2024 EC³
2024 European Conference on Computing in Construction
Chania, Crete, Greece
July 15-17, 2024

RECOMMENDATIONS FOR PRIVATE AND SECURE CDE BASED BIM COLLABORATION

Anja Brelih and Robert Klinc
University of Ljubljana, Faculty of Civil and Geodetic Engineering

Abstract

The digitalization of the construction industry through BIM and CDE raises security and privacy concerns as sensitive data is stored in cloud environments. It is critical to address these concerns related to CDE and provide guidelines and recommendations for users. The paper provides an overview of security and privacy mechanisms at multiple levels that should be implemented in BIM, including data and network security, identity and access management, physical security, and compliance with standards. We examine ISO 19650-5 and recommend a direction to improve BIM related guidelines in order to help users identify potential concerns in their chosen cloud environment.

Introduction

A Common Data Environment (CDE) is a cloud computing infrastructure that serves as a shared digital workspace for project teams to collaborate on Building Information Modelling (BIM). CDE is becoming increasingly important in the construction industry as it provides a centralised repository for managing project information and improving communication between stakeholders (see Figure 1).

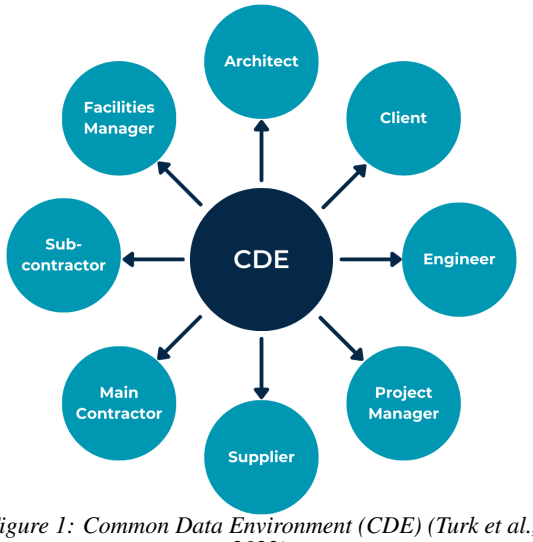

Figure 1: Common Data Environment (CDE) (Turk et al., 2022).

CDEs allow project teams to access and share BIM models and other project data in real time. This can help to improve coordination, reduce errors and shorten project timelines.

Cloud computing is a ubiquitous and rapidly growing computing paradigm that provides users with access to data and applications. Two main models are private and public clouds. In the private cloud, ownership and management of the cloud is in the hands of the organisation providing the applications and access to the resources is not open to everyone as in the public cloud. Cloud computing offers different service models, which are a specific, pre-prepared combination of information technology (IT) resources offered by a cloud service provider and relate to the way in which it offers a service to users. The three main service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) (Manvi and Shyam, 2021). Shared digital workspaces used in the construction industry are typically offered as a SaaS model, where users do not manage and control the cloud infrastructure, but simply utilise cloud software solutions. In commercial CDE environments, providers are responsible for managing the SaaS model and providing upgrades, maintenance and security.

The exponential growth of cloud computing brings numerous benefits, but also a number of security concerns that must be properly understood and addressed in order to successfully deploy solutions in the cloud environment (Sun, 2018). Computing and data in the cloud are associated with various security risks, including loss of governance, isolation failures, data protection, service availability, compliance and legal risks, authentication and authorisation, etc. Cloud computing security refers to maintaining the confidentiality, integrity and availability of data stored in the cloud. Cloud security requirements include robust security, trust, safety, monitoring and governance (Pavithra et al., 2019). These requirements can be directly applied to the security and privacy requirements for CDE environments in the cloud.

This paper provides recommendations for secure and private CDE based BIM collaboration environments. The second chapter provides an overview of the levels of security and privacy mechanisms that need to be implemented in these environments. The third chapter provides an overview of the ISO 19650-5 standard for Security-minded approach to information management. The fourth chapter gives an overview of the BIM Execution Plan with guidelines for users. Chapter five proposes guidelines for users of BIM and CDE environments. The last two chapters provide a discussion and a conclusion.

Cloud Computing Security and Privacy Mechanisms

As the use of BIM and CDE environments increases, so does the number of security risks and threats that need to be addressed and successfully mitigated. These mechanisms are crucial to ensure the aspects of data security, i.e. confidentiality, integrity and availability of data in the cloud, and provide protection against unauthorised access, data loss and cybersecurity threats (Manvi and Shyam, 2021).

The security and privacy mechanisms of cloud computing must be considered on multiple levels in order to provide users with a comprehensive and trustworthy service. In this paper, the mechanisms are categorised into data security, network security, identity and access management, physical security and standards compliance (see Figure 2).

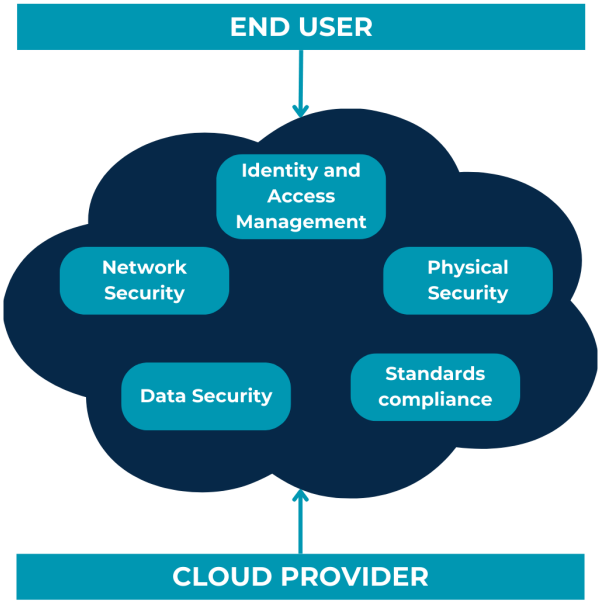

Figure 2: Cloud computing security levels.

Data security

Data security in the cloud differs from traditional data security due to its special storage architecture. Cloud computing generally uses distributed storage. Ownership and control of the data are separated. Users have ownership, but control lies with the cloud service providers. Current data protection in the cloud mainly focuses on data storage, transmission and access authentication and is mostly implemented using cryptography (Xu et al., 2019). By default, data is written in a human-readable format known as plain text, which is vulnerable to unauthorised and potentially malicious access when transmitted over a network. Cloud encryption converts the data into a unreadable format to ensure confidentiality and even data integrity. It is a service offered by cloud storage providers that uses encryption algorithms (Manvi and Shyam, 2021) to convert data into a protected and unreadable form, rendering the encrypted data unusable without knowledge of the key. The encryption process can be carried out using various techniques such as symmetric and asymmetric encryption. In symmetric cryptography, the same key is used for encryption and decryption, as opposed to asymmetric cryptography, where a pair of public and private keys is used for encryption and decryption. An important aspect of data security during transmission or remote storage is maintaining the integrity of the data. To this end, hash functions can be used to ensure that the data received is identical to the original.

Network security

Network security includes the protection of data transmitted over networks such as the internet, the protection of systems and data from network attacks and the protection of the network components themselves. A cloud service provider can ensure the security of the network environment for users by offering cloud services that ensure encryption of data traffic, network monitoring, analysis and control of data traffic, virtual private networks (VPN), firewalls and secure network services (CSA, 2012).

Identity and access management

Cloud computing has had a significant impact on identity and access management (IAM). In both public and private clouds, two parties must work together to manage IAM without compromising security. Cloud computing requires significant changes to the methods used to manage IAM for internal systems. The most important difference is the relationship between the cloud provider and the cloud user. IAM cannot be managed by just one or the other, so a mutually agreed understanding of responsibilities and a secure relationship for managing identity, authorisation and access (CSA, 2021a).

Physical security

Physical security mechanisms include various levels of control and measures to control access and activities. The cloud service provider, who has control over the physical infrastructure, is responsible for ensuring this level of security. It must ensure security against physical attacks as well as natural disasters and power outages. Every aspect of the data center, from location and accessibility to power density and redundancy, must be designed to ensure its security, resilience and efficiency. However, incidents can still occur, whether through a natural disaster, a physical attack or a cyber-attack. It is therefore important that cloud providers are prepared for such situations and have disaster recovery mechanisms in place to ensure business continuity.

Shared responsibility model

The Cloud Security Alliance (CSA, 2021b) identifies the so-called shared responsibility model, which is directly related to two recommendations for security in cloud applications:

1. Cloud providers should clearly document their inter-

nal security controls and characteristics of customers so that the cloud user can make an informed decision. Providers should also properly design and implement these controls.

2. Cloud users should create a responsibility matrix for each individual project to document who implements which controls and how.

The shared responsibility model states that when dealing with cloud computing technology, there are two parties involved who are responsible for implementing and managing different parts of the stack. Building and maintaining trust is critical to this relationship.
Cerić et al. (2021) provide a detailed analysis of the existing literature on trust in megaprojects. The authors identify three different approaches to the study of trust. Namely the psychological, the sociological and the economic. The psychological approach focuses on the dynamics of trust dynamics, while the sociological approach examines trust within groups and organisations. The economic approach, on the other hand, analyses how trust influences economic interactions. The key factors that contribute to trust in such projects are effective communication, transparency, reputation and strong relationships.
Trust is an important aspect of construction projects and it also applies to the collaboration of all parties using or providing BIM and CDE cloud environments. A trusting relationship is important for the successful implementation of these solutions so that the parties involved regulate and respect the activities of the shared responsibility model.
The basis for establishing and maintaining trust in BIM and CDE cloud computing environments between the parties involved in the projects must be clearly defined in the standards and project documentation. The ISO 19650 series of standards focuses on the management of information throughout the lifecycle of a built asset using BIM (BSI, 2023). The clear instructions for managing the security and privacy of the information should also be part of the project documentation, e.g. the BIM Execution Plan.

Standards compliance

In addition to the ISO 19650 series of standards that apply to information management using building information modelling, CDE environments must also comply with the standards that apply to cloud computing. Cloud computing has attracted increasing attention due to security concerns and standardised validation and certification is required to assess cloud security. IT security standards are a structured approach to IT security based on measurable indicators represented by controls (e.g. a checklist) or general but clear requirements (e.g. clauses or principles) Di Giulio et al. (2017). The ISO/IEC 27000 family is the most widely used standard for information security management systems (ISO, 2023). It contains guidelines for the establishment, implementation, maintenance and continuous improvement of an information security management system. The ISO/IEC 27001 standard provides instructions for the establishment, implementation, maintenance, and continuous improvement of an information security management system. Compliance with the ISO/IEC 27001 standard means that the organization or company has established a system to manage risks associated with the security of data held or processed by the company, and that this system complies with all the best practices and principles described in this international standard (ISO, 2022a). In addition to compliance with the ISO/IEC 27001 standard, consideration should also be given to compliance with the ISO/IEC 27017 standard, additional controls with implementation guidance that specifically relate to cloud services (ISO, 2015). It is intended to complement the recommendations of the ISO/IEC 27002 (ISO, 2022b) standard and various other standards in the ISO/IEC 27000 family, such as ISO/IEC 27018 on the privacy implications of cloud computing (ISO, 2019) and ISO/IEC 27031 on business continuity (ISO, 2011). The ISO/IEC 27018 standard focuses on the protection of personally identifiable information (PII) in public clouds that serve as PII processors (ISO, 2022a). Compliance with these standards demonstrates that an organisation has implemented a robust security management system and is essential for ensuring the security of data and information in CDE environments.

ISO 19650-5 standard

The fifth part of the ISO 19650 *"Organization and digitization of information about buildings and civil engineering works, including building information modelling - Information management using building information modelling"* series of standards refers to *"Security-minded approach to information management"*. This part of the standard outlines the requirements for the management of information security in BIM projects (ISO, 2020).

ISO 19650-5 provides a framework to help organisations assess security vulnerabilities in BIM and implement controls to mitigate risk. It recognises that the use of BIM and information management technologies introduces new vulnerabilities that need to be proactively addressed. The standard promotes a risk-based approach to security that can be applied across the organisation. It is designed to help organisations protect sensitive information and ensure the security and resilience of assets, products and services in the built environment (ISO, 2020).

The main part of the standard is divided into six parts, which establish the need for a security-minded approach and provide guidance on developing a security strategy, a management plan with a plan for dealing with security breaches and outline guidance for working with appointed parties. In addition, the standard also contains annexes with further information on (1) the security context, (2) the types of personnel, physical and technical security controls and the management of information security, (3) the assessment in relation to the provision of information to third parties and (4) information sharing agreements.

BIM Execution Plan

The BIM Execution Plan (BEP) is a comprehensive document that helps project stakeholders move forward with clear roles and expectations. It is an essential element that must be created before a construction project begins, and it is a powerful tool for project ownership that drives work through the various design and construction phases. Information that should be included in the BEP includes (1) how the data in the BIM files will be created, managed, documented and shared, (2) elements such as agreed roles and responsibilities within the BIM process, (3) a strategy for key deliverables and a guide to key project milestones, and (4) practical working procedure details. The BEP is a guiding document that helps the different team members to identify and execute the various phases of the project. It can help to present a clear plan with goals and objectives for each step (Ramage, 2022).

Ramage (2022) identifies seven elements of a good BEP: (1) clearly defined roles and responsibilities of each team and organisation, (2) strategic planning, definition of BIM scope and defined key deliverables, (3) project milestones and a realistic timeline, (4) project objectives, (5) model quality control procedures, (6) project reference information with key project contacts, and (7) working procedures that include file naming conventions, construction tolerance expectations, the project approach to annotation, technology infrastructure needs (including hardware and software used), BIM iteration management and data transfer management.

In the third version of the BIM Project Execution Planning Guide (Messner et al., 2021), the authors offer a structured procedure for the creation and implementation of the BEP. The five steps within the procedure include:

1. defining the goals for the implementation of BIM,
2. identifying high value model uses during the project planning, design, construction and operational phases,
3. designing the BIM execution process through the creation of process maps
4. defining the information deliverables, and
5. the development of infrastructure in the form of contracts, communication procedures, technology and quality control to support implementation.

These steps describe the general application of BEP in a project. While steps 1 to 4 mainly contain guidelines for BIM implementation and project-specific organisation, step 5 refers to the technology used. It is essential that this step includes the definition of the required level of security and privacy required, the technologies used and the responsibilities. The requirements for the technological aspect must also be the subject of the contract between the provider and the customer.

The BEP also provides guidelines for defining the infrastructure needs, including hardware, software, networks and modelling content for the project that will be used for BIM. It identifies fourteen specific categories to support the BIM project execution process.

1. **BIM Project Execution Plan Overiview**: review of the plan based on the categories developed after analysing the documents listed below, reviewing current execution plans, discussing the issues with industry experts and revising through a comprehensive review by various industry organisations.
2. **Project Information**: contains basic project information that can be useful for current and future projects. It can be used to introduce new members to the project and help others reviewing the plan to understand the project.
3. **Key Project Contacts**: contains the contacts of the owner, the planners, the consultants, the main contractors, the subcontractors, the manufacturers and the suppliers of the project.
4. **Project Goals / BM Uses**: the plan should include a clear list of BIM goals, the BIM Use Analysis Worksheet and specific information on the selected BIM Uses selected.
5. **Organisational roles / Staffing**: for each selected BIM Use, the team must specify which organisation(s) will staff and perform this Use. This includes the number of staff by job title required to perform the BIM Use, the estimated working hours, the main location where the use will be performed and the lead organisational contact for this Use.
6. **BIM Process Design**: the plan should include the overview map of BIM Uses, a detailed map of each BIM Use and a description of the elements on each map.
7. **BIM Information Exchanges**: the team should document the information exchange created as part of the planning process in the BIM Project Execution Plan. The information exchange illustrates the model elements by discipline, level of detail and any specific attributes that are important to the project.
8. **BIM and Facility Data Requirements**: project owners can have very specific BIM requirements. It is important that the plan documents the BIM requirements in the format specified by the owner.
9. **Collaboration Procedures**: the team must develop its procedures for electronic and active collaboration. This includes the management of models and standard meeting actions and agendas.

10. **Quality Control**: procedures must be defined and implemented to ensure model quality at each project stage and prior to information exchange. Each BIM created during the life cycle of the project must be pre-planned taking into account the model content, the level of detail, the format and the party responsible for the updates and distribution of the model and data to various parties.
11. **Technological Infrastructure Needs**: the team should determine the requirements for hardware, software platforms, software licences, networks and modelling content for the project.
12. **Model Structure**: the team must determine the methods that will ensure the accuracy and scope of the model. Once the planning team has agreed on the collaboration methods and technology infrastructure needs, it should reach a consensus on how the model will be created, organised, communicated and controlled.
13. **Project Deliverables**: the project team should consider what deliverables are required by the project owner. Deliverables should take into account the project phase, the format of the due date and any other specific information about the deliverable.
14. **Delivery Strategy / Contract**: When implementing BIM in a project, attention should be paid to the delivery and contract methods before the project begins.

Guidelines for users of BIM and CDE environments

As BIM and CDE environments contain sensitive information about construction projects, especially financial information, intellectual property and personal data. It is therefore important for providers and users of these environments to take measures to protect the security and privacy of this data.
Users should be aware that BIM and CDE environments are based on new cloud technologies. It is important to verify the provider's compliance with industry standards. By demanding compliance with the standards, users can help to ensure that providers adhere to the rules and standards and clearly communicate these to their users.
Users need clear guidelines on how to use cloud solutions correctly in their projects. Based on current standards and guidelines, users should pay particular attention to the following list that can help protect the security and privacy of sensitive data in BIM and CDE environments:

- **Make a conscious decision about the data you share**. Only share the data that is necessary for the project. Ask questions about the security of the environment snd consult security experts.
- **Assign a data security officer for the project**. This person should be responsible for monitoring the security of the data.
- **Research the provider's security and privacy mechanisms**. Before deciding on a cloud-based CDE, find out about the provider's security practises. Look for providers that are certified to industry standards.
- **Request documentation**. Ask for documentation from the provider outlining security practises.
- **Negotiate the terms**. Include the security requirements and consequences in your contract with the provider.

Discussion

ISO 19650-5 is a valuable standard that provides a framework for information security in information management with BIM. However, the standard could be improved by focusing more on cybersecurity, providing more clarity and consistency, and offering more detailed guidance on how to implement security measures. In particular, the standard should address cybersecurity risks associated with cloud-based technologies, provide clearer and more specific guidance, and offer more specific recommendations for policies, procedures and tools. By improving the standard, organisations using BIM and CDE and providers can better protect sensitive information.
The BIM Execution Plan outlines an important procedure for BIM implementation in construction projects. However, it only focuses on the specifics of construction projects and does not take into account the information security and privacy required when using CDE cloud environments. An important aspect that is ignored is the use of suitable providers that can guarantee an appropriate level of security and meet the required standards for cloud environments.
The shared responsibility model used in cloud environments should be included in the BEP, as it clearly defines which aspects both the provider and the user must guarantee and take into account. It would also be necessary to include in the BEP specific cloud computing technological aspects that are necessary to ensure security and privacy. Experts in the construction field do not focus on information security aspects. Therefore, collaboration with relevant experts in the field of information security and privacy is crucial, as construction projects involve a large amount of often sensitive information.

Conclusion

The use of BIM and CDE environments in construction projects is becoming increasingly common and serves as an important tool for more efficient project management and resource management. With the use of these cloud technologies, it is also of paramount importance to ensure robust security and privacy mechanisms to ensure the confidentiality, integrity and availability of data.
In this paper, we have explored the key aspects of ensuring security and privacy in cloud environments where the user does not have full control over their data in public clouds.

A review of the ISO 19650-5 standard, which focuses on the security-minded approach to information management, has shown that it does not provide adequate guidelines for users and providers of CDE environments to follow when using them. Even the BEP, which is otherwise a powerful tool for planning the specifics of a construction project, does not provide security guidelines.

For safe implementation of BIM and CDE cloud environments in construction projects, it is critical that all stakeholders are aware of the dangers that can result from inadequate security controls. A shared responsibility model should be included in the BEP guidelines, clearly stating which aspects of security must be ensured by both the provider and the user. Users must be aware of the security threats and select a suitable provider of a CDE environment also on the basis of security aspects. In the guidelines for users of CDE and BIM environments, we provide advice that can help users choose the right provider for their security requirements.

A transparent and confidential relationship between the provider and the user of BIM and CDE environments is central to the implementation of these environments. Providers must provide secure solutions, but there is an incentive for users to ensure that appropriate standards are maintained and security aspects are properly disclosed to users so that the services can be trusted.

Acknowledgments

This research was supported by the Slovenian Research Agency under the Young Researcher funding program and research program E-construction (E-Gradbeništvo: P2-0210).

References

BSI (2023). ISO 19650 Building Information Modelling (BIM). https://www.bsigroup.com/en-GB/iso-19650-BIM/ [Accessed: 2023-11-21].

Cerić, A., Vukomanović, M., Ivić, I., and Kolarić, S. (2021). Trust in megaprojects: A comprehensive literature review of research trends. International Journal of Project Management, 39(4):325–338.

CSA (2012). SecaaS Category 10 // Network Security Implementation Guidance. https://cloudsecurityalliance.org/artifacts/secaas-category-10-network-security-implementation-guidance/ [Accessed: 2023-11-21].

CSA (2021a). Security Guidance for Cloud Computing. https://cloudsecurityalliance.org/research/guidance/ [Accessed: 2023-11-20].

CSA (2021b). Security Guidance for Cloud Computing. https://cloudsecurityalliance.org/research/guidance/ [Accessed: 2023-11-20].

Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R. H., and Bashir, M. N. (2017). Cloud standards in comparison: Are new security frameworks improving cloud security? In 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), pages 50–57.

ISO (2011). ISO/IEC 27031:2011 information technology, security techniques, guidelines for information and communication technology readiness for business continuity. https://www.iso.org/standard/44374.html [Accessed: 2024-03-24].

ISO (2015). ISO/IEC 27017:2015 information technology, security techniques, code of practice for information security controls based on iso/iec 27002 for cloud services. https://www.iso.org/standard/43757.html [Accessed: 2024-03-24].

ISO (2019). ISO/IEC 27018:2019 information technology, security techniques, code of practice for protection of personally identifiable information (pii) in public clouds acting as pii processors. https://www.iso.org/standard/76559.html [Accessed: 2024-03-24].

ISO (2020). ISO 19650-5:2020. https://www.iso.org/standard/74206.html [Accessed: 2023-12-06].

ISO (2022a). ISO/IEC 27001:2022 information security, cybersecurity and privacy protection, information security management systems, requirements. https://www.iso.org/standard/27001 [Accessed: 2024-03-24].

ISO (2022b). ISO/IEC 27002:2022 information security, cybersecurity and privacy protection, information security controls. https://www.iso.org/standard/75652.html [Accessed: 2024-03-24].

ISO (2023). ISO/IEC 27000 family. https://www.iso.org/standard/iso-iec-27000-family/ [Accessed: 2023-12-04].

Manvi, S. S. and Shyam, G. K. (2021). Cloud computing: concepts and technologies. CRC Press, Taylor Francis, 1st ed. edition.

Messner, J., Anumba, C., Dubler, C., Goodman, S., Kasprzak, C., Kreider, R., Leicht, R., Saluja, C., Zikic, N., and Bhawani, S. (2021). BIM Project Execution Planning Guide, volume 3.0. Computer Integrated Construction Program, Penn State.

Pavithra, S., Ramya, S., and Prathibha, S. (2019). A survey on cloud security issues and blockchain. In 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), pages 136–140.

Ramage, M. (2022). Trimble Contruction: What is a BIM Execution Plan and what should it include? https://constructible.trimble.com/construction-industry/what-is-a-bim-execution-plan-and-what-should-it-include [Accessed: 2024-01-09].

Sun, X. (2018). Critical security issues in cloud computing: A survey. In 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), pages 216–221.

Turk, Ž., Sonkor, M. S., and Klinc, R. (2022). Cybersecurity assessment of BIM/CDE design environment using cyber assessment framework. Journal of Civil Engineering and Management, 28(5):349–364.

Xu, H., Cao, J., Zhang, J., Gong, L., and Gu, Z. (2019). A survey: Cloud data security based on blockchain technology. In 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC), pages 618–624.