DEVELOPMENT OF FRAMEWORKS FOR SECURING CIVIL INFRASTRUCTURE INFORMATION SYSTEMS FOR BUILDING CONSTRUCTION

Bolaji Kareem Ajisegiri[1], Oyebisi Olaleye Oyewole[2], Gbonjubola Oluwafunmilayo Binuyo[3], Christiana Kappo-Abidemi[4]

[1]Department of Technology Management, African Institute for Science Policy and Innovation, Obafemi Awolowo University, Nigeria
ORCID: https://orcid.org/0009-0001-0315-8490

[2]Department of Technology Management, African Institute for Science Policy and Innovation, Obafemi Awolowo University, Nigeria
ORCID: https://orcid.org/0009-0001-5182-1445

[3]Department of Technology Management, African Institute for Science Policy and Innovation, Obafemi Awolowo University, Nigeria
ORCID: https://orcid.org/0000-0002-4884-3563

[4]School of Development Studies, University of Mpumalanga, CNR D275 and R40 Roads, Riverside, Mbombela, South Africa
ORCID: https://orcid.org/0000-0001-9559-0514

✉Corresponding author: Christiana Kappo-Abidemi, e-mail: C.Kappo-Abidemi@ump.ac.za

ARTICLE INFO

Article history:
Received 18.09.2025
Received in revised form 21.10.2025
Accepted 25.11.2025
Published 30.12.2025

Section:
Information Technology

DOI

10.21303/2313-8416.2025.004093

KEYWORDS

building information modelling (BIM),
civil infrastructure information systems (CIIS),
data loss prevention (DLP),
frameworks,
governance,
risk management and compliance (GRC),
information systems,
NIST-CSF,
key performance indices (KPI)

ABSTRACT

The object of research. The development of compatible security frameworks that align with civil and building construction information systems and BIM was undertaken. The paper examined existing literature on traditional construction management concepts and the systems view of building construction projects. It explored information systems security frameworks for the deployment of cybersecurity principles; examined the risk management in the world of construction management and BIM. This was with the view to developing security protocols that protect BIM data from DLP threats.

Investigated problem. BIM and smart construction rely heavily on continuous data exchange leaving them exposed to cyberattacks. Previous researches in the field confirmed there was no existing cybersecurity standards that are directly applicable to construction project management. The dearth of information on the applicability of the existing ICS framework to construction management warrants that it is develop a new compatible framework solution that accommodate the dynamic capabilities of BIM and the scope, complexity among other of smart construction systems.

The main scientific results. The results showed that the NIST-CSF 2.0 (NIST Cybersecurity Framework), fine-tuned with some adaptabilities in relation to each specific project, is the most compatible and recommended security framework for BIM and CIIS, offering flexibility, scalability, and alignment with both information security and management needs. It also supported the fact that smart construction management is fast becoming a cyber-physical endeavor due to the extended reliance on digital platforms.

The area of practical use of the research results. Hence, the increasing call for government agencies such as the Federal Housing Authority (FHA) of Nigeria to develop construction-specific cybersecurity guidelines. It is also recommended that these agencies should integrate governance, risk management and compliance (GRC) into building approval processes.

Innovative technological product. The adoption of the new framework will empower construction firms to move from reactive to proactive cybersecurity frameworks while deploying ISO 27001 and NIST standards. Firms will hence be positioned to integrate cybersecurity metrics into project performance KPIs.

Scope of the innovative technological product. Cybersecurity must be recognized as a foundational pillar of smart construction and sustainable development in the built environment. Strategic investment, supportive policy frameworks, and capacity building are essential to achieving resilient and secure construction information systems. This is with a view to resolving all conundrum surrounding BIM and building construction for enhanced safety and security of project deliverables.

Kareem Ajisegiri, B., Oyewole, O. O., Binuyo, G. O., Kappo-Abidemi, C. (2025). Development of frameworks for securing civil infrastructure information systems for building construction. ScienceRise, 2, 29–47. http://doi.org/10.21303/2313-8416.2025.004093

1. Introduction

1. 1. The object of the research

This research was aimed at developing security protocols for smart construction information systems for the built environment in Nigeria. The research explored existing frameworks for the deployment of cybersecurity practices, examined construction project risk management approaches, and investigated construction project management lifecycle in the world of building information modelling (BIM). This was with the view to developing compatible framework solutions for security BIM data from data loss prevention (DLP) viewpoint.

Every business is a product of its information systems and building construction business is not an exception. This research lies at the intersection of project management and cybersecurity concepts from the standpoint of technology use and services. The research provides value additions to the increasingly critically digitized construction industry that has transformed from mere experimental concepts to standard operating reality. The move had changed how building construction projects are managed from conception and design to construction and demolition within the domain of architecture, engineering, and construction/facility management (AEC/FM).

1. 2. Problem description

The conceptualization of building and civil engineering project as a system relied on view construction and BIM as information systems powered by the Internet. However, protecting the information systems within the civil engineering and construction domain has presented a myriad of challenges and remains a subject of scholarly discussion. The scope, complexity, interdependencies, and interconnectedness of industrial and civil engineering systems, along with the constantly evolving nature of cyber threats exploiting vulnerabilities in these systems, necessitate the development of alternative security frameworks that align with civil and building construction information systems.

Several risk assessment approaches have been suggested to address only physical security in civil engineering construction [1]. However, there is a dearth of information for holistic frameworks that explained the cybersecurity aspect of the civil engineering construction process that aimed to address the following research gaps:

– effective risk management frameworks
– the use of emerging technologies in cybersecurity
– the effect of cyber activities on critical infrastructure
– the impact of regulations on cybersecurity
– the human factors in cybersecurity.

The above quests prompted the development of this research paper, which aims to establish frameworks for securing civil infrastructure information systems in building construction in Nigeria.

Examining the Code of Practice for Cyber Security in the Built Environment (CoP-CSBE), developed by the Institution of Engineering and Technology (IET), reveals a profound shift in policy, culture, and technology among civil engineering construction companies towards adopting BIM (building information modelling). CoP-CSBE's goal provides standards for companies in enhancing the cybersecurity of their operations within the system by ensuring that processes and elements involved are secured using the CIA (confidentiality, integrity, and availability) triad of information systems and security [2]. Hence, securing processes and elements in the civil engineering construction industry requires to view construction as a system or a collection of systems.

BIM, despite the challenges in its implementation due to the need for expertise and the initial cost outlay, provides with a good starting point and an opportunity for research in securing and understanding the nature of civil engineering infrastructure information systems. This is because, although project management has evolved from industrial and civil engineering project deliverables, the application of information systems and security concepts that guaranteed the security and safety of building construction has been very limited, if not non-existent. Facility planning, design, construction, and operations using BIM allow architects, engineers, and builders to visualize what

will be built in a virtual environment. Therefore, securing BIM data offers granular protection for building infrastructure and the built environment.

In the past, quite a lot of research on technology adoption related to technological services has emerged, particularly in the developed world. Most of them applied research models and frameworks traditionally used within the information systems (IS) literature [3]. Among the various models proposed, the technology acceptance model (TAM) [4], adapted from the theory of reasoned action (TRA) [5], appears to be the most widely accepted among researchers in the field of information systems. TAM posits that a user's adoption of a new information system is determined by their intention to use the system, which in turn is determined by their beliefs about the system [4].

The industrial control systems framework is designed to provide effective risk management for automated industrial processes, systems, and controls. Literature revealed that in what is referred to as smart buildings, many large civil engineering projects, including building facility construction, are increasingly becoming digital and dependent on both OT (operational technologies) and IT (information technology) for the various phases of project management. Securing BIM software systems involves protecting all levels of information exchange, from project initiation through planning, execution, control, monitoring, closure, and maintenance. However, there is a dearth of information on the applicability of the existing ICS framework to BIM and building construction for enhancing the safety and security of project deliverables; hence, this research. The research is therefore designed to address the question: What compatible framework is available for securing BIM data from a data loss prevention (DLP) standpoint? The broader objective of research is to develop frameworks for securing civil infrastructure information systems for building construction in Nigeria.

1. 3. Suggested solution to the problem

The TAM further suggests that two beliefs – perceived usefulness (PU) and perceived ease of use (PEOU) for a technology product are instrumental in explaining the variance in users' intentions. As [4] noted, future technology acceptance research must address how other variables affect usefulness, ease of use and user acceptance. Therefore, when considering the adoption of BIM, perceived ease of use and perceived usefulness may not fully explain behavioral intentions towards using technological services, necessitating a search for additional factors that can better predict technology acceptance. Another theory pertaining to the adoption of new technology is the Innovation Diffusion Theory (IDT) by [6].

According to [6], there are five perceived characteristics of innovation that can be used to form a favorable or unfavorable attitude toward an innovation, namely: relative advantage, compatibility, complexity, trialability, and observability. The two theoretical constructs, PU and PEOU, despite their limitations, are theorized to be fundamental determinants of system use and are operationalized in the technology acceptance model (TAM).

Perceived usefulness (PU): People tend to use or not use an application to the extent they believe will help perform their job better. It is defined as the degree to which a person believes that using a particular system would enhance their job performance [4].

Perceived ease of use (PEOU): Though potential users believe that a given application is useful, they may at the same time believe that it will elicit so much effort to use it. PEOU is hence defined as the degree to which a person believes that using a particular system would be free of effort [4].

The theory of reasoned action (TRA) explains how attitudinal and social influences can shape behavioral intentions. It posits that the strongest or most proximal predictor of volitional behavior is one's behavioral intention. Behavioral intentions are thought to be the result of both an individual influence and a normative influence. The individual influence on intention is a person's attitude towards performing volitional behavior. The normative influence on intention is what [5] referred to as one's subjective norm. One key component of the TRA is an attitude or valence response toward engaging in some volitional behavior. While social scientists disagree about the origins of attitudes, [5] suggested that an attitude toward performing a behavior is a function of the beliefs one holds about the behavior. According to [7], an attitude is the sum of belief strength and belief evaluation.

Belief strength: Beliefs generally link some attribute to a volitional behavior or attitude. Belief strength, therefore referred to as the certainty with which the belief is held.

Belief evaluation: One's attitude toward a volitional behavior is a function of the attributes one links to the behavior and belief evaluation. Belief evaluation is the judgment of whether attributes are positive or negative.

The other important component of TRA is subjective norm. A subjective norm is a function of a normative belief and the motivation to comply with that belief. A normative belief is the perceived expectation of important others regarding volitional behavior. According to [8], normative beliefs are individuals' beliefs about the extent to which significant others think they should or should not perform a particular behavior. Motivation to comply is the real or imagined pressure one feels to match others' perceived expectations through their behavior. It is defined as the degree to which individuals wish to behave consistently with the prescriptions of important others.

Despite widespread use of subjective measures in practice, little attention is paid to their quality and to their correlation with usage behavior. Given the low usage correlations often observed in research studies base important business decisions on invalidated measures may be misinformed about a system's acceptability to users. This explains why the unified theory of acceptance and use of technology is often used in research focusing on the deployment and adoption of technology services. The UTAUT model not only underscores the core determinants predicting intention to adopt and actual adoption but also allows researchers to analyze the contingencies of moderators that would amplify or constrain the effects of these determinants [9].

[10] conducted a critical analysis of BIM systems used in construction projects. They found that the challenges to achieving high adoption of BIM revolve around the proliferation of software packages, interoperability issues, high implementation costs, and a lack of peer-reviewed literature on BIM software systems. [11] stated that the subject matter of IT is the technology itself, which is the hardware and software that support the operations or functions of a business. In other words, IT refers to the design and implementation of information or data within the IS. [12] provided an overview of some information systems security concepts aimed at protecting BIM data.

[13] defined systems as consisting of people, processes, and technologies designed to operate on information. On the other hand, information systems (IS), as opposed to information technologies (IT), focus on how technology is used to manage and analyze data, and how to optimize the flow of information within an organization. [14] stated that the application of information technologies in civil infrastructure design, construction, and maintenance is growing at a rate much faster than ever before.

[15] argued that information systems and the Internet are nowadays at the very core of most businesses and services in companies, organizations, and institutions. [16] conducted a review of the adoption of digital technologies in industrial and civil engineering systems, exploring the various threats faced by organizations operating within these systems. [17] argued that the different phases of civil engineering construction projects are becoming increasingly digital and dependent on the extensive use of information and communication technologies (ICT) throughout the entire project lifecycle, from design to construction, operation, maintenance, and end-of-life.

[18] studied the interpolation between resilient management (RM) and civil infrastructure asset management (IAM) to develop a framework for resilience improvement strategies, including the creation of tactical and operational plans, monitoring execution, and optimizing performance. [19] suggested that BIM has been researched to serve the architecture, engineering, and construction/facility management (AEC/FM) domain by providing detailed 3D building models that could be used throughout the life cycle of a construction project, including planning, design, construction, operation, and dismantling.

The United Kingdom Centre for the Protection of National Infrastructure [2] provided an overview framework for the security of ICSs. These are good practice guides, representing the best of industry practices, including strategies, activities, and approaches that have been proven effective through research, evaluation, and implementation. [2] identified eight core elements of the ICS security framework as depicted in **Fig. 1**.

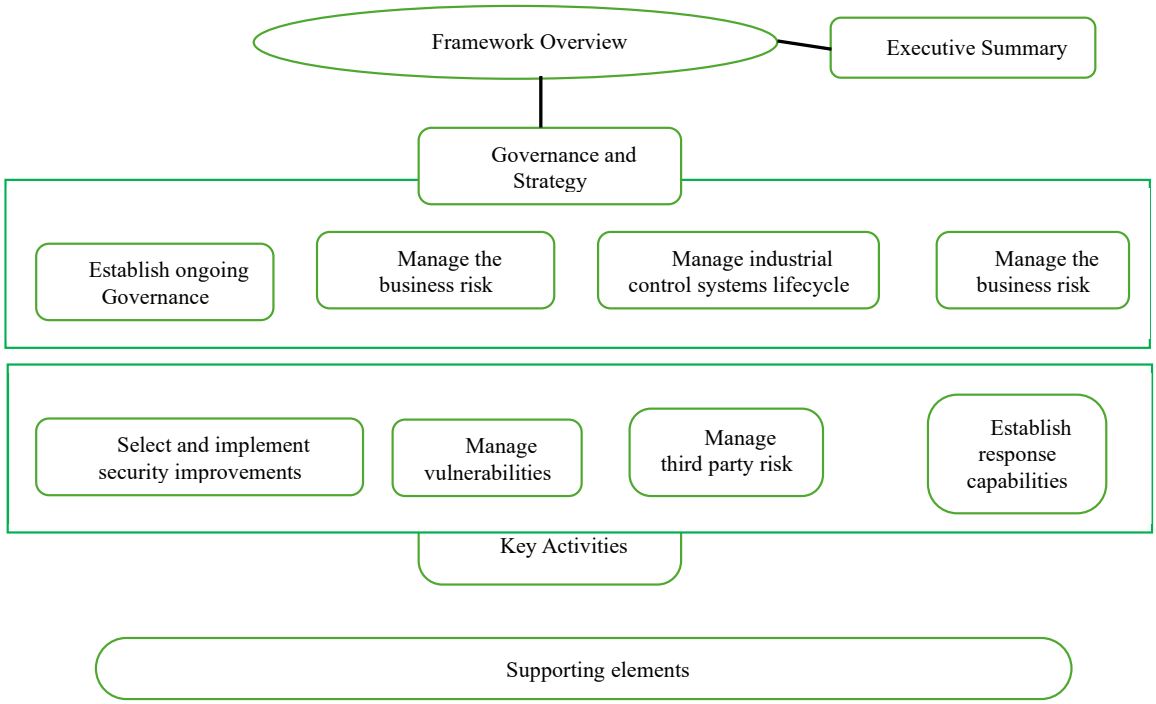

Fig. 1. Security of industrial control systems. source: Centre for the Protection of National Infrastructure [2]
Source: CPNI (2015)

Conceptual and theoretical frameworks.

This research draws on the traditional concept of construction project management, focusing on key elements of the project life cycle: project initiation, planning, execution, monitoring and control, closure, and documentation of lessons learned. **Fig. 2** describes the phases projects go through in building construction management. However, the system view of construction projects is the conceptual approach that underpins this research, considering these projects as complex systems with interconnected components, including people, materials, and processes. As shown in **Fig. 3**, the system view of construction management introduces myriad complexities, interconnectedness, and interdependencies among its various participants. A change in one area of the project is likely to have a significant impact on the other areas.

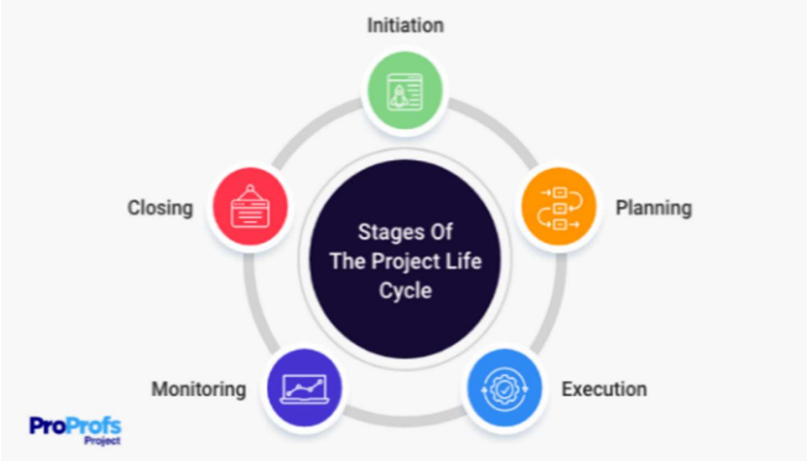

Fig. 2. Theoretical framework – construction project life cycle.
Source: Project Management Body of Knowledge (PMBOK) 2021 [20]

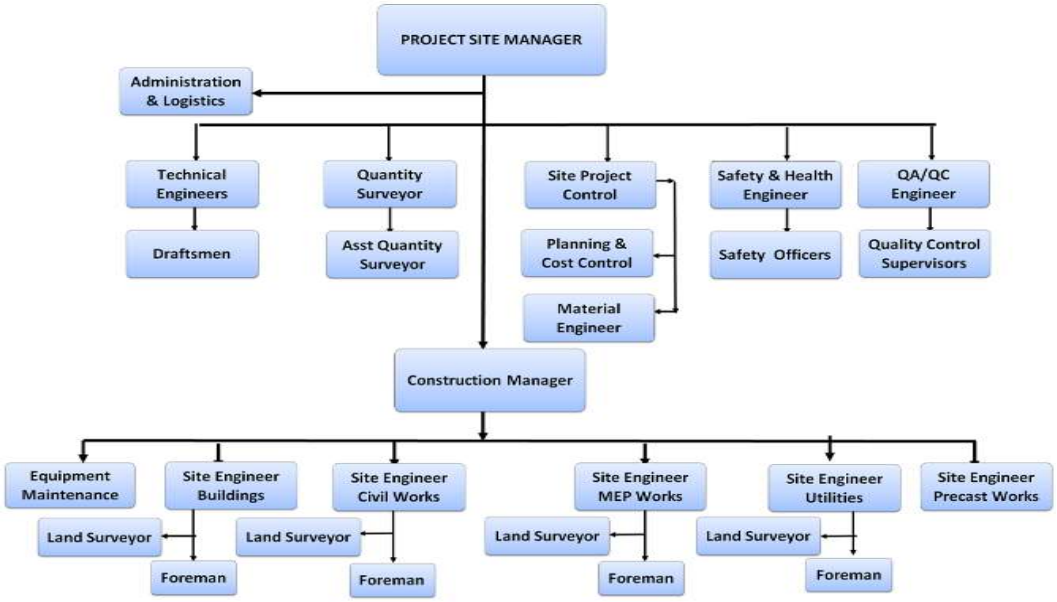

Fig. 3. A system view of building construction project management.
Source: Project Management Body of Knowledge (PMBOK) 2021 [20]

Protecting the information systems of these interconnected components of people, materials, and processes, as depicted from both the system view and project life cycle phases of construction projects, demands that it is possible to scrutinized the existing cybersecurity frameworks, such as NIST, ISO, and CIS controls and align them with the project management theoretical and conceptual frameworks. This is intended to secure civil infrastructure information systems. This will ensure holistic vulnerability management within the system, with a focus on the confidentiality, integrity, and availability of resources. **Fig. 4** provides insight into common information technology and cybersecurity frameworks that can protect the information systems of all businesses, including those in building information modelling.

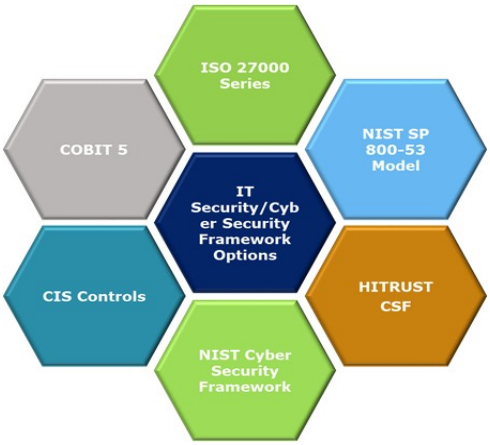

Fig. 4. Information systems and cyber security frameworks. Source: National Institute of Standards and Technology – Cyber Security Framework
Source: (NIST-CSF) 2024

COBIT 5 framework.

COBIT was developed by ISACA (Information Systems Audit and Control Association), formerly the IT Governance Institute (ITGI), to maximize the value of IT through balancing resource utilization, risk levels, and realization of benefits [13]. The COBIT 5 framework has been adopted in construction management software, such as BIM, with a focus on IT governance and the management of construction information systems [21]. According to [13], the framework is built

on five key principles for the effective governance and management of enterprise IT. According to [13], these include the following:

1) Meeting stakeholder needs: aligning IT goals with business objectives to deliver value.

2) Covering enterprise end-to-end: encompassing all IT functions and business areas.

3) Applying a single integrated framework: providing a common language for IT governance.

4) Activating a comprehensive methodology: effective governance fueled and powered by well-crafted policies, tactics, and structured strategies.

5) Draw the lines between governance and management: utilize governance to set directions and actionable accomplishment of programs by management.

COBIT 5, hence, encompasses governance and management structures that various industries relied on, including the architecture, engineering, and construction/facility management (AEC/FM domain, given the current emphasis on information systems for value generation and compliance obligations. [22] recalled how IT has become crucial in supporting, sustaining, and growing enterprises, with top management giving more attention to the direction of IT and its impact on overall organizational decision-making. Adhering to legal and regulatory compliance is synonymous with establishing and executing sound corporate governance structures.

ISO 27000 series framework.

[12] suggested using a security control baseline by selecting a compatible security framework, which is a collection of documented policies and procedures that define how to manage enterprise security. ISO 27000 series is one such framework that emphasizes organizational processes and best practices over specific controls. The framework explains how to implement an ISMS. It provides best practices and guidelines for managing the CIA of information [1]. [22] submitted that ISMS is based on how effectively an organization carries out its risk assessment and measures its risk tolerance levels to manage risks and vulnerabilities.

The motivation to adopt ISMS varies from organization to organization, but the central theme of the framework is the protection of the CIA triad of its data from unauthorized access [23]. The primary standard ISO 27001 outlines the requirements for establishing, implementing, maintaining, and improving an ISMS. Civil and building construction firms face growing cybersecurity threats and data breaches and implementing an ISMS helps them in protecting sensitive information, complying with regulations, and risk reduction [22]. Based on industry-specific needs, the adoption of the ISO 27000 series depends on several factors, including regulatory requirements, business size, and risk exposure [1]. [22] argued that sensitive industries like banking, finance, and audit face stricter compliance mandates and higher adoption rates for ISMS. Civil construction firms have a low adoption rate, but strict adherence to the CoP-CSBE can facilitate increased adoption.

However, implementing ISO 27001 poses challenges, as enumerated by [22]. These challenges include, but are not limited to, the following:

1) Cost and resource constraints: Small businesses may struggle with the costs of compliance.

2) Resistance to change: lack of imbibing change management concepts, as employees may find adoption of new technology services and security controls restrictive.

3) Complexity in implementation: Adapting ISO 27001 to existing business processes can be difficult.

4) Ongoing maintenance: organizations need continuous monitoring and improvement.

Despite the above challenges, the benefits of implementing the framework far outweigh the challenges. [12] highlighted, among others, enhanced data security and risk management, increased client trust and compliance with CoP, competitive advantage, and better internal security culture and employee awareness as the key benefits of implementing ISMS. Hence, successful ISMS implementation requires top management commitment, employee training, and continuous monitoring in order to bring the overall risks within an organization to tolerable levels.

NIST SP 800-53 Model.

NIST SP 800-53 is the preferred guidelines for Security and Privacy Controls for Information Systems and Organizations. The management of information security in the built environment encompasses various areas, including physical and network security, human resources security, and subcontractor and supplier management [24]. NIST SP 800-53 provides guidance on defining processes and procedures that an organization must deploy to assess, monitor, and mitigate cybersecurity risks, and to apply appropriate countermeasures to protect valuable information systems [25].

NIST SP 800-53 has found wide applicability within governmental organizations and contractors handling defense projects in the United States. However, compared to ISO/IEC 27001, it has a different set of security controls. A combination of these two sets of controls for both frameworks is sometimes desirable for certain organizations that serve dual purposes. Civil and building construction facilities fall into government and private infrastructure, depending on the goals for which they are constructed. **Table 1** depicts how ISO 27001 Annex A has changed from its first publication in 2005 to the latest version of 2013.

Based on the framework's specializations and breadth of coverage, it is possible to characterize existing major frameworks in terms of applicability, as shown in Fig. 5, with coverage breadth as the independent variable and specialization as the dependent variable. The breadth of coverage ranges from basic to comprehensive concepts, and the framework specialization varies from narrowly focused to broadly focused. NIST SP 800-53 appears to have wider specialization and more comprehensive coverage. However, ISO 27001 and 27002 seemed to have wider specialization but lower coverage than the NIST SP 800-53.

Table 1

Changes in Annex A of ISO 27001

–	ISO 27001:2005	Revised version of ISO 27001:2013
A.5	Security policy	Information security policies
A.6	Organization of information security	Organization of information security
A.7	Asset management	Human resources security
A.8	Human resources security	Asset management
A.9	Physical and environmental security	Access control
A.10	Communications and operations management	Cryptography
A.11	Access control	Physical and environmental security
A.12	IS acquisition, development and management	Operational security
A.13	Information security incident management	Communication security
A.14	Business continuity management	System acquisition, development and maintenance
A.15	Compliance	Supplier relationship
A.16	–	Information security incident management
A.17	–	Information security aspects of business continuity management
A.18	–	Compliance

Source: NIST (2024).

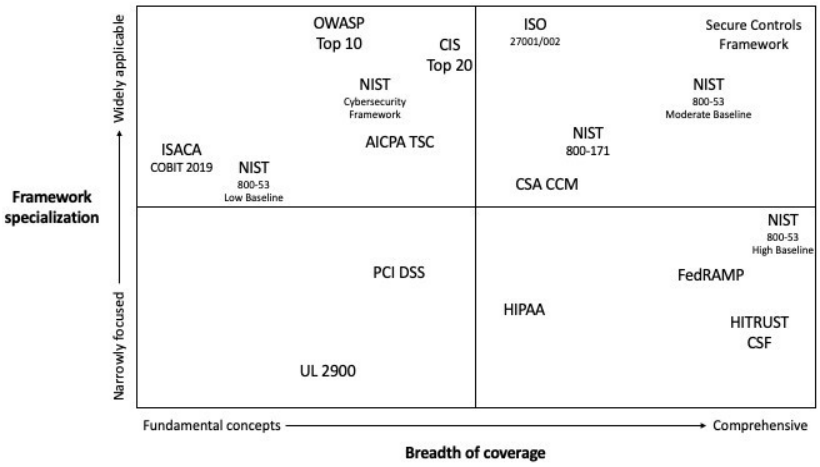

Fig. 5. Information security frameworks based on their specialization and coverage.
Source: National Institute of Standards and Technology – Cyber Security Framework Source: (NIST-CSF) 2024

Companies do not have to select either of these two frameworks and stick to it, nor is one better than the other. [24] opined that they are complementary and can be used within the same

organization. Part of ISO 27000 is certification, and the overall confidence level among clients and stakeholders is boosted when any given organization meets this requirement. The implication is that the organization in question follows information security best practices and delivers an independent, expert assessment of whether its valuable information and information assets are adequately protected [24]. For multi-functional organizations, such as building and civil construction firms that specialise in interconnected infrastructure systems, NIST SP 800-53 can be leveraged to strengthen areas that are missing or inadequately addressed by the ISO 27001 framework.

Table 2

Comparison between NIST SP 800-53 and ISO 27001

–	NIST	ISO
Description	A recognized framework that contains security and privacy controls for information systems and organizations to protect organizational operations and assets with the aim to effectively managing risk	An internationally recognized standard that describes how to manage information security in an organization
Target organizations	It was primarily created to help US federal agencies	Can be implemented in any kind of organization, profit or nonprofit, private or state-owned, small or large
Structure	Contains 1007 controls broken down into 20 control families	Annex A provides 14 control categories with 114 controls
Complexity	Is very detailed and technological in its nature	Less technological, with more emphasis on risk-based approach to managing security
Certification	Is voluntary and relies on self-assessment and self-compliance	Enables companies to become certified, relies on independent audit and certification bodies
Availability	Can be freely downloaded from official source	Distributed on the commercial basis through the official website

Source: Hamdi et al., (2019).

NIST cybersecurity framework (CSF).

NIST CSF has been proposed by the National Institute of Standards and Technology as guidance for organizations in the critical infrastructure Sector (NIST, 2014). The proposal aims to reduce cybersecurity risks within these sectors. The NIST CSF is hence also referred to as the NIST Cybersecurity Framework (CSF) for critical infrastructure. Most organizations prefer to select frameworks that perfectly align with their business processes to reap the maximum benefits. However, depending on the security baselines chosen or adopted, an implementation gap exists between the current and target states, as defined by the NIST CSF risk tiers [26].

The recommendation is to use the NIST CSF in conjunction with existing frameworks, such as COBIT 5, the ISO/IEC 27000 series, or the NIST 800 SP Series [27]. This highlights the NIST CSF's overarching nature compared to other frameworks. As previously noted, there is no one-size-fits-all framework for all organizations. The best standard practice is to use a combination of frameworks. However, it is highly desirable to deploy the NIST CSF by placing existing frameworks on top of it to identify implementation gaps within these frameworks [24]. Additionally, because the NIST CSF has been found not to be comprehensive enough to explain all information security-related processes a given organization might undertake, it is significant to identify implementation gaps in the NIST CSF with a view to closing them.

NIST CSF is a risk-based framework at the core of its undertakings. These endeavors are initially grouped into 98 subcategories, which are then grouped into 22 categories, otherwise known as control objectives [26]. Accordingly, these categories are themselves grouped into five functions: identify, protect, detect, respond, and recover. The functions are described diagrammatically in **Fig. 6** that include identification, protection, detection, response, and recovery. In addition to the core, NIST (2014) identified the profile and the implementation level as the other two key components of the framework. Currently, the core is divided into five risk management functions and 23 categories, grouped under these five functions, as described in **Fig. 7**. The profile encompasses the overall adjustments and priorities of activities and results for various sectoral industries, according to organizational needs [24]. The implementation level is key to an organization's measures of its position within the framework in terms of compliance and adoption levels.

These five functions are concurrent and continuous, and, when implemented together, provide a high-level, strategic view of an organization's security risk management program. Therefore, from a strategic viewpoint, the nature of NIST CSF according to [23] is:

1) focus on information security high-level requirements;

2) approach for their development of an information security program and policy.

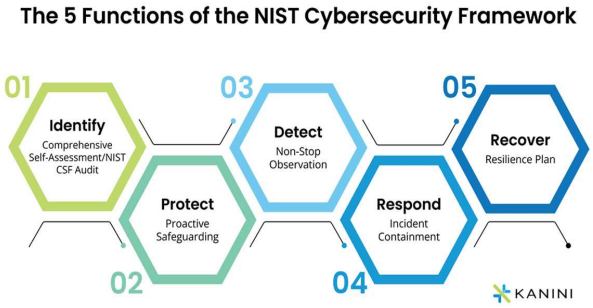

Fig. 6. The 5 functions of the NIST Cybersecurity Framework. Source: NIST (2024)

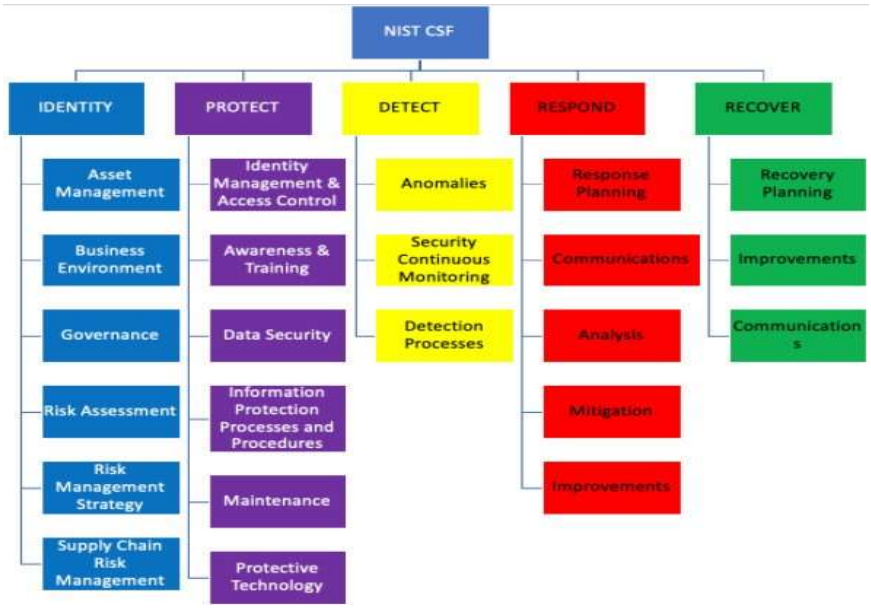

Fig. 7. Functions and categories of NIST CSF. Source: National Institute of Standards and Technology – Cyber Security Framework. Source: (NIST-CSF) 2024

According to [27], the five functions were defined as follows:

a) Identification: Development of complete knowledge about the cyber environment, particularly systems, assets, data, and capabilities;

b) protect: appropriate deployment and development to limit potential cybersecurity crash events;

c) detection: developing and implementing appropriate activities to identify cybersecurity events quickly;

d) respond: develop and implement appropriate activities to avoid the unwanted impact of cybersecurity events;

e) recovery: development and recovery activities to maintain resilience plans and restore capabilities that may be compromised by a cybersecurity incident.

The second nature defined above places NIST CSF in the category of policy frameworks, and thus, it represents a high-level statement from the top management of an organization.

Collaboration between NIST CSF and other frameworks.

The foregoing discussions positioned the NIST CSF at the policy formulation level from a strategic viewpoint. It follows that other frameworks, including COBIT 5, ISO/IEC 27000 series and NIST SP 800 Series, are based on standards, guidelines, and practices for which [23] defined their nature from the tactical viewpoint as:

1) focus on information security technical and function controls (customizable);

2) approaches for developing checklists and conducting compliance and audit assessments.

Guidelines, standards, and practices are key to the effective implementation of policies. A well-implemented policy enjoys the support of key components, including standards, guidelines, and best practices. This explains the relationship between NIST CSF and other frameworks. In addition, compliance assessment has been identified as a key component of the COBIT-5 and ISO/IEC 27000 series, but is not present in the NIST CSF [26]. For completeness and comprehensiveness, the compliance assessment is added to create 23 categories of control objectives in the NIST CSF. This category will have 4 subcategories or activities, namely:

– legal and regulatory compliance;

– information privacy;

– intellectual property;

– compliance with security policies and standards.

It is essential to briefly differentiate between policies, standards, guidelines, practices, and procedures. Policies are high-powered statements from the top management. Standards and guidelines are mandatory approaches to doing things. Practices are the accepted norms within a given organization, while procedures are optional but represent a step-by-step approach to accomplishing standards and guidelines.

[26] stated that compliance assessment has been addressed in NIST SP 800 Series under the risk monitoring process, including the roles and responsibilities associated with it. The main objectives of this subcategory are:

1) compliance: verifying the existence of the control put in place;

2) efficiency and effectiveness of control: ensuring the identified control to mitigate the risk is implemented correctly and operating as intended.

The updated categories or assessed areas are key to measuring the adoption levels of sound cybersecurity strategies from the standpoint of the security capability maturity model. **Table 3** presents the 23 assessed areas or categories of control objectives for the NIST CSF, along with the relevant civil and building construction activities that may be applicable to each category. The obvious fact is that leveraging NIST CSF with the ISO/IEC 27000 series could benefit the civil and building infrastructure sector more.

Table 3

The 23 control objectives for NIST CSF

S/N	Categories	Relevant civil and building construction activities
1	**2**	**3**
1	Asset management	Construction equipment and facilities, information systems, building information modelling (BIM)
2	Business environment	Consulting, contracting, and construction areas, interactions with various stakeholders and other organizations
3	Governance	Code of Practice in the built environment
4	Risk assessment	–
5	Risk management strategy	–
6	Compliance assessment	–
7	Access control	–
8	Awareness and training	–
9	Data security	–
10	Information protection processes and procedures	–
11	Maintenance	–
12	Protective technology	–
13	Anomalies and events	–

Continuation of Table 3

1	2	3
14	Security continuous monitoring	–
15	Detection processes	–
16	Response planning	–
17	Response communications	–
18	Response analysis	–
19	Response mitigation	–
20	Response Improvements	–
21	Recovery planning	–
22	Recovery improvements	–
23	Recovery communications	–

Source: Almuhammadi & Alsaleh (2018).

Corporate governance in civil and building construction management.

Corporate governance (CG) has significantly contributed to balancing social and economic goals from the perspectives of civil and building construction management [28]. The social goals focus on societal well-being and ethical responsibility. This encompasses social diversity and inclusion, while also ensuring environmental sustainability and community development. Whereas the focus of economic goals is on financial performance, profitability, and maximizing shareholders' value.

Therefore, incorporating CP into civil and building construction project management ensures that the infrastructure is safe, sustainable, and inclusive. [28] argued from the risk management perspective of building construction, that preventing project failure is about ensuring buildings meet the code of practice in the built environment. Therefore, it is often expedient to develop new strategies to manage risks and respond more quickly to a rapidly changing construction management landscape [29]. These strategies often revolve around internal rules that dictate and guide the allocation of rights and responsibilities to boards of directors, top management, stakeholders, and shareholders. The CG structure preserves and protects these shared rights and responsibilities, ensuring transparency and accountability through controlled decision-making processes, thereby preventing coercion within any corporate organization [30].

Within the domain of building and civil construction management, there is an overlap between social and economic goals. Therefore, project managers strive to ensure a balance. After all, building and civil engineering infrastructure endeavors are classified as social projects. In fact, economically viable projects from a cost-effective standpoint do support social goals, such as affordable housing [30]. Meanwhile, socially responsible designs, including green buildings, cultural centers, and cinemas, can attract economic incentives or higher market demand [31]. Additionally, effective construction management that prioritizes worker safety and compliance with environmental regulations can be a panacea for avoiding costly project delays or legal issues, thereby aligning with corporate economic objectives [29]. Hence, balancing social and economic goals ensures that projects are both financially sustainable and socially beneficial. This reflects the broader governance mandate to optimize services for multiple stakeholders, both efficiently and effectively.

Conceptual framework for establishing the ongoing governance.

The conceptual framework for CG in the domain of civil and building construction management integrates core principles, components, and concepts to align stakeholders' interests with the company's strategic objectives. Stakeholders of concern in the industry include shareholders, employees, clients, communities, and regulators, all of whom share roles and responsibilities. [31] argued in support of accountability as one of the key principles guiding effective CP. They submitted that construction companies must answer shareholders for their financial performance. They must also answer to the regulators for compliance with safety and environmental standards. Other principles of value include transparency, fairness, and responsibility.

The board of directors is responsible for the strategic oversight of the company, focusing on long-term planning and ensuring that projects align with both economic and social goals. An efficient CG framework is one that bridges the economic and social priorities of the project. **Fig. 8** depicts a CG framework that emphasizes the interplay between various components and stakeholders.

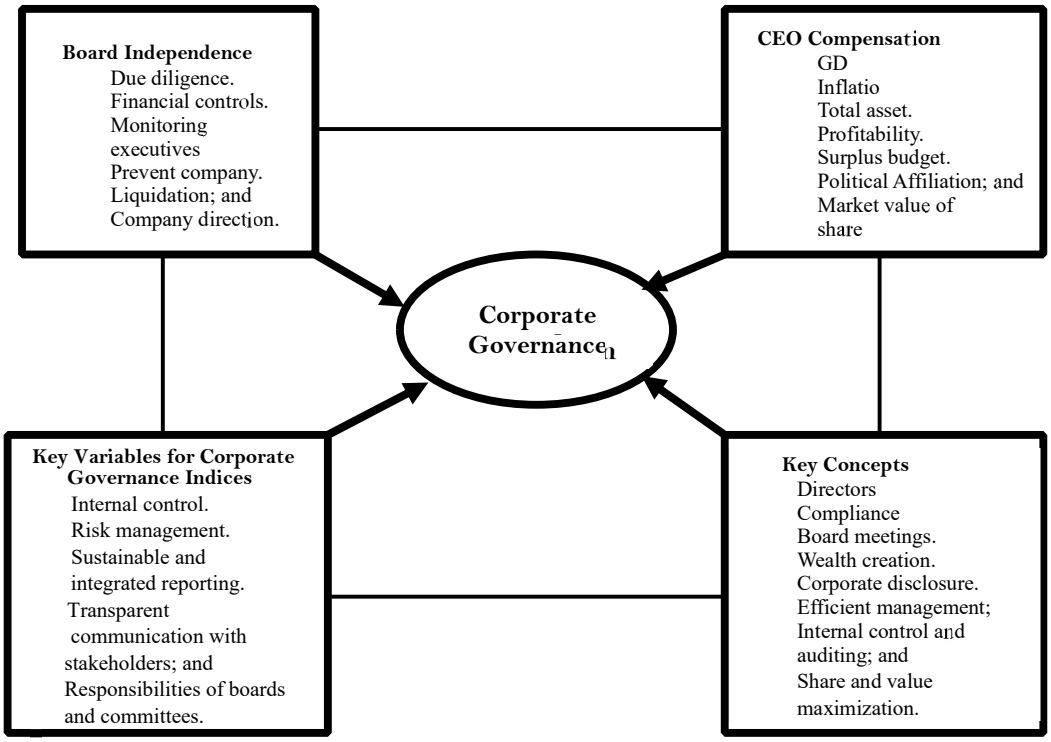

Fig. 8. Conceptual framework for corporate governance.
Source: Boateng *et al.* (2019).

Effective governance in the construction sector requires a bespoke strategy that addresses industry-specific complexities, including project lifecycles, intricate supply chains, and stringent regulations [29]. Implementing a successful governance structure requires a clear definition of roles, a formal charter, integrated ESG goals, and a diverse, skilled board committed to transparency and accountability [31]. To manage the inherent risks of construction projects, especially those involving extensive subcontracting and significant safety concerns, organizations must embed sound ethical principles, adopt robust risk management practices, and ensure contractual transparency [30].

Overview of construction project risk management.

The PMBOK (Project Management Body of Knowledge) enumerated the essential steps of project risk management (PMBOK, 2013). The first step in any comprehensive risk management process is to plan for risk management. This should be done as part of the construction project planning and continue throughout the project's duration, including maintenance, and at the end of its life. Planning risk management involves defining roles and responsibilities, identifying risk categories, and establishing procedures for risk identification, analysis, and response [32]. Considering categorizing construction project risks, the PMBOK did not prescribe specific categories to deploy but emphasized grouping risks by their attributes and characteristics to streamline analysis and response planning.

For civil and building construction, an attempt is made using a structured approach to categorize the business risks into six distinct groups as follows:

a) operation risks;
b) financial risks;
c) environmental risks;
d) regulatory and compliance risks;
e) stakeholder risks;
f) technical or technology risks.

When the identified risks are grouped into the above categories, it is bound to improve the efficiency and effectiveness of risk management processes.

Other key project risk management processes, in addition to plan risk management, include identifying risks, performing qualitative and quantitative risk analysis, planning risk responses, and monitoring and controlling risks. For context, managing business risks in civil and building construction project management involves a structured approach to identify, assess (qualitatively and quantitatively), and mitigate potential issues that could impact project success, while continually monitoring and controlling risks. The essential processes in civil and building construction project risk management are depicted in **Fig. 2.10.** The idea of maintaining a dynamic risk register to track identified risks, their status, and mitigation actions has been found helpful in various project, product, or process management endeavors. This has facilitated prompt and effective risk monitoring and control. Other strategies for monitoring and controlling risks in construction project management include regular reviews, contingency plans, and post-project analysis.

Managing the project lifecycle in the world of BIM.

BIM is a digital representation of a building's or infrastructure's physical and functional characteristics, facilitating collaboration among architects, engineers, contractors, and other stakeholders who work together to create comprehensive 3D virtual models of a project [10]. [19] stated that BIM has been researched as an intelligent, data-rich model that encompasses the entire lifecycle of a project, from conception and design to construction and demolition.

[14] demonstrated in a Chinese high-rise that integrating BIM and value engineering produced 10% savings in both cost and duration through enhanced design modifications, cost data extraction, and virtual evaluation of alternatives. [10], working across multiple case studies, found that BIM adoption resulted in approximately 20% faster project completion and 15% lower costs, while design errors decreased by 30% and RFIs (Requests for Information) declined by 25%, reflecting improved communication and coordination. [14] conducted a systematic review of the literature and found that BIM, when combined with methods such as lean construction, genetic algorithms, integrated project delivery, and value engineering, enhances cost control and estimation, leading to reduced timelines and budgets.

[14] in a Shanghai pilot project, BIM in MEP (mechanical, electrical, and plumbing) review and clash detection uncovered thousands of errors before construction – significantly reducing RFIs, rework, design changes, and improving coordination, scheduling, and cost management. BIM software is shaping the landscapes and skylines of tomorrow by revolutionizing project collaboration, saving time and cost, increasing safety and efficiency, reducing errors and making impossible ideas possible [33]

It is a groundbreaking innovation in architecture and engineering since the introduction of computers, and a game-changer in construction management [14]. It transforms the way to construct projects by providing a unified, data-rich, collaborative platform, paving the way for greater efficiency and cost-effectiveness in our building projects [33]. So, whenever to visualize an extremely impressive skyscraper, smart building, or an attractive piece of engineering infrastructure project, it is recognized that behind this piece of art and engineering façade lies the unbelievable power of BIM at work.

2. Methodology and methods

The purpose is to develop the most compatible security framework for BIM in civil infrastructure information systems (CIIS) from both information security and building construction management perspectives. For this reason, the existing literature in construction project management and information systems and security has been scrutinized with a view to synthesizing insights from these fields.

To further illustrate and characterize this, let's draw on the guidance offered by grounded theory in qualitative research. Such direction suggested adopting, adapting, and contextualizing existing models, theories, and frameworks to meet the objectives, with a view to possibly developing a completely new framework or modifying the existing ones. The research utilized secondary data from existing information systems security frameworks and construction domains.

3. Results and discussions

The core of this research is at the intersection of construction project management and information systems security. The work entails reviewing the existing general knowledge in the

public domain and focus group discussions with cybersecurity, civil, and construction management professionals within the following context:

BIM is the digital representation of a facility's physical and functional elements, widely used in construction for design, planning, and management. Building information modelling (BIM) in civil infrastructure is a critical asset due to complex data integration and is highly vulnerable to cyber threats.

Civil infrastructure information systems (CIIS) manage data across interconnected physical and digital environments, presenting unique security challenges. Effective security requires a dual focus on traditional information security principles (confidentiality, integrity, and availability) and construction management priorities (project delivery, stakeholder collaboration, and protection of shared design information). The significant societal impact of potential downtime or breaches in critical infrastructure necessitates robust governance and optimized information security strategies within construction management.

In terms of governance and strategy, the four key items needed from a seamlessly compatible framework are:

a) establishing ongoing governance;

b) managing the business risks;

c) managing construction project lifecycle;

d) improving awareness and skills by training and re-training.

Within the holistic risk management processes, it is pertinent to recognize the following four key activities which the proposed framework must support. The activities are:

a) selecting and implementing security improvements;

b) managing vulnerabilities in the assets;

c) managing third-party and supply chain risks;

d) establishing response capabilities.

3. 1. Existing cybersecurity frameworks

As no single framework meets all the criteria listed above, it is expedient to summarize the characteristics of existing frameworks in terms of their strengths and weaknesses. Some of the information security frameworks that featured in this review include the following:

1) NIST Cybersecurity Framework (CSF) 2.0 (2024) [34];

2) COBIT 5 (Control Objectives for Information and Related Technologies) 5 (2019) [35];

3) ISO/IEC 27001 – International Standard for Information Security Management Systems (ISMS) (2022);

4) (Cloud Security Alliance) – Security, Trust & Assurance Registry (CSA) STAR (2025) [36];

5) NERC CIP (North American Electric Reliability Corporation – Critical Infrastructure Protection) (2022) [37];

6) SABSA (Sherwood Applied Business Security Architecture) (2025) [38].

For application in construction and building information modelling (BIM) environments, particularly in critical information infrastructure security (CIIS), the six major frameworks are summarized by their strengths and weaknesses. Thus, multiple cybersecurity frameworks exist, including NIST, COBIT, ISO/IEC 27001, CSA STAR, NERC CIP, and SABSA, each offering unique strengths for risk management and governance. No single framework fully addresses the specific cybersecurity needs of the construction industry's civil infrastructure information systems (CIIS), requiring organizations to customize or supplement existing frameworks.

3. 2. Construction-specific security needs

Research confirms that integrating building information modelling (BIM) within civil infrastructure information systems (CIIS) introduces distinctive cybersecurity challenges spanning governance, regulatory compliance, and long-term strategy across both information security and project management domains.

It is possible to highlight some of these conundrums, which the developed framework in **Fig. 9** is meant to address:

Dynamic Processes: Construction involves overlapping organizational boundaries, with multiple stakeholders (e.g., architects, contractors, owners) accessing shared BIM models.

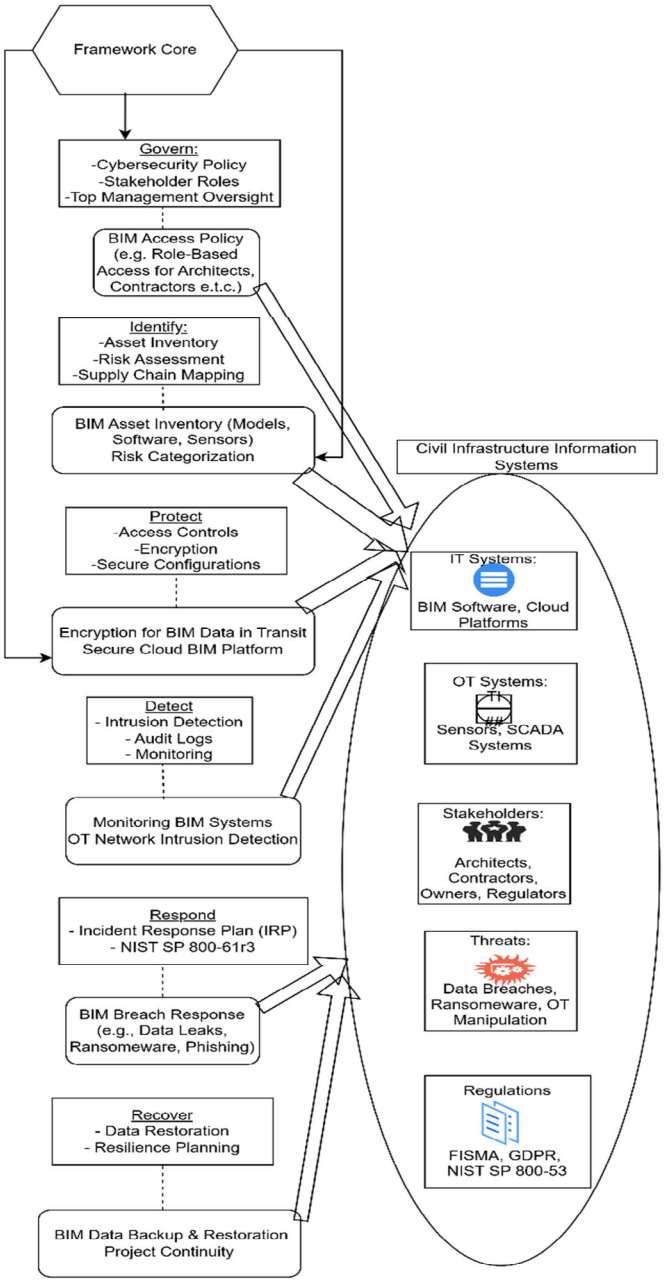

Fig. 9. Frameworks for securing BIM for CIIS. Security Framework. Research (2025)

Exposed Design Information: BIM models contain sensitive data (e.g., structural details of dams) that, if compromised, can lead to physical harm or national security risks.

OT-IT Integration: CIIS combines IT (e.g., BIM software) and OT (e.g., control systems for infrastructure), requiring a framework that bridges these domains.

Vulnerability of Control Information: Critical infrastructure relies on control data (e.g., sensor data), which is vulnerable to manipulation.

Regulatory Compliance: Construction firms must comply with standards such as FISMA (for U.S. federal projects) or GDPR (for EU projects), necessitating alignment with NIST or ISO standards.

Selection of the most compatible framework.

Relying on the foregoing evaluation, NIST-CSF 2.0 of 2024 is the most compatible security framework for BIM in CIIS for Nigeria and the entire construction world, for the following reasons:

1. Flexibility and Scalability: CSF 2.0 is adaptable to organizations of all sizes, from small construction firms to large infrastructure operators, unlike ISO 27001's resource-intensive requirements.

2. Comprehensive Scope: Covers governance, risk management, and supply chain security, addressing construction's dynamic stakeholder environment and CIIS's IT-OT integration.

3. Alignment with CIIS Needs: Designed for critical infrastructure, it supports risk categorization and continuous monitoring, crucial for protecting BIM data and control systems.

4. Industry Adoption: Widely used (e.g., Boise State University, U.K. Cyber Governance Code mapping), ensuring interoperability with other standards (e.g., NIST SP 800-53, FISMA).

5. Construction-Specific Fit: Its governance focus aligns with construction management's need for senior-level oversight, while its supply chain focus addresses multi-vendor challenges.

6. Support Resources: CSF 2.0 offers quick-start guides, profiles (e.g., incident response), and a searchable catalogue, easing implementation for construction firms with limited cybersecurity expertise.

While ISO 27001 and COBIT 5 are robust, they are less tailored to CIIS's OT-IT convergence and dynamic construction processes. SABSA is promising but requires additional tools for BIM integration. NERC CIP and CSA STAR are too sector specific.

3. 3. Customization for BIM in CIIS

To adapt and operationalize CSF 2.0 for BIM, it is customized and tailored it to address construction-specific risks based on the framework core of NIST CSF (Cybersecurity Framework) 2.0:

– govern: establish a cybersecurity policy for BIM access, defining roles for project managers, IT teams, and contractors. Ensure senior management oversees risk decisions;

– identify: inventory BIM assets (e.g., models, software, sensors) and categorize risks (e.g., structural data exposure, OT vulnerabilities). Map supply chain dependencies (e.g., third-party BIM platforms);

– protect: building access controls (e.g., role-based access for BIM models), encryption for data in transit, and secure cloud configurations for BIM platforms;

– detect: deploy monitoring tools for BIM systems (e.g., intrusion detection for OT networks) and audit logs for shared design data;

– respond: develop incident response plans for BIM breaches (e.g., data leaks, ransomware), leveraging NIST SP 800-61r3 guidelines;

– recover: plan for BIM data restoration and infrastructure resilience, ensuring minimal project delays.

Limitations of research. The research relied on secondary data from the existing cybersecurity frameworks. Primary data was not utilized in this report. A comprehensive review of relevant frameworks was undertaken to identify the best fit in terms of detail, elements, and comprehensiveness. As Mantha & García de Soto (2021) concluded that no existing cybersecurity standards are directly applicable to construction project life cycles. Their paper titled "Cybersecurity challenges and vulnerability assessment in the construction industry" presented a comprehensive study on cybersecurity risk within the context of the rapidly digitizing construction industry. Hence, this research is limited in that it relied on existing data and knowledge to develop a new cybersecurity framework for smart construction.

Prospects for further research. Further studies will continue in order to accomplish the remaining objectives. The UTAUT will be modelled to examine the constructs and variables that affect the deployment of sound cybersecurity concepts for securing civil infrastructure systems in building construction in Nigeria. This theory, along with TRA and TAM, has been utilized in previous research to develop the variables and measures for these determinants. The CMM (capability maturity model), informed by focus group discussions with key stakeholders, will be adapted to reflect the understanding of the levels of adoption of sound cybersecurity principles in securing civil infrastructure systems for building construction in Nigeria. Finally, to gain a deeper understanding of the risk management approaches and cultures of the participating organizations, the research may employ the concept of ethnography to intervene and participate as a member of the sample frame.

4. Conclusions

NIST-CSF 2.0 remains the most compatible and recommended security framework for BIM in CIIS, offering flexibility, scalability, and alignment with both information security and con-

struction management needs. The six functions can be customized to protect BIM assets, address IT-OT integration, and manage dynamic construction processes. The proposed diagram illustrates this customization, mapping NIST functions to BIM-specific measures within the CIIS context, providing a clear, actionable guide for implementation.

Conflict of interest

The authors declare that there is no conflict of interest in relation to this paper or the published research results, including financial aspects of conducting the research, obtaining and using its results, and any non-financial personal relationships.

Funding

The research was performed without financial support

Data availability

Data will be made available on reasonable request.

Use of artificial intelligence

Grok AI was primarily used to review existing cybersecurity frameworks. The AI model utilized was Grok-4.0, and the review was compared against standards including NIST-CSF, COBIT-5, and ISO/IEC 27001.

Acknowledgement

Obafemi Awolowo University and the University of Mpumalanga research office is acknowledged for providing an enabling environment for research and collaboration.

Authors' contributions

Bolaji Ajisegiri: Conceptualization, Methodology, Writing – original draft; **Gbojubola Binuyo:** Supervision, Visualization, Validation; **Oyebisi Oyeleye:** Investigation, Data curation, Formal analysis; **Christiana Kappo-Abidemi:** Writing – review and editing.

References

[1] Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, 4 (2), 92–100. https://doi.org/10.4236/jis.2013.42011

[2] CPNI (2015). Centre for the Protection of National Infrastructure.

[3] Hoehle, H., Huff, S. (2012). Electronic banking channels and task-channel fit. Paper presented at the Thirtieth International Conference on Information Systems. https://doi.org/10.1016/j.dss.2012.04.010

[4] Hoehle, H., Huff, S. (2009). Electronic Banking Channels and Task-Channel Fit (2009). ICIS 2009 Proceedings, 98. Available at: http://aisel.aisnet.org/icis2009/98

[5] Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13 (3), 319–340. https://doi.org/10.2307/249008

[6] Ajzen, I., Fishbein, M. (1980). Understanding Attitudes and Predicting Social Behaviour. Englewood Cliffs: Prentice-Hall.

[7] Rogers, E. M. (1983). Diffusion of innovations. New York: The Free Press, A Division of Macmillan Publishing Co., Inc.

[8] Davis, F. D., Bagozzi, R. P., Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. Management Science, 35 (8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

[9] Hale, J. L., Householder, B. J., Greene, K. L.; Dillard, J. P. Pfau. M. (Eds.) (2002). The Theory of Reasoned Action. The persuasion handbook: Developments in theory and practice. Thousand Oaks: Sage, 259–286. https://doi.org/10.4135/9781412976046.n14

[10] Venkatesh, V., Zhang, X. (2010). Unified Theory of Acceptance and Use of Technology: U.S. Vs. China. Journal of Global Information Technology Management, 13 (1), 5–27. https://doi.org/10.1080/1097198x.2010.10856507

[11] Abanda, F. H., Vidalakis, C., Oti, A. H., Tah, J. H. M. (2015). A critical analysis of Building Information Modelling systems used in construction projects. Advances in Engineering Software, 90, 183–201. https://doi.org/10.1016/j.advengsoft.2015.08.009

[12] Chapple, M., Stewart, J. M., Gibson, D. (2021). (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide. Sybex.

[13] Deane, A., Kraus, A. (2021). Certified Information Systems Security Professional (CISSP) – An (ISC)2 Certification. The Official (ISC)2 CISSP CBK Reference. Pub. Sybex.

[14] Harris, S., Maymi, F. (2022). All-in-One CISSP Exam Guide. Ninth. Certified Information Systems Security Professional Exam. McGraw-Hill.
[15] Li, C. Z., Guo, Z., Su, D., Xiao, B., Tam, V. W. Y. (2022). The Application of Advanced Information Technologies in Civil Infrastructure Construction and Maintenance. Sustainability, 14 (13), 7761. https://doi.org/10.3390/su14137761
[16] Rajaonah, B. (2017). A view of trust and information system security from the perspective of critical infrastructure protection. Ingénierie Des Systèmes d'information, 22 (1), 109–133. https://doi.org/10.3166/isi.22.1.109-133
[17] Saidabad, M. Y., Shaverdi, P., Mohammadiyeh, S. A., Parvin, B. G., Parvin, L. G. (2023). Cybersecurity and risk management in industrial and civil engineering systems. 13th International Conference on Mechanical, Construction, Industrial, & civil Engineering.
[18] Turk, Ž., García de Soto, B., Mantha, B. R. K., Maciel, A., Georgescu, A. (2022). A systemic framework for addressing cybersecurity in construction. Automation in Construction, 133, 103988. https://doi.org/10.1016/j.autcon.2021.103988
[19] Yang, Y., Ng, S. T., Xu, F. J., Skitmore, M., Zhou, S. (2019). Towards Resilient Civil Infrastructure Asset Management: An Information Elicitation and Analytical Framework. Sustainability, 11 (16), 4439. https://doi.org/10.3390/su11164439
[20] Zhu, J., Wright, G., Wang, J., Wang, X. (2018). A Critical Review of the Integration of Geographic Information System and Building Information Modelling at the Data Level. ISPRS International Journal of Geo-Information, 7 (2), 66. https://doi.org/10.3390/ijgi7020066
[21] Project Management Body of Knowledge (2021). PMBOK. Available at: https://tegnum.edu.pe/wp-content/uploads/2023/09/Project-Management-Institute-A-Guide-to-the-Project-Management-Body-of-Knowledge-PMBOK-R-Guide-PMBOK®%EF%B8%8F-Guide-Project-Management-Institute-2021.pdf
[22] De Haes, S., Van Grembergen, W., Debreceny, R. S. (2013). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. Journal of Information Systems, 27 (1), 307–324. https://doi.org/10.2308/isys-50422
[23] Hamdi, Z., Anir Norman, A., Nuha Abdul Molok, N., Hassandoust, F. (2019). A Comparative Review of ISMS Implementation Based on ISO 27000 Series in Organizations of Different Business Sectors. Journal of Physics: Conference Series, 1339 (1), 012103. https://doi.org/10.1088/1742-6596/1339/1/012103
[24] Azhari, F., Abdi, F., Shojaie, A. abbas. (2014). Using System Dynamics Method to Manage Construction and Demolition Waste. International Journal of System Dynamics Applications, 3 (4), 65–86. https://doi.org/10.4018/ijsda.2014100104
[25] Kurii, Y., Opirskyy, I. (2022). Analysis and comparison of the NIST SP 800-53 and ISO/IEC 27001. Cybersecurity Providing in Information and Telecommunication Systems 2022, CPITS-2022, 21–32
[26] Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards – A Review and Comprehensive Overview. Electronics, 11 (14), 2181. https://doi.org/10.3390/electronics11142181
[27] Almomani, I., Ahmed, M., Maglaras, L. (2021). Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. PeerJ Computer Science, 7, e703. https://doi.org/10.7717/peerj-cs.703
[28] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements (2022). International Organization for Standardization.
[29] Alzarooni, K. (2014). The challenges of corporate governance systems for construction project management. [Dissertation for the Master of Science; Project Management at the British University]. Available at: https://bspace.buid.ac.ae/items/84bb30ac-a626-4776-b500-aac6c4f5d708
[30] Henisz, W. J., Levitt, R. E. (2009). Normative and Cognitive Institutional Supports for Relational Contracting in Infrastructure Projects. [Unpublished manuscript].
[31] Ayuso, S., Argandoña, A. (2009). Responsible Corporate Governance: Towards a Stakeholder Board of Directors? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.1349090
[32] Boateng, F., Owusu-Manu, D., Adesi, M., Pawn, E., Edwards, D. J. (2019). Aligning strategic objectives to corporate governance objectives in a construction professional service firm. Journal of Construction Project Management and Innovation, 9 (1), 1–17.
[33] Richardson, G. L., Jackson, B. M. (2025). Project Management Theory and Practice. Auerbach Publications. https://doi.org/10.1201/9781003528920
[34] Park, J. K., Yang, S. J., Lehto, X (2007). Adoption of mobile technologies for Chinese consumers. Journal of Electronic Commerce Research, 8 (3), 196–206.
[35] National Institute of Standards and Technology (2024). Cybersecurity Framework 2.0.
[36] Control Objectives for Information and Related Technologies 5 (2019). Information Systems Audit and Control Association.
[37] Cloud Security Alliance – Security, Trust & Assurance Registry. Available at: https://cloudsecurityalliance.org/star/registry
[38] North American Electric Reliability Corporation – Critical Infrastructure Protection. Available at: https://www.tufin.com/solutions/nerc-cip
[39] Sherwood Applied Business Security Architecture. Available at: https://sabsa.org/