Maturity Model for Building Information Management and Security

Eduardo Ribeiro dos Santos, eduardo.ribeiro@fau.ufrj.br
PROARQ, Federal University of Rio de Janeiro, Brazil

Monica Santos Salgado, monicassalgado@fau.ufrj.br
PROARQ, Federal University of Rio de Janeiro, Brazil

Sergio Scheer, sergioscheer@gmail.com
Federal University of Paraná, Brazil

Abstract
The adoption of Building Information Modeling (BIM) in architectural Brazilian offices has been rapidly increasing due to the numerous benefits it provides architects in their design decision-making process. However, when using BIM, information related to the physical and functional aspects of the building can be read and interpreted by computers. As a result, this information becomes vulnerable to intentional or accidental cyber-attacks. Considering this, it is essential for architects to employ strategies to safeguard project information. This paper proposes a maturity model for the adoption of information management and security, specifically tailored to architectural firms that utilize BIM in their project development. The model is structured based on guidelines found in the ISO 19650 series, as well as the Brazilian General Data Protection Law and other relevant directives. Additionally, a risk matrix was developed in conjunction with an analysis of documents from companies that have incorporated BIM into their projects. The maturity model outlines pathways for architectural firms to implement measures that ensure information security throughout project development. These measures contribute to advancing BIM adoption while considering the risks associated with innovative processes.

Keywords: BIM, Information Security, Information Management

1 Introduction

Due to the fact that government institutions and companies have been suffering from a constant increase in security incidents, Alencar (2018), points out that in the academic area, research dealing with the subject in question focuses mainly on technical aspects in relation to systems, networks and physical security. Dealing only with issues related to technology is not enough to achieve information security, and a connection with other areas is necessary to address issues related to management, governance, processes, procedures and especially human aspects.

The World Economic Forum, in its 2024 report on the global vision of cybersecurity, highlights that most organizations are not adequately equipped to face challenges related to information security. Several factors contribute to this, including the high cost of implementing security tools, the increase in the quantity and variety of malware, the advancement and use of generative artificial intelligence, the scarcity of qualified professionals to deal with these issues and, above all, the desire to adopt new technologies to boost the business. Protecting older systems used by organizations has also been identified as a key issue (WEF, 2024).

As BIM adoption (*Building Information Modeling*) and the increasing use of ICTs (Information and Communication Technologies) by the construction industry occurs, mainly by architectural offices, seeking to meet the demands of an increasingly demanding market, it becomes relevant to embrace the concept of collaborative work. This implies not only greater openness and transparency, but also the sharing and use of detailed models with a large amount of information. This set of information is generated from data in digital format, which is read, understood and processed by the computer, transforming it into intelligent data. As a result, the possibility of extracting this information by people who are not professional experts in the field becomes more real every day.

This paper, part of a doctoral thesis, aims to present a maturity model for the adoption of Building Information Management and Security (BIMS). For this, a risk analysis was used to identify information management and security (IMS) guidelines for the standards: NBR ISO 19650 parts 1 and 2, ISO parts 4 and 5; ABNT ISO 27001 and LGPD (General Data Protection Law - Brazilian law that deals with Data Protection). As a result, a maturity model with 5 sets of guidelines for IMS is presented. These sets of guidelines aim not only to evaluate project companies, but also to guide the steps to be taken so that the production of collaborative information is carried out safely.

2 Information Management and Security (IMS) in the BIM context

Information security, despite involving a set of people, processes and technology (De Oliveira, 2012; Da Silva, 2015), is treated in different fields: confidentiality, integrity, availability, legality, authenticity, auditability and non-repudiation. The complexity of organizational environments relating to design, construction, operation and maintenance companies means that decision-making on the development of buildings is based on information. As a result, the need to manage and secure information becomes increasingly necessary.

With the aim of guiding professionals during the adoption of BIM, the International Organization for Standardization (ISO) has been establishing regulations regarding information management for the use of Building Information Modeling. Among the standards we can highlight the ISO 19650 series. With a focus on improving the delivery of information regarding design specifications when using ICTs (UKBIM, 2019), ISO 19650 is divided into 6 parts. In Brazil, in 2020, parts 1 and 2 were published in Portuguese version by the Brazilian Association of Technical Standards (ABNT), the body responsible for developing and publishing standards in Brazil.

Part 5 of the standard present aspects of the information security approach to information management. The main of this part is to help professionals understand the vulnerabilities in relation to computer systems and present the challenges to be considered when using ICTs in the development of projects.

Turk et al. (2022) highlight that the development phases of projects that intensively use information are the most vulnerable to cybersecurity risks. The main cybersecurity incidents in building include data breaches and loss of information ownership (Mantha et al, 2021). Peres (2019) highlights the occurrence of cyber-attacks which, although they do not cause damage, aim to recognize, map and spy on information, as in an installation in the electricity sector, for example.

In Brazil, on August 14, 2018, Federal Law No. 13,709 was established, which establishes rules for the processing and protection of personal data, this law is known as the General Data Protection Law or LGPD (Brazil, 2018). Furthermore, the Brazilian Association of Technical Standards (ABNT) has been publishing specific standards, such as NBR ISO/IEC 27001, which deals with the requirements for IMS systems. This standard, as well as ISO 19.650-5 and LGPD, directly impact the AECO industry and the entire process of design, execution, operation and maintenance of the building.

3 Risk Analysis in the BIM context

The concept of "risk" has evolved over time. In pre-modern times, it was seen neutrally, associated with the probability of gain or loss. In the modern era, it became associated with a negative danger factor (Granjo, 2006). Today, risk is linked to uncertainty in relation to an organization's strategic objectives, and can represent both threats and opportunities (ABNT, 2018; PMI, 2022). For information security, risk is understood as the possibility of a specific threat taking advantage of the weaknesses of a certain resource, or a set of resources. (Brunner et al., 2020).

According to ABNT NBR ISO 31000 (2018), Rosa and Toledo (2015), Simão et al. (2019), ABNT NBR ISO/IEC 27005 (2019), Ariyani and Sudarma (2016), De Oliveira (2017), Takagi and Varajão (2020), Frederico (2021), Sari et al (2020) and Vargas and Campos (2022), risk analysis must occur considering the following steps: definition of the context, identification of risks, analysis of risks, assessment of risks, treatment of risks and acceptance of risks.

Considering the above, in *definition of the context*, the chosen focus was the field of legality considering the aspects presented NBR ISO 19650 part 1 (ABNT, 2020a) and NBR ISO 19650 part 2 (ABNT, 2020b), ISO 19650 part 4 (ISO, 2022) and ISO 19650 part 5 (ISO, 2020), LGPD - General data protection law (Brazil, 2018) and NBR ISO/IEC 27001 (ABNT, 2022c).

For the risk identification and analysis stages, the afore mentioned standards and law were analyzed and consolidated with the aim of identifying aspects that would determine guidelines for IMS. The result of this analysis culminated in a total of 59 guidelines (to be presented in the maturity model)

In relation to risk assessment, a probability and impact matrix (PIM) was used. In order for the probability factor of PIM to occur, a documentary analysis was carried out with companies associated with BIM Forum Brazil and public bodies that act as hirers and hired in an architectural project development process. The objective of this document analysis was to understand how issues related to management and information security are handled when using BIM and to compare them with the guidelines identified through the practices used by these companies. In total, 9 companies and public bodies contributed 94 documents to the research. These documents include Scope of contracting; Terms and confidentiality agreements; Contracts and draft contracts for service provision; Compliance Agreement; Design guidelines; Third party management policies; Notice; Terms of reference; Risk Matrix; BIM manuals, produced by the company itself or by third parties; BIM Project Booklet; and Data Security Protocols.

Regarding the impact factor, it was established that the guidelines related to the initial stages of information management were considered a Very High impact factor; the guidelines relating to the steps that deal with the organization and distribution of Information as High impact; and guidelines that address issues about the use of information and Development of products and services as a medium impact.

As a result of the risk analysis, none of the guidelines presented Low Risk and 7% presented medium risk. 93% of the guidelines are presented as High Risk. The high number of guidelines presented as High Risk is due to the fact that approximately 70% of the guidelines identified and highlighted by the research are not even mentioned in the documents and protocols delivered by companies.

4 Maturity Model for Building Information Management and Security (BIMS)

After the identification and risk classifications of the guidelines for IMS, a strategy was established as risk treatment and acceptance to guide the adoption of the respective guidelines. This strategy resulted in the Maturity Model presented in this article.

According to Salgado (2022) BIM "Maturity" and "Capacity" are concepts discussed by several authors that highlight the importance of establishing a BIM Implementation Plan for companies. According to BIMe (2023), BIM Maturity is the gradual and continuous improvement in quality, repeatability and predictability within the available BIM capacity, and is expressed as Maturity Levels.

The importance of these models lies in the chance they provide companies to implement BIM, especially because there are organizations that are hesitant to adopt BIM due to the complexity of choosing the most appropriate implementation techniques. Likewise, for companies seeking to improve their BIM deliveries, especially regarding information security issues, these models are valuable as they offer guidelines for identifying and prioritizing subsequent steps.

Maturity Models are built for knowledge management, information technology governance and Building Information Modeling, varying according to the size of the company, sector of activity, location and organizational perspectives (Oliveira, 2011). Stages range from 3 to 5, with an initial focus on preparation and adoption, followed by integration, evaluation and routine processes.

In information technology governance, models such as COBIT, ITIL and CMMI-SVC are used, with levels ranging from 0 (incomplete) to 6. The initial phase is covered at Level 1, the managerial phase at Levels 2 to 4, the established process at levels 3 and 4, and the optimized phase generally at levels 4 and 5 (Aguiar et al, 2018).

In the context of Building Information Modeling, models such as NBIMS CMM and BIM Maturity Matrix are used to evaluate the adoption of BIM by construction companies. Levels range from 5 to 6, with the first stages covering basic subjects and the rest considered advanced (Magalhães, 2022; Yilmaz et.al., 2017).

Finally, Lima et al (2021) state that the structure of a maturity model must include three factors: objectives, issues and metrics. The objectives define the model's guidelines, the questions help identify guidelines adopted at a specific stage, and the metric defines the company's degree of maturity.

Therefore, there is no specific standard for organizing the steps that will make up a Maturity Model, as they are built according to the objectives for their application. But this flow is organized into initial, intermediate and final phases. Considering the above, 5 Sets of Guidelines were established: IMS Initiation, IMS Planning, IMS Approach, IMS Quality Control and New Guidelines for IMS.

It is worth mentioning that, unlike some existing Maturity Models, the one presented in this article does not use the term levels, stages or phases. This is because companies can comply with several guidelines in different sets at the same time, and consequently have different maturities across these sets when considering specific objectives for BIMS adoption. That said, maturity will occur in two spheres, one in each Set of Guidelines and the other in general.

To group the guidelines into their respective sets, an analysis of the relationship between the guidelines was carried out, seeking to establish a logical sequence between predecessor and successor activities/decisions. For example: before "developing the planning, implementation, control of processes and records for the operation of the Information Security Management System (ISMS)", it is necessary to "carry out the planning of the ISMS". Therefore, the first cited guideline must be in a later set of guidelines than the second cited.

4.1 Set of Guidelines 1 – Getting Started with IMS

This set of guidelines aims to evaluate and assist in preparing for the beginning of the adoption of the information security approach. It is the basis, as any action not taken could have a negative impact on others, which could affect the success of information security. The guidelines represent 11.86% of the total. The guidelines are:

- establish information security requirements in the OIR (Organization Information Requirements).
- establish information security requirements in the PIR (Project Information Requirements).
- establish information security requirements in the EIR (Exchange Information Requirements).
- determine if an information security approach is necessary.
- need for an information security approach using a sensitivity assessment process.
- define information security objectives.
- establish information security policy.

4.2 Guideline Set 2 - IMS Planning

This set of guidelines has the highest number of guidelines, 29 out of 59, representing 49.15% of the total guidelines. Its objective is to plan actions for the guidelines of this set are:

- understand the range of security risks.
- identify organizational sensitivities.
- undertake a sensitivity assessment process.
- establish what the sensitivities of third parties are.
- carry out planning of the Information Security Management System (ISMS), establishing resources to implement, maintain and continuously improve the ISMS.

- develop an information security strategy.
- develop a security breach/incident management plan.
- establish security, technical and administrative measures capable of protecting personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication or any form of inappropriate or unlawful processing.
- defining a responsibility matrix.
- establish governance and accountability for security approach.
- establish the information provider(s) and data custodian.
- establish the recipient(s) of information.
- definition of data processing agent.
- definition of the data controller agent.
- definition of the data operator agent.
- establish the information reviewer(s).
- defining who will be responsible for delivering the information.
- definition of roles and functions in information management.
- establish planning for information delivery.
- definition of the information delivery cycle.
- define information exchange review criteria.
- criteria for providing information to third parties.
- establish logistics security.
- development of the security approach.
- determine the stages/phases for information exchange.
- define the process for exchanging information.
- establish agreements related to intellectual property.
- conduct security policy awareness.

4.3 **Guideline Set 3 - IMS Approach**

The third set of the Maturity Model deals with guidelines on the security approach. Therefore, they are guidelines that determine the application of the aspects to be addressed during information security. This set of guidelines represents 20.34% of the total guidelines (12 out of 59), and its guidelines are:

- establishment of the personal data protection impact report.
- planning, implementation and control of processes for the operation of the ISMS.
- document questions about the ISMS.
- establish the communication process.
- establish open schema standards.
- establish open data formats.
- treatment of information security risks.
- establish provision of a common data environment (CDE).
- start security approach.
- carry out internal and external communication for the ISMS.
- develop security risk mitigation measures.
- establish criteria for checking the availability of reference information and shared resources.

4.4 **Guideline Set 4 - IMS Quality Control**

Guideline Set 4 addresses quality control when IMS is addressed. In this set, guidelines that deal with recording the results of the sensitivity assessment and the application of the security screening process stand out. In total there are 11 guidelines, which represent 18.64% of the total. These guidelines are:

- record the result of the sensitivity assessment.
- establish delivery team risk register.
- manage accountability and responsibility for security.

- document residual and tolerated security risks.
- record the result of applying the security screening process.
- archive the project information model.
- monitoring and auditing.
- review of sensitivity assessment.
- security strategy review.
- review of the security management plan.
- carry out an assessment of risks relating to information security.

4.5 Guideline Set 5 – New Guidelines for IMS

Guideline Set 5 does not have any guidelines, it is a set made to group new guidelines taken from other standards and/or laws, as well as specific guidelines defined for a given project that are not listed in the previous sets. This set aims at a flow of continuous improvement in the IMS process.

4.6 Maturity Model Metrics

About metric for determining the degree of maturity, the reference established by the Organizational BIM Assessment – Version 1.03 (CICRP, 2013) was taken as a reference, where it was adjusted so that it could meet the needs of the model and the result presented in percentage terms. Therefore, the formula to determine the degree (in percentage) of the maturity model is:

$$GR = (QA/QP) * 100$$

Where: GR is Maturity Degree, QA is total number of guidelines met and QP is total number of possible guidelines.

In addition to presenting the degree of maturity in percentage terms, it is essential that it is classified, determining whether a company is at an initial, intermediate or advanced stage in relation to the adoption of BIMS within a specific set of guidelines and in general.

The definition of classifications is generally based on scoring systems but does not follow a specific rule. In view of this, the following classification of the degree of maturity is proposed: “Insufficient”: less than or equal to 40%; “Good Practices”: greater than 40% and less than or equal to 70%; “Best Practices”: greater than 70% and less than or equal to 90%; and “Excellence”: greater than 90%.

It is worth noting that for the general classification, not only the degree of maturity reached must also be considered, but also that the first two sets of guidelines cannot have a classification lower than the general classification. For example, the general classification cannot be “Good Practices” if the classification of set of guidelines 1 is “Insufficient” even if the degree of maturity achieved is between 40% and 70%.

5 Conclusion

The article highlights the complexity of the guidelines for Information Management and Security in architectural projects that use the Building Information Model (BIM). The research indicates that those involved are not prepared to protect project information, making an implementation strategy necessary.

The proposed Maturity Model does not solve all aspects of information security in the use of BIM, but it offers an organized path for the adoption of these aspects. It covers the initiation, planning and implementation stages of the IMS, including approach and quality control. The model allows the inclusion of new future guidelines and the maintenance of continuous quality flows.

The Maturity Model guidelines address a fundamental field of information security: legality. The structure of the model allows adjustments to these guidelines according to the need and complexity of the project, as well as the size of the organizations involved in the design phases.

By organizing the guidelines into sets, the model allows the office to choose which guidelines are most viable for initial adoption, progressing at each stage and as a whole. The choice of which guidelines to implement may be associated with the risks that the office is willing to take.

Although the study considered Brazilian legal aspects, the guidelines and proposed maturity model are adaptable and can be adopted in other scenarios and countries.

Acknowledgements

The authors thank CAPES and CNPQ for their financial support and the companies that contributed to the research with the documents.

References

ABNT, Brazilian Association of Technical Standards. ABNT NBR 31000. Risk Management - Guidelines. 2018.

ABNT – Brazilian Association of Technical Standards. ABNT NBR ISO/IEC 27005. Information technology - security techniques - information security risk management. 2019.

ABNT, Brazilian Association of Technical Standards. ABNT NBR 19650-1 Organization of information about construction work - Information management using building information modeling - Part 1: Concepts and principles. 2022a.

ABNT, Brazilian Association of Technical Standards. ABNT NBR 19650-2 Organization of information about building work - Information management using building information modeling - Part 2: Asset delivery phase. 2022b.

ABNT, Brazilian Association of Technical Standards. NBR ISO/IEC 27001. Information security, cybersecurity and privacy protection - information security management systems – requirements. 2022c.

AGUIAR, João et al. An overlapless incident management maturity model for multi-framework assessment (ITIL, COBIT, CMMI-SVC). Interdisciplinary Journal of Information, Knowledge, and Management, v. 13, p. 137-163, 2018.

ALENCAR, Gliner Dias. Primasia: a strategy for prioritizing and assessing information security maturity adaptable to the corporate environment. Federal University of Pernambuco, Post-graduation in Computer Science. Doctoral thesis. Recife. 2018.

ARIYANI, Sri; SUDARMA, Made. Implementation Of The ISO/IEC 27005 In Risk Security Analysis of Management Information System. J. Eng. Res. Appl, v. 6, n. 8, p. 1-6, 2016.

BIMe initiative. BIM Dictionary. 2023. In stock: <https://bimdictionary.com/>. Accessed December 22, 2023.

BRAZIL, LAW No. 13,709, of August 14, 2018. General Personal Data Protection Law (LGPD). Brasília, 2018.

BRUNNER, Michael et al. Risk management practices in information security: Exploring the status quo in the DACH region. Computers & Security, v. 92, p. 101776, 2020.

CICRP, Computer Integrated Construction Research Program. BIM Planning Guide for Facility Owners. Version 2.0, June, The Pennsylvania State University, University Park, PA, USA. 2013.

DA SILVA, Luiz Fernando Costa Pereira. Risk management in information technology as a critical success factor in information security management in federal public administration bodies: case study of the Brazilian Post and Telegraph Company-ECT. Ibero-American Journal of Information Science, v. 8, no. 1, p. 87-87, 2015.

DE OLIVEIRA, Paulo Leandro. Information security in small businesses. Technology Magazine, v. 33, no. 1, p. 7-11, 2012.

DE OLIVEIRA, Warlisson Costa. Implementation of information security policies at Pneucar based on ABNT NBR ISO/IEC 27005 guidelines. Monograph. BACHELOR OF SCIENCE IN COMPUTER SCIENCE. FIC - CARATINGA 2017.

FREDERICO, Guilherme F. Project Management for Supply Chains 4.0: A conceptual framework proposal based on PMBOK methodology. Operations Management Research, v. 14, n. 3-4, p. 434-450, 2021.

GRANJO, Paulo. The Concept of Risk: Janus reinvented. When the concept of “risk” becomes dangerous. Social Analysis, p. 1167-1179, 2006.

ISO – International Standard Organization. BS EN ISO 19650-4. Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 4: Information exchange. ed, 2022.

ISO – International Standard Organization. BS EN ISO 19650-5. Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 5: Security-minded approach to information management. ed, 2020.

LIMA, L.O.; CATAI, R.E.; SCHEER, S. Analysis of maturity models to measure the implementation of Building Information Modeling (BIM). Project Management & Technology. São Carlos, v16, n2, Feb. 2021. https://doi.org/10.11606/gtp.v16i2.167253.

MAGALHÃES, Cristiane Ramos. Macro BIM adoption: automation of a maturity assessment instrument with an emphasis on the notable publications component. Doctoral thesis Rio de Janeiro: UFRJ / FAU, 2022.

MANTHA, Bharadwaj; DE SOTO, Borja Garcia; KARRI, Ramesh. Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment. Sustainable Cities and Society, v. 66, p. 102682, 2021.

OLIVEIRA, Mírian. Knowledge management maturity models: quantity or quality? Information management in the era of cloud computing, 2011, Portugal., 2011.

PERES, Nilson Tinassi. A cybersecurity approach in electrical power systems. São Carlos School of Engineering. University of Sao Paulo. Monography. San Carlos. 2019.

PMI, Project Management Institute. Project management knowledge guide. PMBOK Guide. 7.ed. New York. Project Management Institute (PMI), 2022.

ROSA, Germano Mendes; TOLEDO, J. C. de. Risk management and the ISO 31000 standard: importance and impasses towards consensus. In: V Brazilian Congress of Production Engineering. 2015. p. 13.

SALGADO, M.S. Adoption of the Uses of the BIM Model as a strategy for inclusion in undergraduate education: case study. ENTAC2022. In: NATIONAL MEETING ON BUILT ENVIRONMENT TECHNOLOGY, 19., 2022, Canela. Anais... Porto Alegre: ANTAC, 2022. p. 1-10.

SARI, Endah Murtiana et al. Comparison of risk management analysis between PMBOK (2017), ISO (31000: 2018) AND AS/NZS (4360: 2009). PalArch's Journal of Archaeology of Egypt/Egyptology, v. 17, n. 10, p. 1439-1451, 2020.

SIMÃO, Victor Gomes et al. Comparative analysis between ABNT NBR ISO 9001:2015 and ABNT NBR ISO 31000:2009: the risk mentality in quality management systems. Electronic Magazine Systems & Management Volume 14, Number 3, 2019, pp. 310-322.

TAKAGI, Nilton; VARAJÃO, João. Success management and the project management body of knowledge (PMBOK): An integrated perspective. INTERNATIONAL RESEARCH WORKSHOP ON IT PROJECT MANAGEMENT (IRWITPM). Association for Information Systems. 2020.

TURK, Žiga; SONKOR, Muammer Semih; KLINC, Robert. Cybersecurity assessment of BIM/CDE design environment using cyber assessment framework. Journal of Civil Engineering and Management, v. 28, n. 5, p. 349–364-349–364, 2022.

UKBIM Alliance. Information management according to BS EN ISO 19650, Guidance Part 1: Concepts. UKBIM Alliance. Londres, Reino Unido. 2019.

VARGAS, Danieli Braun; CAMPOS, Lucila Maria de Souza. Risk Management: A Parallel Between ISO 31000 (2018) and the PMBOK Guide (2017). Proceedings of the International Conference on Industrial Engineering and Operations Management Istanbul, Turkey, IEOM Society International, PAG 1474-14/83. March 7-10, 2022.

WEF, World Economic Forum. Global Cybersecurity Outlook 2024. Insight Report. Janeiro 2024.

YILMAZ, Gökçen; AKÇAMETE GÜNGÖR, Aslı; DEMIRÖRS, Onur. A review on capability and maturity models of building ınformation modelling. LC3 2017: Volume I – Proceedings of the Joint Conference on Computing in Constructions, Heraklion, Greece, 2017.