework was transferred to this level. The SMECRA, CRAMM, CSA4SMMES, AVACIBER, CyFEr, and SvEm elements were excluded due to the complexity of their implementation in small organizations. At level 7, experts recommended removing only the HISFM framework.

5.1. Experts' Concerns About the Model

This section presents the experts' concerns and suggestions for the maturity model, including their initial version and the updates they suggested.

Evolution of small organizations to the highest level: "I believe that from level 4 onwards, small businesses may have difficulty advancing because the recommendations require greater financial resources than the previous recommendations. Furthermore, it is impossible to advance from level 5 to 7 without the guidance of a security expert" (E1). We have designed a model in which, at levels 0-2, the organization can select a non-technical professional to implement basic security measures. From levels 3 to 5, the same professional(s) can conduct these measures, provided they are mentored by an expert. Levels 6 and 7 require an expert who dedicates a few hours per week to leading the efforts in these organizations.

Need for support materials: "I felt that descriptions alone could be insufficient to support organizations in implementing security mechanisms. An example would be: Use tools to monitor threats, but which tool to choose? How to install it? This level of detail can come either from a detailed guideline to Brazilian organizations based on the other elements or from a community of practice in which professionals voluntarily support these organizations" (E2). Our maturity model is in its initial phase and will need to be complemented with practical guidelines for implementing security features, which will be developed and finalized during their application in small organizations.

Several elements in the first version of the model: "I understand the idea of offering a list with frameworks, standards, and guidelines to the small businesses. However, this makes it difficult to choose which ones are most recommended and what adaptations are needed for each element to work in small businesses. I recommend choosing 1 to 3 elements per type at each level, removing some that are generic or that are too complex to adapt for small businesses"(E3). Both experts scored each level for the elements they considered should be removed, and this is reflected in the reduction of elements in the new version shown in Figure 3.

All recommendations and suggestions presented by the experts were considered and have influenced the model and its intended use. As this is at an early stage of maturity, practical application experience should also contribute to its refinement, along with

greater participation by more experts.

6. Threats to Validity

This research presents a preliminary maturity model based primarily on a systematic literature mapping and an initial round of expert evaluation. It occurs because the proposed model is in an early stage, and we understand that it should be evaluated by more InfoSec experts and applied in real organizations to adjust their recommendations. It will support the assessment of the model's practical effectiveness, usability, and impact on InfoSec practices.

Another limitation concerns the sample size and scope of the expert evaluation. The study initially relies on interviews with three InfoSec experts from Brazil, but a broader evaluation involving a more diverse group of experts across regions, industries, and organizational contexts would strengthen the model's robustness. Also, the proposed maturity model may face limitations regarding its applicability across different settings in small organizations, which are highly heterogeneous in terms of resources, technological maturity, and regulatory environments.

7. Future Plans

In this paper, we propose a preliminary InfoSec GRC maturity model specifically designed for micro and small organizations, addressing their well-known constraints such as limited resources, lack of specialized employees, and low InfoSec awareness. By structuring InfoSec practices into progressive maturity levels, the model offers a practical pathway for organizations to gradually improve their InfoSec posture without requiring immediate access to expert knowledge (levels 1 and 2).

The results of the initial evaluation with domain experts indicate that the model has the potential to be both relevant and applicable to Brazilian small organizations. The feedback obtained supported improving the model's structure by refining its elements, enhancing its usability, and aligning it more closely with real-world constraints. These findings suggest that the proposed model has the potential to bridge the gap between theoretical InfoSec frameworks and the practical needs of micro and small organizations.

Beyond its current state, the main contribution of this work is to establish a foundation for future empirical investigation. This model provides a structured basis for further evaluation, refinement, and practical application. Future work should focus on applying the model in case studies and action research settings, and on expanding the evaluation to include a broader range of InfoSec experts.

Acknowledgements

The authors acknowledge CAPES/PROEX for their financial support during the development of this work. Avelino F. Zorzo is financed by CNPq grant #308752/2025-2.

We used the tool Grammarly [3] in order to improve the writing process and avoid typing issues.

[3]https://www.grammarly.com/ — Accessed on Mar, 28, 2026 at 21:43.

References

Ahmed, N. N. and Nanath, K. (2021). Exploring cybersecurity ecosystem in the middle east: Towards an sme recommender system. *Journal of Cyber Security and Mobility*, 10(3):511–536.

AL-Dosari, K. and Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (smes): A meta-analysis approach. *Electronics*, 12(17):3629.

Alahmari, A. A. and Duncan, R. A. (2021). Investigating potential barriers to cybersecurity risk management investment in smes. In *Proceedings of the International Conference on Electronics, Computers and Artificial Intelligence*, pages 1–6, Pitesti, Romania. IEEE.

Alharbi, F., Alsulami, M., Al-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., and Al-Otaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in saudi arabia. *Sensors*, 21(20):6901.

Almubayedh, D., Alazman, G., Alabdali, M., Al-Refai, R., Nagy, N., et al. (2018). Security related issues in saudi arabia small organizations: a saudi case study. In *Proceedings of the Saudi Computer Society National Computer Conference*, pages 1–6, Riyadh, Saudi Arabia. IEEE.

Anass, R., Saliha, A., and Roudiès, O. (2020). A concept & compliance study of security maturity models with iso 21827. In *International Conference on Enterprise Information Systems*, pages 385–392, Online Streaming. IEEE.

Archibald, J. and Renaud, K. (2018). Pointer: A gdpr-compliant framework for human pentesting (for smes). In *Proceedings of the International Symposium on Human Aspects of Information Security & Assurance*, pages 147–157, Dundee, Scotland. Springer.

Azinheira, B., Antunes, M., Maximiano, M., and Gomes, R. (2023). A methodology for mapping cybersecurity standards into governance guidelines for sme in portugal. *Procedia Computer Science*, 219:121–128.

Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., and Adeusi, K. B. (2024). Digital transformation in smes: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances*, 19(2):134–153.

Carías, J. F., Arrizabalaga, S., Labaka, L., and Hernantes, J. (2021). Cyber resilience self-assessment tool (cr-sat) for smes. *IEEE Access*, 9:20–33.

Cartwright, A., Cartwright, E., and Edun, E. S. (2023). Cascading information on best practice: Cyber security risk management in uk micro and small businesses and the role of it companies. *Computers & Security*, 131:103288.

Chidukwani, A., Zander, S., and Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. *IEEE Access*, 10:85701–85719.

Cruzado, C. F., Rodriguez-Baca, L. S., Huanca-López, L. G., and Acuña-Salinas, E. I. (2022). Reference framework "hogo" for cybersecurity in smes based on iso 27002

and 27032. In *Proceedings of the International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, pages 35–40, Noida, India. IEEE.

Flick, U. (2014). *An introduction to qualitative research*. Sage Publications.

Harsch, A., Idler, S., and Thurner, S. (2014). Assuming a state of compromise: A best practise approach for smes on incident response management. In *Proceedings of the International Conference on IT Security Incident Management & IT Forensics*, pages 76–84, Münster, Germany. IEEE.

Heidenreich, M. (2017). How to design a method for measuring it security in micro enterprises for it security level measuring? a literature analysis. In *Proceedings of the Communication and Information Technologies*, pages 1–9, Vysoke Tatry, Slovakia. IEEE.

Jahankhani, H., Meda, L. N., and Samadi, M. (2022). Cybersecurity challenges in small and medium enterprise (smes). In Jahankhani, H., Kilpin, D., and Kendzierskyj, S., editors, *Blockchain and Other Emerging Technologies for Digital Business Strategies*, chapter 1, pages 1–19. Springer, Cham, Switzerland.

Jain, R., Prajapati, D., and Dangi, A. (2023). Transforming the financial sector: A review of recent advancements in fintech. *International Journal for Research Trends and Innovation*, 8(2):250–267.

Javaid, M. I. and Iqbal, M. M. W. (2017). A comprehensive people, process and technology (ppt) application model for information systems (is) risk management in small/medium enterprises (sme). In *Proceedings of the international conference on communication technologies*, pages 78–90, Rawalpindi, Pakistan. IEEE.

Jayathilaka, H. and Wijayanayake, J. (2025). Systematic literature review on developing an ai framework for sme cybersecurity identification and personalized recommendations. *Journal of Desk Research Review and Analysis*, 2(2):233–247.

Kaušpadienė, L., Ramanauskaitė, S., and Čenys, A. (2019). Information security management framework suitability estimation for small and medium enterprise. *Technological and Economic Development of Economy*, 25(5):1–19.

Kwong, J. and Pearlson, K. (2024). Supply chain cybersecurity and small and medium-sized enterprises (smes): Exploring shortcomings in third party risk management of smes. In *Proceedings of the Hawaii International Conference on System Sciences*, pages 211–224, Honolulu, USA. Springer.

Lejaka, T. K., da Veiga, A., and Loock, M. (2023). Towards roles and responsibilities in a cyber security awareness framework for south african small, medium, and micro enterprises (smmes). In *Proceedings of the International Symposium on Human Aspects of Information Security and Assurance*, pages 211–224, Kent, UK. Springer.

Mlakar, I., Jeran, P., Šafran, V., and Logothetis, V. (2021). A cost-effective security framework to protect micro enterprises: Palantir e-commerce use case. In *Proceedings of the International Symposium on Digital Forensics and Security*, pages 1–6, Elazig, Turkey. IEEE.

Mutalib, M. M. A., Zainol, Z., and Halip, M. H. M. (2021). Mitigating malware threats at small medium enterprise (sme) organisation: A review and framework. In *Proceed-*

ings of the IEEE International Conference on Recent Advances and Innovations in Engineering, pages 1–6, Kedah, Malaysia. IEEE.

Ogbeide, V. O., Omorogiuwa, O., and Salami, E. E. (2024). A cyber security framework to strengthen small and medium scale enterprises (smes) in nigeria. *International Journal of Science Academic Research*, 4(9):6301–6310.

Ozkan, B. Y. and Spruit, M. (2019). Cybersecurity standardisation for smes: the stakeholders' perspectives and a research agenda. *International Journal of Standardization Research*, 17(2):41–72.

Pérez, A. G., Martínez, A. L., and Pérez, M. G. (2023). Adaptive vulnerability-based risk identification software with virtualization functions for dynamic management. *Journal of Network and Computer Applications*, 219:103728.

Ponsard, C. and Grandclaudon, J. (2019). Guidelines and tool support for building a cybersecurity awareness program for smes. In *Proceedings of the International Conference on Information Systems Security and Privacy*, pages 335–357, Prague, Czech Republic. Springer.

Scholl, M. and Schuktomow, R. (2021). The current state of–information security awareness" in german smes. *International Journal of Emerging Technology and Advanced Engineering*, 11(12):151–163.

Wardana, A. A. and Suryani, E. (2021). Evaluation of information security management in micro, small, and medium enterprises (msmes) using penilaian mandiri keamanan informasi (paman kami). In *Proceedings of the International Conference on Management of Technology, Innovation, and Project*, pages 1–12, Surabaya, Indonesia. MOTIP.

Yigit Ozkan, B. and Spruit, M. (2023). Adaptable security maturity assessment and standardization for digital smes. *Journal of Computer Information Systems*, 63(4):965–987.

About the Authors

Caio Steglich has a BSc degree in Information Systems (2016) and a MSc (2019) degree on computer science from Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS, Porto Alegre, Brazil). Currently, he is a PhD student at PUCRS and this paper is an outcome related to his doctoral research. Today, he is an adjunct professor at Uniasselvi (Centro Universitário Leonardo da Vinci).

Ildevana Poltronieri Rodrigues has Bsc degree on Mathematics (2003) from Universidade da Região da Campanha (URCAMP) and Bsc degree in Information Systems (2016) and a MSc (2018) and a PhD (2021) degree in computer science from Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS, Porto Alegre, Brazil). Dra. Ildevana currently is an adjunct professor at Universidade Federal do Pampa (UNIPAMPA, Alegrete, Brazil).

Avelino Francisco Zorzo has a BSc (1989) and a MSc (1994) degree in computer science from Universidade Federal do Rio Grande do Sul (Porto Alegre, Brazil). He received a PhD in computer science from University of Newcastle (Newcastle, UK) in 1999, and was a postdoctoral fellow (2012) at the Cybercrime and Computer Security Centre at the same university. Currently he is a full professor at Pontifical Catholic University of Rio Grande do Sul (PUCRS). Dr. Zorzo served as the education director of the Brazilian Computing Society (2015–2017) and was coordinator for postgraduate accreditation at the Ministry of Education of Brazil (2014–2030). His main research topics are security, digital forensics, blockchain, fault tolerance, and software testing.

Daniel Dalalana Bertoglio has a BSc (2008) degree in Computer Science from Universidade Feevale, an MSc (2011) degree in Applied Computing from Universidade do Vale do Rio dos Sinos, and a PhD (2019) from Pontifícia Universidade Católica do Rio Grande do Sul. He is currently the CEO of WSS Security and a adjunct professor at Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS).