www.itcon.org - Journal of Information Technology in Construction - ISSN 1874-4753

BUILDING DIGITAL TRUST IN CDE-BASED BIM WORKFLOWS: KEY STRATEGIES

SUBMITTED: January 2025
REVISED: March 2025
PUBLISHED: April 2025
EDITOR: Robert Amor
DOI: 10.36680/j.itcon.2025.022

Anja Brelih, PhD candidate,
University of Ljubljana, Faculty of Civil and Geodetic Engineering, Chair of Construction Management
ORCID: https://orcid.org/0009-0005-5951-5628
anja.brelih@fgg.uni-lj.si

Robert Klinc, PhD,
University of Ljubljana, Faculty of Civil and Geodetic Engineering, Chair of Construction Management
ORCID: https://orcid.org/0000-0002-0027-420X
robert.klinc@fgg.uni-lj.si

SUMMARY: *The adoption of Building Information Modeling (BIM) and Common Data Environments (CDE) in construction has increased the need for robust security and privacy frameworks, especially as these platforms increasingly leverage cloud-based technologies. This paper examines the mechanisms required to protect sensitive project data in BIM and CDE environments, including financial data, intellectual property and personal data. It emphasises the crucial role of trust — cognition-based, affect-based and system-based — in promoting safe and collaborative workflows and explores the concept of digital trust as a foundation for reliable partnerships in cloud-based construction environments. A critical analysis of ISO 19650-5 identifies significant gaps in addressing the complexity of cyber security and argues for explicit technical guidelines to protect against cyber threats. It also highlights inconsistencies in the transparency of security practises of widely used BIM and CDE providers and emphasises the need for improved disclosure to increase user trust. To provide a structured approach to threat mitigation, we introduce the Process for Attack Simulation and Threat Analysis (PASTA) framework and demonstrate its applicability in aligning business and technical risks within BIM and CDE workflows. In addition, this paper proposes to integrate security requirements into the BIM Execution Plan (BEP) to improve alignment across all project phases. Recommendations are provided for providers and users to establish a trust-based approach to information security that ensures compliance with standards and promotes the resilience of construction workflows. This paper highlights practical pathways to enhance the security of BIM and CDE implementations, focusing on robust technical safeguards and the role of trust in collaborative projects.*

KEYWORDS: *Building Information Modeling (BIM), Common Data Environment (CDE), digital trust, security, PASTA methodology, standardization.*

REFERENCE: *Anja Brelih & Robert Klinc (2025). Building digital trust in CDE-based BIM workflows: Key strategies. Journal of Information Technology in Construction (ITcon), Vol. 30, pg. 524-543, DOI: 10.36680/j.itcon.2025.022*

1. INTRODUCTION

The construction industry has always relied on efficient communication, as the successful exchange of information is crucial for turning plans into reality. As Kalay (1999) noted, the architecture, engineering and construction (AEC) industry also differs from other disciplines and fields in which a single expert can perform a task completely independently. An individual in the construction industry represents and performs only a part of a coherent whole and can rarely perform a task completely independently. This also means that a single task cannot be carried out without the contribution of all the experts in the areas involved. The fragmentation of knowledge and expertise in the construction industry has created a situation in which no individual is able to complete a construction project without the co-operation of experts from the fields of architecture, civil engineering, mechanical engineering, project management, financial consultancy, law and others. Dolla et al. (2024) pointed out that effective communication between stakeholders to optimise the flow of information in projects is one of the most important aspects of project execution.

The increasing use of information and communication technologies (ICT) has revolutionised the way construction projects are planned, designed and executed. These technologies have facilitated the seamless exchange of information, allowing project stakeholders to collaborate remotely and access project data in real time. In recent years, developments have paved the way for collaboration based on Building Information Modeling (BIM), in which various aspects of a project are combined into a single, shared model. The BIM approach is becoming increasingly important in the construction industry as it connects project participants and creates a transparent workflow. A key component of BIM-based digital transformation is the Common Data Environment (CDE). CDE, a cloud computing infrastructure, is a shared centralised digital workspace that enables project teams to collaborate on BIM models and other project data.

While technological advancements have undoubtedly streamlined communication processes, they have also brought new challenges, particularly in the area of cyber security. With the increasing adoption of BIM and CDE, the need for security and privacy management is becoming increasingly important. These environments contain sensitive information about construction projects, including financial information, intellectual property and personal data. Therefore, it is important that CDE providers and users have a clear understanding of the security and privacy mechanisms required and used to protect this data. As it was observed by Klinc et al. (2010), the construction industry must deal with the changes brought by newly developed IT ecosystems and cope with the shift from self-integration of technology and software investments based on ownership to those based on subscriptions (assembled, managed and maintained by an external provider). This change is also closely linked to relationships with (outsourced) IT partners and security, which ultimately affects mutual trust. As cloud computing is a shared technology model where different enitities are responsible for implementing and managing different parts of the stack, the responsibility for security is also shared between all parties involved.

Mahamadu et al. (2013) recognized the problem of integrating BIM and cloud computing as early as 2013. They identify four levels of protective solutions that can be used to overcome these challenges: Infrastructure, Information, Contract and Level of Trust. They propose the development of a suitable risk assessment model for evaluating BIM cloud requirements, as different levels of risk are associated with different cloud models.

Das et al. (2021) discuss the importance of BIM security and the potential benefits of using encryption and blockchain technology to improve security. The authors identify seven components that they use to define three levels of BIM security. They also review existing technologies to promote cybersecurity, including encryption protocols, distributed database technology and blockchain technology. Based on this review, the authors propose two conceptual frameworks: (1) a framework based on encryption strategies to securely store and distribute BIM and (2) a framework based on blockchain to record BIM changes in a tamper-proof ledger for the untrusted environment of construction projects.

Turk et al. (2022) discuss the applicability of the Cyber Assessment Framework (CAF) to the BIM and CDE design environment and identify a number of cybersecurity risks that should be considered when using BIM and CDE. They also provide recommendations for mitigating these risks, including (1) implementing a risk management process to identify, assess, and manage cybersecurity risks, (2) implementing technical controls such as access controls, encryption, and firewalls, and (3) implementing organizational controls such as security awareness training and incident response procedures.

Despite the digital transformation, the fundamental importance of trust in construction communication remains unchanged. Trust is the foundation on which successful collaboration is built. It promotes open dialogue, transparency and mutual respect - important elements for minimising risks and ensuring project success. In the context of cyber security, trust is even more important as it supports the secure exchange of sensitive information. In the age of digitalisation, it is important to build a digital trust, which is by definition, given by WEF (2022), an »*individuals' expectation that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values*«.

This paper explores the critical role of digital trust in securing CDE-based BIM workflows in the construction sector. It emphasises the growing reliance on cloud-based technologies and examines the interplay of security, privacy and trust in collaborative digital environments. We start with points of departure forcusing on cloud computing, the shared responsibility model in cloud environments, trust in construction projects and digital trust. We also introduce security and privacy mechanisms used in cloud environments and present the PASTA threat model. Next, we explore different types of trust (cognition, affect and system-based) that exist in construction projects and relate them to the ISO 19650 series standards, the BIM Execution Plan and the security and privacy mechanisms used by BIM and CDE providers. We end this part with the application of the PASTA threat model to CDE-based BIM workflows. In the the end, we discuss the results and the paper concludes with section five, where we present the main findings and provide recommendations to strengthen digital trust and resilience in construction workflows.

2. POINTS OF DEPARTURE

2.1 Cloud computing

Cloud computing has become an integral part of modern construction projects, especially with the introduction of BIM and CDE. These systems facilitate collaboration and efficiency, but also bring complex challenges in ensuring security and privacy.

Cloud computing is a ubiquitous and rapidly growing computing paradigm that provides users with access to data and applications. CDE environments can be implemented as on-premise or off-premise infrastructure. These implementations can correspond to different cloud deployment models based on location, ownership and overall accessibility. Two main models are private and public clouds. In the private cloud, ownership and management of the cloud is in the hands of the company 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 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 & 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 use 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 with it numerous benefits, but also a number of security concerns that must be properly understood and addressed in order to successfully adopt solutions in the cloud environment (Sun, 2018). Computing and data in the cloud are associated with several security risks, including loss of governance, isolation failures, data protection, service availability, compliance and legal risks, authentication and authorization 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, assurance, 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.

2.2 Shared Responsibility Model

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

1. Cloud providers should clearly document their internal security controls and the 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 describes how security in the cloud is divided between providers and users, with the division varying depending on the type of service. Providers secure the core infrastructure for IaaS, the platform for PaaS and most layers for SaaS, while users manage application-specific settings and access controls. The spectrum shown in Figure 1 illustrates how the responsibility for security in cloud services decreases for the user with less customizable service models and highlights the importance of clear roles for effective security (Rajesh et al., 2024).

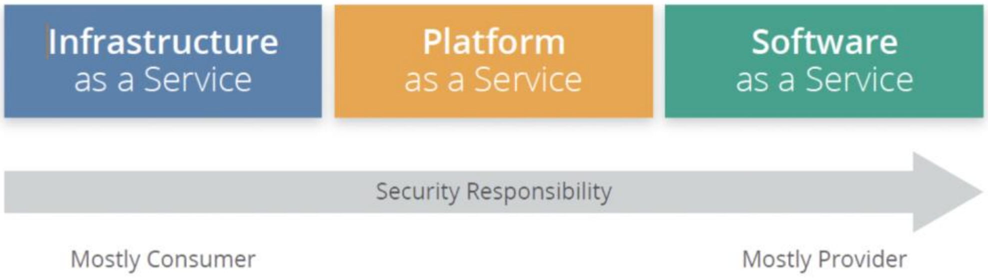


Figure 1: Spectrum of security responsibilities between user and provider (CSA, 2024).

Cloud computing technologies such as BIM and CDE involve two parties that are responsible for implementing and managing different parts of the stack. Building and maintaining trust is critical to this relationship.

2.3 Trust in construction projects

Trust is crucial in construction project management. While it is hard to build and easily broken, rebuilding trust is even harder (Cerić, 2016). The key factors that contribute to trust in such projects are effective communication, transparency, reputation and strong relationships (Cerić et al., 2021)

Trust is an important aspect of construction projects and 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 project documentation.

Wong et al. (2008) identify three types of trust elements in construction projects:

- **Cognition-based trust** – i.e. knowledge about the partners and their reliability. It is based on the belief in the reliability and competence of the parties involved. This includes assessing the track record and competence of partners and stakeholders in delivering secure and effective solutions in BIM and CDE environments.
- **Affect-based trust** – i.e. the way a person connects with others and invests in mutual relationships. It arises from emotional bonds and interpersonal relationships. It reflects the confidence that parties will act in good faith and prioritize project success, especially in digital environments where collaboration occurs.
- **System-based trust** – i.e. contractual, formal, and procedural agreements. It is created through formal structures such as contracts, standards and compliance mechanisms. It ensures that predefined protocols and legal agreements are in place to ensure secure and transparent operations.

All three forms of trust are of almost equal importance, since the three facets of trust co-exist and are mutually dependent. A system is only as good as its weakest point, hence a trust building project manager must be able to install robust system, care for the stakeholders and team members (Wong et al., 2008).

2.4 Digital trust

Digital trust is the cornerstone for fostering reliable collaboration in CDE-based BIM workflows, where shared digital environments require the alignment of technological safeguards and interpersonal relationships.

As defined by the World Economic Forum (WEF), digital trust encompasses the confidence of stakeholders that digital technologies and the organisations that use them will protect their interests and uphold societal values (WEF, 2022). This concept goes beyond the technical parameters and builds a bridge between people's expectations and the operational realities of cloud-based BIM implementations.

In the construction sector, digital trust is a crucial factor for the integration of advanced digital solutions without jeopardising security or privacy. The shared responsibility model inherent in cloud computing emphasises the importance of clearly delineated roles and responsibilities between stakeholders (CSA, 2021). Digital trust in CDE-based BIM workflows is supported by frameworks such as the ISO 19650 standard and the BIM Execution Plan, which set out principles for transparency, accountability and secure collaboration. These frameworks address the specific challenges that cloud-based environments bring while promoting trust between all stakeholders.

Digital trust not only supports seamless workflows, but also strengthens the collective ability to address cybersecurity threats and ensure compliance. In this way, it bridges the gap between traditional trust in construction projects and the modern requirements of secure, cloud-based digital collaboration.

2.5 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. The use of mechanisms is crucial to ensure the aspects of data security, i.e. confidentiality, integrity and availability of data in the cloud, and provides protection against unauthorized access, data loss and cybersecurity threats (Manvi & Shyam, 2021):

- **Confidentiality** is the prevention of intentional or unintentional unauthorized disclosure of content.
- **Integrity** is the assurance that the content has not been intentionally or unexpectedly altered.
- **Availability** ensures that the service is available when needed and allows authorized users to access it.

In CDE environments, where the user typically uses the SaaS service model, the provider is responsible for almost all security, as the user can only access and manage the application and has no control over how the application works (CSA, 2021). With cloud computing, user data is confidential, but external and virtual data storage, multiple tenants, big data and other technologies can appear very insecure due to security vulnerabilities and lack of privacy. Therefore, cloud computing providers need to be more incentivized to address security issues and provide more reliable solutions to make it more useful and widely available to users (Bamasoud et al., 2021).

The security and privacy mechanisms of cloud computing need to be considered on multiple levels to provide a comprehensive and trustworthy service. We categorized the mechanisms into information security, physical security, and standards compliance.

2.5.1 Information security

The responsibility model shown in Figure 2 for managing the various layers of cloud environments differs depending on the service model used. The security mechanisms are considered at each layer and are managed by the user or provider of the cloud service. The CDE environment in the on-premise implementation is managed by the user, who is the owner of the infrastructure. In an off-premise implementation, the responsibilities for security are divided between the user and the service provider, depending on the type of service model. With IaaS, the cloud provider secures the basic infrastructure, while the customer is responsible for securing everything they build on top of it. With PaaS, the provider secures the platform and the customer manages their applications and settings. With SaaS, the provider manages most of the security and leaves the user in control of access and permissions (CSA, 2024).

Data Security in the cloud differs from traditional data security due to its special storage architecture. Cloud computing generally uses distributed storage. Data ownership and control are separated. Users have ownership, but control lies within 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 plaintext, which is vulnerable to unauthorized and potentially malicious access when transmitted over a network. Cloud encryption is the transformation of data into a secret format to ensure confidentiality and even data integrity. It is a service offered by cloud storage providers that uses encryption algorithms (Manvi & Shyam, 2021) to convert data into a protected and unreadable form, making the encrypted data unusable without knowledge of the key. The encryption process can be carried out using different techniques such as symmetric and asymmetric encryption. In symmetric cryptography, the same key is used for encryption and decryption, unlike asymmetric cryptography, which uses a pair of public and private keys for encryption and decryption. There are several algorithms for symmetric encryption, the most used being the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES) or its variant Triple DES. The best-known representative of asymmetric encryption or public-key cryptography is the RSA algorithm, named after its creators Rivest, Shamir and Adleman. An important aspect of data security during transmission or remote storage is maintaining the integrity of the data. Hash functions can be used for this purpose to ensure that the received data is identical to the original. Most used hash functions used in practice are the 256-bit Secure Hash Algorithm 256-bit (SHA-256) and the Message Digest Algorithm 5 (MD5).

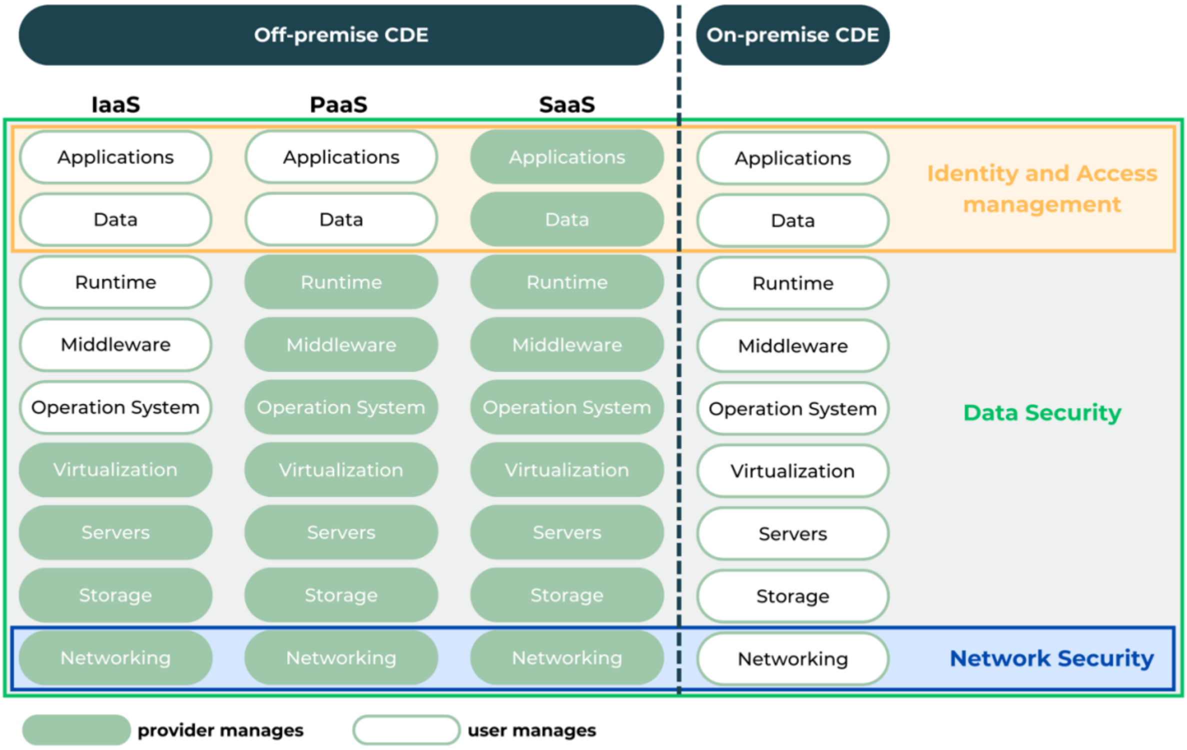


Figure 2: Responsibility model for information security mechanisms regarding cloud service models.

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

Cloud computing has a strong impact on *Identity and Access management (IAM)*. In public and private clouds, two parties need to manage IAM without compromising security. Cloud computing leads to many changes in the way IAM is managed for internal systems. The most important difference is the relationship between the provider and the cloud user. IAM cannot be managed by just one or the other, so a confidential relationship and the definition of responsibilities are required to enable the management of identity, authorization and access (CSA, 2021). There are several standards for identity and access management used in cloud computing. According to (CSA, 2021), the most widely used standards for identity verification include SAML (Security Assertion Markup Language), OAuth 2.0 and OpenID, which fall under Single Sign-On (SSO).

2.5.2 Physical security

Ensuring the physical security of the server infrastructure also plays an important role in the provision of security mechanisms in the cloud. 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. Data centers are secure facilities to which only authorized individuals have physical access and which are video-monitored and guarded by security personnel to detect suspicious activity.

However, incidents can still occur, whether due to 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. Unlike other technologies, cloud computing must take into account the involvement of third parties and the inherent differences in the use of shared resources. Backing up data stored in the cloud plays an important role if a system fails and important data needs to be restored. Various strategies are used when implementing data backups, e.g. full backups, incremental backups and differential backups. Depending on the importance and sensitivity of the data stored in the cloud, it is important to consider which backup approach should be used.

2.5.3 Standards compliance

Apart from ISO 19650 series of standards which apply to Information management using BIM, CDE environments must also comply with standards that apply to cloud computing. Over the last decade, the issue of information security in cloud computing has attracted a lot of attention from governments and the IT industry. To effectively measure the level of security offered by cloud service providers, so that cloud users can choose the most suitable provider for their security needs, standardization of validation and certification procedures is required. 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).

Cloud computing standards are constantly evolving. It is therefore important for cloud providers and users to keep up to date with the latest standards to ensure their cloud environments are secure and compliant. The ISO/IEC 27000 family of standards is considered the most widely used standard for information security management systems and their requirements. Together, they enable organizations to manage the security of assets such as financial information, intellectual property, employee data and information entrusted to third parties (ISO, 2022a). 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, 2022b). 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 standard and various other standards in the ISO/IEC 27000 family, such as ISO/IEC 27018 on the privacy implications of cloud computing and ISO/IEC 27031 on business continuity. The ISO/IEC 27018 standard focuses on the protection of personally identifiable information (PII) in public clouds that serve as PII processors (ISO, 2022b).

System and Organization Controls 2 (SOC 2) is concerned with auditing the operational processes of IT organizations that provide services of any kind and is considered the global standard for cybersecurity risk management systems. The organization's policies, practices and controls are established to meet the five trust principles (security, availability, processing integrity, confidentiality and privacy), which are evaluated in the audit report.

3. FRAMEWORK FOR ENSURING DIGITAL TRUST IN CDE-BASED BIM WORKFLOWS

In many BIM and CDE projects, cognition-based, affect-based and system-based trust are often not fully realized, leading to potential security and privacy vulnerabilities and a general lack of trust between stakeholders in the shared responsibility model. This trust gap can undermine collaboration and put critical information at risk. To address these challenges, we propose a framework specifically tailored to improve security and privacy in BIM and CDE environments. Our framework is based on the PASTA threat model, which provides a structured approach to identifying, assessing and mitigating risks, helping to create a secure foundation for trust in all aspects of project collaboration.

3.1 Cognition-based trust - ISO 19650 standards

Cognition-based trust, which is based on the understanding of a partner's reliability, is closely aligned with the principles of the ISO 19650 series of standards. The ISO 19650 series of standards focuses on the management of information throughout the life cycle of a building using BIM (BSI, 2023). By promoting clear, structured information sharing and accountability, ISO 19650 supports cognition-based trust by providing transparency in roles, responsibilities and data accuracy. This structured approach enables project partners to build trust, reduce uncertainty and improve joint decision-making through a consistent flow of information and reliable data management.

The ISO 19650 series, titled "*Organization and digitization of information about buildings and civil engineering works, including building information modelling - Information management using building information modelling*", is an international standard for managing information over the whole life cycle of a built asset using BIM (BSI, 2023). The series is divided into five parts:

1. **Concepts and principles**: an overview of the principles and concepts of information management using BIM.
2. **Delivery phase of the assets**: requirements for managing information during the delivery phase of a built asset, from planning and design to construction.
3. **Operational phase of the assets**: requirements for managing information during the operational phase of a built asset, from handover to maintenance and demolition.
4. **Information exchange**: requirements for the exchange of BIM information between different software applications and stakeholders.
5. **Security-minded approach to information management**: requirements for the management of information security in BIM projects.

The ISO 19650-5 Security minded approach to information management using BIM standard provides a framework to help organizations understand the key vulnerabilities and the types of controls required to limit the resulting security risks to a level that is tolerable for stakeholders. The standard recognizes that the use of computer-based technologies already supports new ways of working, but that the inherent vulnerabilities and resulting security risks must also be considered. The standard promotes the adoption of a security-minded, risk-based approach that can be applied both inside and outside organizations. It assumes that the implementation of the measures outlined in it will help to reduce the risk of loss, misuse or alteration of sensitive information that may impact the security and resilience of assets, products, the built environment or the services provided by, from or through them. The document is aimed at all organizations involved in the use of information management and technologies in all activities related to built assets or products and the provision of services in the built environment (ISO, 2020). The main part of the standard is divided into six chapters:

1. **Establishing the need for a security-minded approach using sensitivity assessment process**. The chapter describes the spectrum of security risks, identifying organizational sensitivities, identifying third party sensitivities, recording, and reviewing the assessment. It outlines the process of determining whether a security-minded approach is required at all, specifies the need to record the outcome of the security triage process, and provides instructions to follow if a security-minded approach is required.

2. **Initiating the security-minded approach**. It provides instructions for establishing governance, accountability, responsibility and commencing the development for the approach within the organization and between multiple organizations in collaboration. It points out that the activities described for implementing the approach must be carried out by a suitably qualified and experienced individual.
3. **Developing a security strategy**. This chapter explains what must be included in a security strategy. It also includes instructions on how to assess security risks and develop mitigation measures with appropriate documentation and a review plan.
4. **Developing a security management plan**. It lists everything that must be included in a security plan. It contains instructions for passing on information to third parties and for logistical security, which can be obtained from specialists. It contains instructions for monitoring, auditing, and reviewing the security management plan and managing responsibility and accountability for security.
5. **Developing a security breach/incident management plan**. Chapter contains instructions for a possible security breach or incident. It contains information on how to create a plan which includes incident detection and containment, recovery, and post incident review.
6. **Working with appointed parties**. This chapter provides instructions for work outside formal appointments, e.g. tendering and measures contained in appointment documents where they will encounter sensitive information.

The standard also includes four annexes with 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. The annexes contain further information on the security of sensitive information and help the parties involved to determine the approach.

3.2 Affect-based trust - BIM Execution Plan

Affect-based trust that arises from personal connections and mutual investment in relationships should be well supported in project documentation, e.g. the BIM Execution Plan (BEP). Project documentation should include clear instructions for managing information security, privacy and collaboration practices to help partners build trust through shared commitments to project integrity.

The BEP is a comprehensive document that helps project stakeholders move forward with clear roles and expectations. It is an essential deliverable 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 execution 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) details of practical workflows. 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 organization, (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) work 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 organization, 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 requirements, including hardware, software, networks and modeling content for the project to be used for BIM. It identifies fourteen specific categories to support the BIM project execution process.

1. **BIM Project Execution Plan Overview**: review of the plan based on the categories developed after analyzing the documents listed below, reviewing current execution plans, discussing the issues with industry experts, and revising through a comprehensive review by various industry organizations.
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 / BIM Uses**: the plan should include a clear list of BIM goals, the BIM Use Analysis Worksheet and specific information on the selected BIM Uses.
5. **Organizational roles / Staffing**: for each selected BIM Use, the team must specify which organization(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 organizational 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 considering 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 licenses, networks, and modeling 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, organized, communicated, and controlled.
13. **Project Deliverables**: the project team should consider what deliverables are required by the project owner. Deliverables should consider 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.

3.3 System-based trust - BIM and CDE providers security and privacy assessment

With *system-based trust*, the parties assume the reliability and efficiency of the system, which is usually taken for granted. In BIM workflows, stakeholders typically rely on the seamless operation of CDEs for data exchange and collaboration, often without examining the underlying security measures or privacy safeguards. However, assessing the security and privacy capabilities of BIM and CDE providers is critical to reinforcing this trust and ensuring that the assumed system reliability is backed up by strong security safeguards. By conducting security assessments, project teams can verify confidence in the system and ensure that security and privacy are aligned with project requirements and hidden risks are minimized.

As BIM and CDE environments become more widespread in construction projects, the number of tools offering these functions is also increasing. CDE providers use the cloud computing infrastructure to deliver the services to end users and must ensure the security and privacy mechanisms described in section 2.3 to guarantee confidentiality, integrity, and availability. Table 1 shows the assessment of these mechanisms for Dalux (2023a; 2023b; 2020), Procore (2023; 2024), Autodesk BIM360 (2024), Bentley Systems (2024a; 2024b), and Trimble (2023; 2024) based on publicly available information.

Table 1: BIM and CDE providers security and privacy assessment.

		Dalux	**Procore**	**BIM360**	**Bentley Systems**	**Trimble**
Data Security	Encryption	**	Stored data encrypted. **	Stored data encrypted with AES-256.	Stored data encrypted (Azure Storage Service Encryption).	*
	Hashing	Argon2, BCrypt, PBKDF2 (and similar) functions used for passwords.	*	Salted hashed passwords.	One way salted hashed passwords.	*
Network Security	Firewall	*	✓	✓	✓	*
	Transport Layer Security (TLS)	✓	TLS v1.2 with 256-bit encryption.	TLS v1.2 with secure cipher suites.	TLS v1.2.	*
IAM	Authentication	✓**	Single Sign On via SAML. OAuth 2.0 API authentication with third-party applications.	Single Sign On.	Single Sign On.	Single Sign On.
	Authorization	✓**	Role-based access.	Role-based access.	Role-based access.	**
Physical Security	Location	Uses Amazon Web Services EMEA SARL.	16 secure global file storage locations. Uses private cloud infrastructure for data at rest.	All data is stored in secured data centers owned and powered by Amazon Web Services.	Uses Microsoft Azure cloud provider.	Uses Amazon Web Services.
	Backup	Backup on daily basis.	Redundant infrastructure with several replicas of the application software on each server. All data are copied to off-site storage every 20 minutes. Replication distributes this	Data is replicated between data centers in separate locations. Replication prevents the possibility of data loss or delay in service if failover to a backup data center is required.	At least two web server components, two Application Server Components, and the database is mirrored. All systems are backed up daily at a minimum and	**

			offline snapshot across the United States.	Data is usually replicated within 15 minutes.	hourly for transaction logs.	
	Availability	**	99,9% uptime.	High availability with redundant systems.	99,9% uptime.	99,98% uptime.
Standards compliance	SOC 2	*	SOC 2 (Type 2) compliant.	SOC 2 (Type 2) compliant.	SOC 2 (Type 2) compliant.	SOC 2 (Type 2) compliant.
	ISO 19650	*	*	*	*	*
	ISO 27000	Provider of hosting service is ISO 27001 (or equivalent standard) compliant.	ISO 27001:2013 compliant.	ISO 27001, ISO 27017, and ISO 27018 compliant.	ISO 27001:2013 compliant.	ISO 27001:2013 compliant.

* Information is not provided.

** Not clear.

Based on the information we have collected, we have some understanding of how selected CDE providers handle sensitive user data. Procore, BIM360 and Bentley Systems provide the necessary data about their security mechanisms, while Dalux and Trimble Connect only provide partial information.

The *Data Security* mechanisms, especially encryption, are explicitly stated at BIM360 and linked to the cloud service provider at Bentley Systems. Other providers only state that they provide encryption. Similarly, only BIM360, Bentley Systems and Procore provide suitable information for *Network Security* and *IAM*.

Physical Security depends on whether CDE providers rent capacity from third-party providers or whether they have their own cloud infrastructure. As users host their data in the application, they need to have an idea of where and how their data is stored, what the availability is and what backup methods are used. This is particularly important in the European Union, where information privacy is governed by the General Data Protection Regulation (GDPR). Procore, BIM360 and Bentley Systems provide sufficient information to end users, while Dalux and Trimble Connect do not provide the necessary insight.

We have examined the selected providers for compliance with the standards applicable to cloud and BIM environments. All, apart from Dalux, comply with the SOC 2 standard. The selected providers also comply with at least the ISO 27001 standard for information security management systems from the ISO 27000 family of standards. Only BIM360 complies with the ISO 27017 and ISO 27018 standards, which contain guidelines for information management in cloud environments. However, none of the selected providers refer to compliance with ISO 19650 standard, which regulates information management when using BIM, or support users in complying with this standard.

3.4 The PASTA threat model

The Process for Attack Simulation and Threat Analysis (PASTA) is a risk-centric threat modeling framework introduced by Tony UcedaVélez in 2012 (UcedaVelez & Morana, 2015). It was developed to bridge the gap between business objectives and technical requirements and provides a structured approach to analyzing security threats. The PASTA framework is characterized by its comprehensive, multi-stage methodology, ranging from high-level business risk assessment to detailed attack modeling. This makes it highly adaptable to different domains and ensures a thorough security analysis at a technical and business level (VerSprite, 2021).

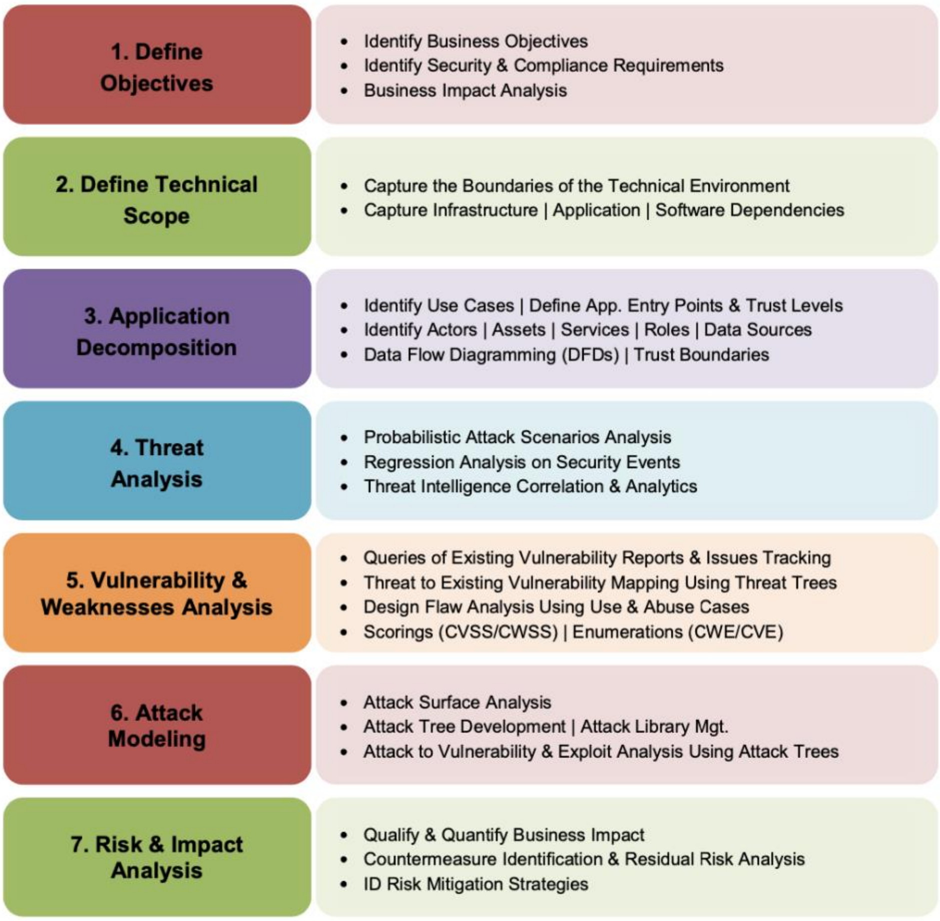

1. Define Objectives
Identify Business Objectives
Identify Security & Compliance Requirements
Business Impact Analysis
2. Define Technical Scope
Capture the Boundaries of the Technical Environment
Capture Infrastructure | Application | Software Dependencies
3. Application Decomposition
Identify Use Cases | Define App. Entry Points & Trust Levels
Identify Actors | Assets | Services | Roles | Data Sources
Data Flow Diagramming (DFDs) | Trust Boundaries
4. Threat Analysis
Probabilistic Attack Scenarios Analysis
Regression Analysis on Security Events
Threat Intelligence Correlation & Analytics
5. Vulnerability & Weaknesses Analysis
Queries of Existing Vulnerability Reports & Issues Tracking
Threat to Existing Vulnerability Mapping Using Threat Trees
Design Flaw Analysis Using Use & Abuse Cases
Scorings (CVSS/CWSS) | Enumerations (CWE/CVE)
6. Attack Modeling
Attack Surface Analysis
Attack Tree Development | Attack Library Mgt.
Attack to Vulnerability & Exploit Analysis Using Attack Trees
7. Risk & Impact Analysis
Qualify & Quantify Business Impact
Countermeasure Identification & Residual Risk Analysis
ID Risk Mitigation Strategies

Figure 3: Seven stages of PASTA (UcedaVelez & Morana, 2015).

PASTA is divided into seven different stages (Figure 3), each focusing on identifying, assessing, and reducing risks. The stages ensure a holistic assessment of risks by considering both technical vulnerabilities and their potential impact on business operations. This approach aligns system vulnerabilities with business risks and provides a risk-centric perspective that can be applied across industries. The seven stages are as follows (Shevchenko et al., 2018; Siddique, 2021; Wolf et al., 2021):

1. **Define Objectives:** This first stage focuses on identifying the business goals, key assets, and security requirements of the system. It includes a Business Impact Analysis (BIA) to prioritize the system's security needs by evaluating potential consequences on the business if key assets are compromised.
2. **Define the Technical Scope**: At this stage, the boundaries of the technical environment are defined, including the infrastructure, software dependencies, and application layers. By mapping out the system architecture, analysts identify critical components and areas of potential exposure. Network diagrams and high-level architectural diagrams may be used here to visualize the system's technical landscape.
3. **Application Decomposition**: The system is broken down into components, identifying key entry points, roles, and data flows. Data flow diagrams (DFDs) are commonly used to highlight where vulnerabilities may occur by tracking the movement of data within the system and defining trust boundaries.
4. **Threat Analysis**: In this stage, a comprehensive analysis of potential threats is conducted, incorporating known vulnerabilities and likely attack scenarios. Threat libraries, such as Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, can be employed to systematically identify threats that are relevant to the system under analysis.
5. **Vulnerability and Weakness Analysis**: The system is examined for specific vulnerabilities, referencing public databases like the Common Vulnerabilities and Exposures (CVE) repository. PASTA maps these vulnerabilities to the identified threats, focusing on mitigating weaknesses that pose the greatest risk to both business operations and technical functionality.

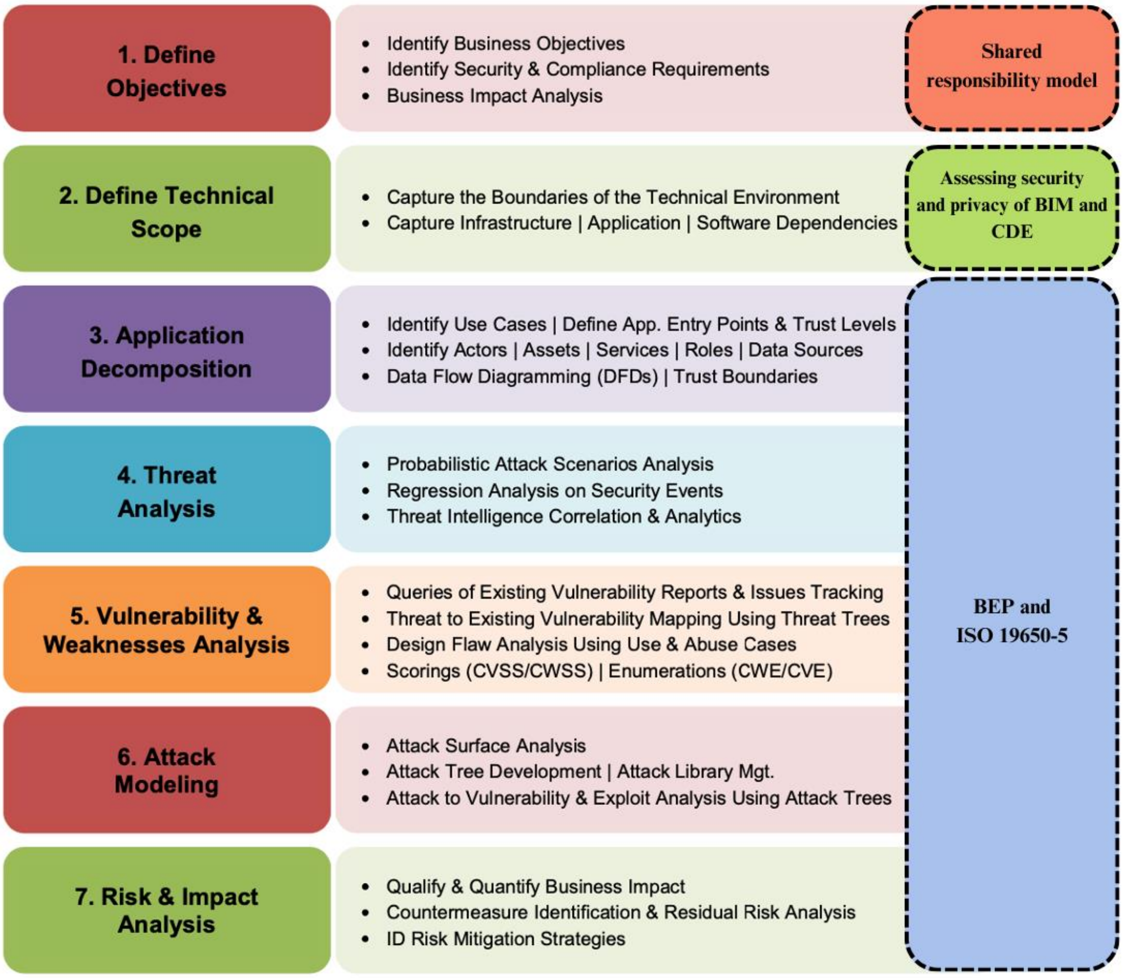
6. **Attack Modeling**: Vulnerabilities are analyzed through attack trees or other models that visualize how potential threats could exploit system weaknesses. These models help security analysts anticipate an attacker's methods and formulate appropriate defensive strategies.
7. **Risk and Impact Analysis**: The final stage of PASTA quantifies the risks associated with identified threats and vulnerabilities. This involves calculating scores using metrics like the Common Vulnerability Scoring System (CVSS) to prioritize mitigation strategies and balance the cost of security measures against potential business impacts.

PASTA's multi-stage process ensures that both business objectives and technical constraints are taken into account, making it a flexible and comprehensive framework for assessing threats across different industries.

Key features of PASTA:

- **Risk-driven focus:** PASTA prioritizes risks based on business impact. This ensures that security solutions are aligned with the organization's most important assets and services.
- **Attack simulation:** By developing attack models and simulating potential threats, PASTA allows organizations to anticipate how attackers might exploit vulnerabilities in their systems. This proactive approach is critical to formulating robust defenses.
- **Iterative nature:** PASTA is an iterative framework that enables continuous improvement of threat analysis as new vulnerabilities and attack methods are discovered. This makes it adaptable to evolving security landscapes, especially in industries where cybersecurity risks are constantly changing.

3.4.1 PASTA for BIM and CDE



1. Define Objectives
• Identify Business Objectives
• Identify Security & Compliance Requirements
• Business Impact Analysis
Shared responsibility model
2. Define Technical Scope
• Capture the Boundaries of the Technical Environment
• Capture Infrastructure | Application | Software Dependencies
Assessing security and privacy of BIM and CDE
3. Application Decomposition
• Identify Use Cases | Define App. Entry Points & Trust Levels
• Identify Actors | Assets | Services | Roles | Data Sources
• Data Flow Diagramming (DFDs) | Trust Boundaries
4. Threat Analysis
• Probabilistic Attack Scenarios Analysis
• Regression Analysis on Security Events
• Threat Intelligence Correlation & Analytics
5. Vulnerability & Weaknesses Analysis
• Queries of Existing Vulnerability Reports & Issues Tracking
• Threat to Existing Vulnerability Mapping Using Threat Trees
• Design Flaw Analysis Using Use & Abuse Cases
• Scorings (CVSS/CWSS) | Enumerations (CWE/CVE)
6. Attack Modeling
• Attack Surface Analysis
• Attack Tree Development | Attack Library Mgt.
• Attack to Vulnerability & Exploit Analysis Using Attack Trees
7. Risk & Impact Analysis
• Qualify & Quantify Business Impact
• Countermeasure Identification & Residual Risk Analysis
• ID Risk Mitigation Strategies
BEP and ISO 19650-5

Figure 4: PASTA threat model for BIM and CDE.

The digitalization of construction processes through cloud-based solutions brings new challenges for cybersecurity. The PASTA framework provides a robust approach to addressing these risks by combining administrative, technical and organizational security measures in a structured, iterative process that adapts to evolving threats.

The framework can be adapted to BIM and CDE environments by integrating its seven stages into the lifecycle of these systems. This ensures continuous protection against cyber threats while ensuring compliance with legal standards.

Stage 1: Define Business and Security Objectives

In the context of BIM and CDE, the first step of PASTA is to clearly define the objectives for security and privacy. This includes protecting the confidentiality, integrity and availability of sensitive project data, ensuring compliance with legal frameworks and maintaining the trust of all parties involved. In this context, it is important to clarify the responsibilities of the data owner and the cloud service provider, which is often overlooked in cloud environments. Contractual obligations must include specific security standards and responsibilities to ensure long-term security. Defining the *shared responsibilities model* is extremely important in the initial phase of the project as it has an impact on the entire course of the project.

Stage 2: Define the Technical Scope

In this stage, PASTA assesses the technical architecture of BIM and CDE environments, including the cloud infrastructure. This scope covers all components required for the operation of BIM and CDE, such as data repositories, APIs, user interfaces and third-party integrations. Identifying all entry points into the system helps to highlight potential vulnerabilities. The division of responsibility between the service provider and the user organization must be clearly defined here, particularly with regard to data storage, encryption and identity management. *Assessing the security and privacy* of BIM and CDE providers is an important part of this stage, as it can reveal various discrepancies between the users' requirements and the mechanisms used by the cloud service providers.

Stage 3: Application Decomposition

In BIM and CDE environments, application decomposition is about mapping data flows, identifying key processes and defining trust boundaries within the system. The *BEP* plays a crucial role in this phase, as it describes in detail how data is created, managed and exchanged between stakeholders. It provides a structured approach to defining trust boundaries, data exchange protocols and collaboration mechanisms and ensures that data flows are aligned with security and privacy objectives. The *ISO 19650-5* standard complements this by providing a security-minded approach to managing sensitive information within trust boundaries, reducing the risk of misuse or alteration of important project data.

Stage 4: Threat Analysis

Threat analysis in BIM and CDE environments assesses potential risks such as unauthorized access, data breaches or cloud service disruptions. *ISO 19650-5* provides guidelines for a security process that identifies the sensitivities of companies and third parties to prioritize the threats. The *BIM execution plan* supports this phase by outlining specific threat scenarios and mitigation strategies in conjunction with the data management and access protocols outlined in the project documentation. Together, these elements ensure that evolving threats are continually assessed and addressed.

Stage 5: Vulnerability and Weakness Analysis

This stage identifies vulnerabilities such as incorrectly configured access controls or inadequate encryption in BIM and CDE environments. The *BEP* helps to eliminate these vulnerabilities by defining quality control measures and outlining responsibilities for securing models and exchanging data. *ISO 19650-5* supports this stage by recommending a systematic assessment of security risks and the implementation of mitigation measures to ensure alignment between the organization's risk profiles and security controls.

Stage 6: Attack Modeling

Attack modeling illustrates how vulnerabilities in BIM and CDE systems could be exploited so that stakeholders can anticipate attack paths. The *BEP* provides a basis for this by defining procedures for access control, incident response and data recovery. These measures, in conjunction with the recommendations of *ISO 19650-5*, enable proactive defense strategies, such as improving authentication protocols or isolating critical data assets from external access points.

Stage 7: Risk and Impact Analysis

In the final stage, the impact of potential risks on the project objectives and system functionality is quantified. The *BEP* ensures that this analysis is directly linked to project deliverables and milestones and emphasizes the importance of uninterrupted access to accurate and secure data. *ISO 19650-5* emphasizes this by promoting a security-minded approach to project documentation and workflows to ensure that risk mitigation strategies are both practicable and aligned with project objectives.

4. DISCUSSION

This paper highlights the importance of addressing security and privacy concerns in BIM and CDE environments, given their increasing reliance on cloud-based technologies and the highly sensitive nature of the information they manage. Although the ISO 19650-5 standard provides a basic framework for information security, there are several critical areas where it is inadequate and could be improved to better address the complexity of modern cloud-based construction workflows.

4.1 Gaps in ISO 19650-5

While the ISO 19650-5 standard provides a basic framework for information security in BIM, it does not adequately address internet-based threats such as cyberattacks, data breaches and malware. This gap is becoming increasingly important as BIM projects move to public cloud platforms, which inherently introduce new risks. In addition, the ambiguous wording of the standard and the lack of explicit technical guidance hinder its effectiveness. Enhancements such as detailed guidance on encryption, identity management and incident response, ideally included in Annex B, would increase its usefulness.

The lack of an explicit connection between BIM and CDE providers and user organizations also weakens its applicability. Clear definitions of roles, responsibilities and technical safeguards are necessary to align stakeholders on a consistent approach to data security.

4.2 The Role of BIM and CDE Providers

Our analysis shows that CDE providers are not consistent in their disclosure of security and privacy mechanisms. Transparency is not only beneficial, but essential for building digital trust. While providers such as Procore and Bentley Systems adhere to industry standards and provide clear security information, others do not go into enough detail, preventing users from effectively assessing the reliability of services.

Providers should be encouraged or required to disclose their security mechanisms and compliance with relevant standards so that users can make informed decisions. This transparency is a cornerstone for promoting trust and ensuring compliance with project-specific security requirements.

4.3 Technical Requirements in the BEP

The BIM Execution Plan (BEP) plays a crucial role in project execution but often neglects critical technical safeguards. Including explicit security and privacy requirements would ensure alignment with project standards and mitigate risks such as data breaches and unauthorized access. This integration strengthens the BEP not only as a tool for workflow management, but also robust security planning.

4.4 User Guidelines for Security and Privacy

Users of BIM and CDE environments must adopt proactive measures to protect sensitive information. Key recommendations include:

1. **Data minimization**: Share only the data necessary for the project and consult security experts to evaluate the risks.
2. **Data Security Officer**: Appoint a dedicated officer to oversee the security and privacy measures implemented throughout the project.

3. **Provider vetting**: Research providers' security practices and give preference to those that are certified to industry standards.
4. **Documentation**: Request clear documentation on providers' security practices and use this as a basis for contract negotiations.
5. **Contractual security terms**: Include security requirements and potential consequences for violations explicitly in contracts with providers.

4.5 The Value of the PASTA Framework

Integrating the PASTA threat model into BIM and CDE workflows provides a structured, iterative approach to risk assessment and mitigation. By matching business risks with technical vulnerabilities, PASTA ensures a comprehensive assessment of threats while promoting proactive measures to address them. This approach is particularly valuable in dynamic, cloud-based environments where security challenges evolve rapidly. Combined with increased user awareness and improved standards, the PASTA framework strengthens the foundation for digital trust and resilience in BIM and CDE environments.

5. CONCLUSION

The increasing use of BIM and CDE in construction projects requires robust security and privacy measures to protect sensitive project information. This paper provides a comprehensive overview of the mechanisms required for effective information management and highlights the technologies and standards that ensure the confidentiality, integrity and availability of data in these environments. It also emphasises the role of digital trust as a cornerstone for successful collaboration in cloud-based workflows by linking technical safeguards and human relationships.

Our assessment of selected CDE providers revealed significant inconsistencies in terms of transparency and implementation of security and privacy mechanisms. While some providers demonstrate clear adherence to security standards and offer detailed information about their policies, others provide only partial or incomplete details. This lack of transparency undermines system-based trust, making it difficult for users to make informed decisions. A standardised approach to the disclosure of security and privacy measures is essential to close this gap and increase trust in these systems.

Beyond general cloud security standards, BIM and CDE solutions need to integrate additional security measures tailored to the specific needs of the construction industry. Cognition-based trust can be strengthened by reinforcing and adhering to the ISO 19650 series of standards, which promotes transparency and accountability in information management. Similarly, affect-based trust is strengthened through a comprehensive BEP that defines the roles of collaboration and establishes shared commitments to project integrity.

On the other hand, the ISO 19650-5 standard provides a basic framework for information security, but needs to be further refined to address the nuances of cybersecurity in cloud-based environments. By introducing explicit technical requirements and ensuring alignment between BIM users and CDE providers, the standard could close existing gaps and promote a security-minded approach. Including these requirements in the BEP would further improve the integration of security and privacy into project workflows and ensure that these considerations are treated as core elements of project planning and execution, rather than an afterthought.

One key finding from this research is that CDE providers need to improve the transparency of their security mechanisms and strictly adhere to the relevant standards. Users, in turn, need to take a more proactive role in understanding and mitigating security risks by requiring clearer documentation, vetting providers against industry standards and including security considerations in contractual agreements.

Adopting the PASTA threat model provides a structured, iterative approach to managing security risks in BIM and CDE environments. By continuously assessing threats, vulnerabilities and their impact on the organisation, this framework ensures that security remains a dynamic and evolving element of digital collaboration. Combined with improved transparency from providers and proactive engagement from users, PASTA is helping to build the digital trust required for secure and resilient construction operations.

To summarise, building and maintaining digital trust in CDE-based BIM workflows is critical to overcoming the challenges of digital transformation in the construction sector. This trust, supported by robust standards, transparent provider practices and collaborative frameworks, forms the basis for secure and efficient project delivery in an increasingly connected world.

ACKNOWLEDGMENTS

This paper is significantly extended and improved version of our previous work which was presented at 2024 European Conference on Computing in Construction (EC3) in Crete, Greece and 2024 International Conference on Computing in Civil and Building Engineering (ICCCBE) in Montréal, Canada.

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

REFERENCES

Autodesk. (2024). Security Whitepaper. Autodesk Construction Cloud. https://www.autodesk.com/bim-360/construction-management-software/security/ [Accessed: 2023-12-05].

Bamasoud, D. M., Al-Dossary, A. S., Al-Harthy, N. M., Al-Shomrany, R. A., Alghamdi, G. S., & Algahmdi, R. O. (2021). Privacy and Security Issues in Cloud Computing: A Survey Paper. 2021 International Conference on Information Technology (ICIT), 387–392. https://doi.org/10.1109/ICIT52682.2021.9491632

Bentley. (2024a). Bentley Systems Trust Portal. Bentley. https://trustportal.bentley.com [Accessed: 2023-12-05].

Bentley. (2024b). Bentley Trust Center. Bentley. https://www.bentley.com/legal/trust-center/ [Accessed: 2023-12-05].

BSI. (2023). ISO 19650—Building Information Modelling (BIM). The British Standards Institution. https://www.bsigroup.com/en-GB/iso-19650-BIM/ [Accessed: 2023-11-23].

Cerić, A. (2016). Trust in Construction Projects (1st ed.). https://www.routledge.com/Trust-in-Construction-Projects/Ceric/p/book/9781138814165

Cerić, A., Vukomanović, M., Ivić, I., & Kolarić, S. (2021). Trust in megaprojects: A comprehensive literature review of research trends. International Journal of Project Management, 39(4), 325–338. https://doi.org/10.1016/j.ijproman.2020.10.007

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

CSA. (2021). Security Guidance for Cloud Computing. Cloud Security Alliance. https://cloudsecurityalliance.org/research/guidance/ [Accessed: 2023-11-21].

CSA. (2024). What is the Shared Responsibility Model in the Cloud?. Cloud Security Alliance. https://cloudsecurityalliance.org/blog/2024/01/25/what-is-the-shared-responsibility-model-in-the-cloud [Accessed: 2024-10-16].

Dalux. (2020). Data Processing Agreement. Dalux. https://www.dalux.com/wp-content/uploads/2022/08/Data-Processing-Agreement_en-2.pdf [Accessed: 2023-12-05].

Dalux. (2023a). Privacy Notice. Dalux. https://www.dalux.com/privacy-policy/ [Accessed: 2023-12-05].

Dalux. (2023b). Terms and conditions noncommercial use. Dalux. https://www.dalux.com/terms-and-conditions-noncommercial-use/ [Accessed: 2023-12-05].

Das, M., Tao, X., & Cheng, J. C. P. (2021). BIM security: A critical review and recommendations using encryption strategy and blockchain. *Automation in Construction*, *126*, 103682. https://doi.org/10.1016/j.autcon.2021.103682

Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R. H., & Bashir, M. N. (2017). Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security? 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), 50–57. https://doi.org/10.1109/CLOUD.2017.16

Dolla, T., Venkatachalam, S., & Kumar Delhi, V. S. (2024). Institutional shaping of CDE implementation in BIM-enabled AEC projects. Journal of Information Technology in Construction, 29, 826–849. https://doi.org/10.36680/j.itcon.2024.036

ISO. (2015). ISO/IEC 27017:2015. International Organization for Standardization. https://www.iso.org/standard/43757.html [Accessed: 2023-12-05].

ISO. (2020). ISO 19650-5:2020. International Organization for Standardization. https://www.iso.org/standard/74206.html [Accessed: 2023-12-05].

ISO. (2022a). ISO/IEC 27000 family. International Organization for Standardization. https://www.iso.org/standard/iso-iec-27000-family [Accessed: 2023-12-04].

ISO. (2022b). ISO/IEC 27001:2022. International Organization for Standardization. https://www.iso.org/standard/27001 [Accessed: 2023-12-04].

Kalay, Y. E. (1999). The future of CAAD: From computer-aided design to Computer-aided collaboration. In G. Augenbroe & C. Eastman (Eds.), Computers in Building: Proceedings of the CAADfutures'99 Conference. Proceedings of the Eighth International Conference on Computer Aided Architectural Design Futures held at Georgia Institute of Technology, Atlanta, Georgia, USA on June 7–8, 1999 (pp. 13–30). Springer US. https://doi.org/10.1007/978-1-4615-5047-1_2

Klinc, R., Turk, Ž., & Dolenc, M. (2009). Engineering collaboration 2.0: Requirements and expectations. Journal of Information Technology in Construction (ITcon), 14(31), 473–488.

Klinc, R., Turk, Ž., & Dolenc, M. (2010). ICT enabled communication in construction 2.0. Pollack Periodica, 5(1), 109–120. https://doi.org/10.1556/Pollack.5.2010.1.8

Mahamadu, A.-M., Mahdjoubi, L., & Booth, C. (2013). Challenges to BIM-Cloud Integration: Implication of Security Issues on Secure Collaboration. 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, 209–214. https://doi.org/10.1109/CloudCom.2013.127

Manvi, S. S., & Shyam, G. K. (2021). Cloud Computing: Concepts and Technologies (1st ed.). CRC Press, Taylor & Francis.

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

Pavithra, S., Ramya, S., & Prathibha, S. (2019). A Survey On Cloud Security Issues And Blockchain. 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), 136–140. https://doi.org/10.1109/ICCCT2.2019.8824891

Procore. (2023). Procore Security and Data Governance Standards. Procore. https://www.procore.com//trust-and-security/security [Accessed: 2023-12-06].

Procore. (2024). Privacy Notice. Procore. https://www.procore.com//legal/privacy [Accessed: 2023-12-06].

Rajesh, Y. S., Kumar, V. G. K., & Poojari, A. (2024). A Unified Approach Toward Security Audit and Compliance in Cloud Computing. Journal of The Institution of Engineers (India): Series B, 105(3), 733–750. https://doi.org/10.1007/s40031-024-01034-x

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

Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P., & Woody, C. (2018). Threat Modeling: A Summary of Available Methods.

Siddique, A. (2021). Threat Modeling Methodologies for Network Security. https://doi.org/10.13140/RG.2.2.19672.42249

Sun, X. (2018). Critical Security Issues in Cloud Computing: A Survey. 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), 216–221. https://doi.org/10.1109/BDS/HPSC/IDS18.2018.00053

Trimble. (2023). Data Protection & Compliance for the Construction Industry. Trimble. https://www.viewpoint.com/security [Accessed: 2024-11-11].

Trimble. (2024). Share data and track activities. Trimble. https://www.trimble.com/en/products/trimble-connect/data-share-tracking [Accessed: 2024-11-11].

Turk, Ž., Sonkor, M. S., & Klinc, R. (2022). Cybersecurity assessment of BIM/CDE design environment using cyber assessment framework. Journal of Civil Engineering and Management, 28(5), Article 5. https://doi.org/10.3846/jcem.2022.16682

UcedaVelez, T., & Morana, M. M. (2015). Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. John Wiley & Sons.

VerSprite. (2021). Benefits of PASTA Threat Modeling and its 7 Steps. VerSprite. https://versprite.com/blog/what-is-pasta-threat-modeling/ [Accessed 2024-10-26].

WEF. (2022). Earning Digital Trust: Decision-Making for Trustworthy Technologies. World Economic Forum. https://www.weforum.org/publications/earning-digital-trust-decision-making-for-trustworthy-technologies/

Wolf, A., Simopoulos, D., D'Avino, L., & Schwaiger, P. (2021). The PASTA threat model implementation in the IoT development life cycle. 1195–1204. https://dl.gi.de/handle/20.500.12116/34700

Wong, W. K., Cheung, S. O., Yiu, T. W., & Pang, H. Y. (2008). A framework for trust in construction contracting. International Journal of Project Management, 26(8), 821–829. https://doi.org/10.1016/j.ijproman.2007.11.004

Xu, H., Cao, J., Zhang, J., Gong, L., & Gu, Z. (2019). A Survey: Cloud Data Security Based on Blockchain Technology. 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC), 618–624. https://doi.org/10.1109/DSC.2019.00100