Global Academic Frontiers, Vol. 4, Issue 3, 2026, pp. 1-14 Print ISSN 2995-5688 Online ISSN 2995-570X
DOI: https://doi.org/10.5281/zenodo.22854580

An ISMS-Oriented Architecture for Intelligent Property Management Based on ISO/IEC 27001:2022

Xiaoxue Yang[1,*]

[1] Wuhan Vocational College of Software and Engineering, Wuhan, China
* Corresponding author Email: 48845987@qq.com
Received 13 September 2026; Accepted 18 September 2026; Published 20 September 2026
© 2026 The Author(s).This is an open access article under the CC BY license.

Abstract: The digital transformation of property management has led to the increasing integration of information technology (IT), operational technology (OT), and Internet of Things (IoT) devices. However, information security management in property enterprises is often separated from daily business processes and relies heavily on manual documentation, resulting in fragmented asset management, inefficient security control implementation, and difficulties in collecting and tracing audit evidence. To address these issues, this study proposes an Information Security Management System (ISMS)-oriented architecture for intelligent property management based on ISO/IEC 27001:2022. A standard – process – function mapping method is introduced to transform information security requirements into executable business workflows and system functions. The proposed architecture integrates asset and risk management, security control implementation, supplier and outsourcing management, incident response, audit evidence management, and security metrics within a unified framework. Particular attention is given to the integrated governance of IT, OT, and IoT assets and to the traceability of security activities throughout property management processes. A prototype system is further designed to demonstrate the implementation of the proposed architecture, and functional verification is used to examine its feasibility in typical property management scenarios. The proposed approach provides a systematic method for embedding ISMS requirements into intelligent property management systems and offers a practical reference for property enterprises seeking to improve security governance, audit readiness, and continuous improvement capabilities.

Keywords: Information Security Management System (ISMS); ISO/IEC 27001:2022; intelligent property management; information security governance; IT/OT/IoT integration; audit evidence

1. Introduction

Digital technologies have become an essential part of modern property management. Daily operations increasingly depend on interconnected platforms and devices for access control, video surveillance, parking management, energy monitoring, equipment maintenance, visitor services, and other routine activities. The growing use of Internet of Things (IoT) devices and building automation technologies has further extended the boundary of property information systems from conventional information technology (IT) infrastructure to operational technology (OT) and physical facilities. Similar changes have been observed in smart buildings, where connected sensors, automation systems, and management platforms are gradually replacing isolated building subsystems (Minoli et al., 2017; Kumar et al., 2021). While such integration improves operational efficiency, it also makes information security more difficult to manage.

The difficulty is not simply caused by an increasing number of connected devices. Property management has a particular organizational and operational structure. A property project may involve management personnel,

residents or tenants, equipment operators, external maintenance teams, security contractors, software vendors, and other service providers. These parties may access different systems at different times and for different purposes. Meanwhile, information assets are distributed across business applications, cloud services, network equipment, building automation systems, cameras, access-control terminals, and numerous IoT devices. The boundary between information systems and physical operations is therefore becoming less clear. Studies of building automation and intelligent-building environments have shown that increased connectivity expands the cyber-physical attack surface and introduces security, privacy, and interoperability concerns (Graveto et al., 2022; Li et al., 2023; Llaria et al., 2021).

ISO/IEC 27001 provides a systematic approach to managing information security risks. The 2022 edition specifies requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS) and places information security within an organizational risk-management process (ISO/IEC, 2022a). Supporting guidance in ISO/IEC 27002:2022 and ISO/IEC 27005:2022 further addresses information security controls and risk management (ISO/IEC, 2022b, 2022c). For property enterprises, this provides a useful basis for managing assets, access, suppliers, incidents, operational changes, and other security-related activities.

In practice, however, applying an ISMS to property management is not only a matter of adopting a set of security controls. A considerable amount of security management work is still performed through documents, spreadsheets, approval records, inspection forms, and manually collected evidence. Business systems may record work orders or equipment information, while security management records are maintained separately. As a result, a requirement defined by an ISMS may not have a direct and traceable relationship with the corresponding business process, responsible person, system function, and implementation evidence. This separation becomes particularly inconvenient during internal inspections, corrective actions, management reviews, and certification audits.

The problem is more evident when IT, OT, and IoT resources have to be governed within the same management environment. Existing smart-building research has examined IoT architectures, device connectivity, building automation, energy management, and cyberattack detection (Minoli et al., 2017; Kumar et al., 2021; Graveto et al., 2022). Research on building automation security has also focused on vulnerabilities, attack paths, detection, and resilient operation (Li et al., 2023). These studies provide important technical foundations, but a management question remains: how can information security requirements be translated into routine property-management activities that can be executed, recorded, traced, and reviewed within an information system?

This study approaches the problem from the perspective of system architecture rather than the design of an individual security algorithm. An ISMS-oriented architecture for intelligent property management is proposed based on ISO/IEC 27001:2022. At the center of the approach is a standard – process – function mapping method. Security requirements are associated with relevant property-management processes and then connected to system functions and operational records. In this way, activities such as asset registration, risk treatment, supplier assessment, incident handling, corrective action, and evidence collection can be managed as related parts of the same system instead of as independent compliance documents.

The proposed architecture also considers the mixed IT/OT/IoT environment commonly found in property operations. It organizes asset and risk management, security controls, supplier and outsourcing management, incident management, audit evidence, and security metrics within a unified structure. The intention is not to replace the ISMS itself, nor to introduce another independent security platform. Rather, the architecture provides a way to embed ISMS-related activities into existing property-management processes and to preserve the evidence generated during their execution.

The contribution of this study is mainly architectural and methodological. It adapts an ISMS-oriented architecture to property-management scenarios in which IT, OT, IoT, and outsourced services coexist, and uses a standard – process – function mapping method to connect security requirements with executable and traceable system activities. A prototype implementation is then used to examine whether the architecture can support

representative security-management tasks in practice. The purpose of this validation is functional feasibility rather than large-scale performance benchmarking.

2. Methods

2.1 Research Design

This study adopted an architecture-oriented design approach to investigate how the requirements of an Information Security Management System (ISMS) can be incorporated into intelligent property management. Rather than treating information security as an independent technical component, the research focused on the relationship between security requirements, routine management activities, and the information systems used to support these activities. ISO/IEC 27001:2022 was used as the principal reference for defining information security management requirements, with ISO/IEC 27002:2022 and ISO/IEC 27005:2022 providing complementary guidance on security controls and risk management (ISO/IEC, 2022a, 2022b, 2022c).

The research process combined standard analysis, scenario analysis, system modeling, and prototype implementation. Requirements related to information assets, risk treatment, access control, supplier relationships, incident management, operational activities, and audit evidence were examined in the context of typical property operations. These requirements were then translated into management processes and corresponding system functions. The resulting relationships formed the basis for the proposed architecture.

Property management was considered as a mixed digital and physical operating environment, consistent with the converged IT/OT/IoT characteristics widely reported in smart-building and building-automation environments (Minoli et al., 2017; Graveto et al., 2022; Li et al., 2023). In addition to conventional IT resources such as servers, databases, networks, and business applications, the scope included OT and IoT resources used in access control, video surveillance, parking management, building automation, energy monitoring, and equipment maintenance. External service providers and contractors were also included because outsourced maintenance and temporary system access are common in property operations.

The study therefore concentrates on architectural feasibility and functional integration. Prototype implementation is used to examine whether the proposed model can represent and connect typical security-management activities. It is not intended as a large-scale performance benchmark or an evaluation of a particular security algorithm.

2.2 Standard-Process-Function Mapping Method

A central problem in applying ISO/IEC 27001:2022 to property management is the distance between a management requirement and its actual execution. ISO/IEC 27002:2022 describes a broad set of information security controls, but organizations still need an implementation mechanism that connects those controls to operational processes and evidence (ISO/IEC, 2022b). A security requirement may be clearly documented at the organizational level, while its implementation is distributed across work orders, approval records, equipment platforms, spreadsheets, inspection records, and different departments. To reduce this separation, a standard-process-function mapping method was developed.

The method contains three connected layers. The standard layer describes information security requirements and controls relevant to the organization. The process layer identifies the operational or management activities through which a requirement is implemented. The function layer represents the information-system functions required to execute or record those activities. The relationship can be expressed conceptually as: Security requirement -> Management process -> System function -> Operational record/evidence.

The mapping is not necessarily one-to-one. A supplier-related security requirement, for example, may involve supplier qualification, contract review, authorization, maintenance activities, periodic evaluation, and termination of access. These activities can involve several system functions and generate different records. Conversely, an asset-

management function may support multiple security requirements because asset identification is relevant to risk assessment, access management, incident handling, and change management.

For each mapped item, several pieces of contextual information are maintained, including the related business scenario, responsible role, applicable asset or supplier, implementation status, and available evidence. This allows a control requirement to be followed from its management origin to its actual execution rather than being represented only by a policy document.

The same principle is applied to the Statement of Applicability (SoA), which in ISO/IEC 27001:2022 is used to document applicable controls and their implementation status (ISO/IEC, 2022a). Instead of treating the SoA as an isolated document prepared mainly for assessment, the proposed method associates applicable controls with their implementation processes, responsible roles, system records, and supporting evidence. Changes in implementation status can therefore be reflected in the corresponding management records.

Table 1. Example of the standard-process-function mapping

Security area	Property management process	Supporting system function	Typical evidence
Asset management	Asset registration and classification	Unified asset inventory	Asset record and change history
Access control	User and contractor authorization	Access approval workflow	Approval and authorization record
Supplier security	Supplier assessment and maintenance management	Supplier management	Assessment and service records
Incident management	Reporting, handling and closure	Incident workflow	Incident and corrective-action records
Change management	Equipment or system change	Change approval workflow	Approval and implementation record
Internal audit	Control review and evidence collection	Evidence management	Audit record and evidence package

2.3 Overall Architecture

The proposed architecture organizes information security activities around shared assets, risks, processes, and evidence. Its layered structure also reflects the need to coordinate technical and organizational security functions across heterogeneous building systems (Graveto et al., 2022; Li et al., 2023). It does not attempt to replace existing property business systems or device platforms. Instead, it provides a management layer through which security-related information from different operational domains can be organized and traced.

Five logical layers are used in the architecture: the asset and data layer, risk and control layer, process and workflow layer, evidence and audit layer, and metrics and decision layer.

The asset and data layer provides the basic objects used by the other layers. These include IT equipment, OT facilities, IoT devices, software systems, data resources, users, suppliers, and relevant organizational information. Existing property platforms can remain responsible for their original operational functions, while security-related attributes are referenced or recorded within the ISMS-oriented architecture.

Above this foundation, the risk and control layer links assets and operational scenarios with identified risks, treatment decisions, and applicable security controls. The process and workflow layer converts management activities into executable tasks. Approval, assessment, inspection, incident handling, corrective action, supplier review, and other activities can therefore be assigned to responsible roles and followed through their life cycles.

Evidence is generated during these activities rather than being collected only before an audit. The evidence and audit layer maintains the relationship among controls, tasks, records, documents, logs, and corrective actions. The upper metrics and decision layer summarizes implementation status and selected management indicators for review.

This layered organization is intended to preserve the relationship between management decisions and operational activities. A risk identified for a particular asset, for instance, can be associated with a treatment measure, a responsible person, an implementation task, and evidence of completion. The architecture therefore emphasizes traceability across layers rather than simply storing information in separate functional modules.The overall structure of the proposed ISMS-oriented intelligent property management system is illustrated in Fig. 1.

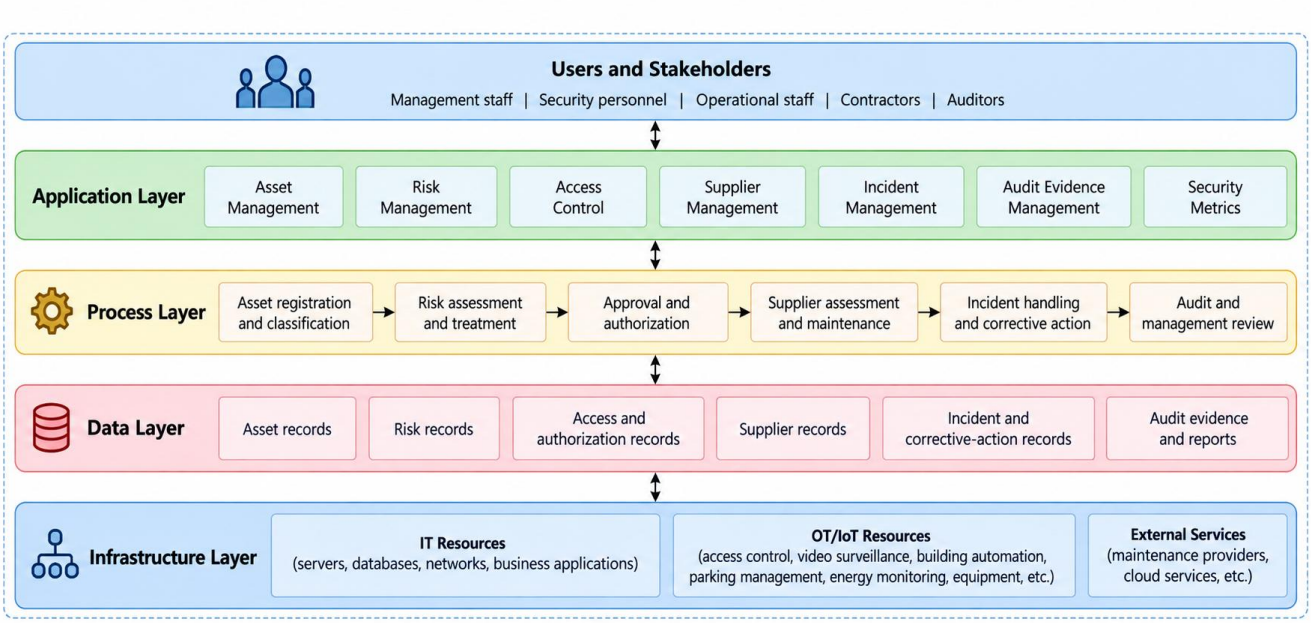


Fig. 1. Overall architecture of the proposed ISMS-oriented intelligent property management system.

2.4 Unified Asset and Risk Management

Asset identification provides the starting point for risk-based information security management and is closely related to the risk-identification and treatment principles described in ISO/IEC 27005:2022 (ISO/IEC, 2022c). In property environments, however, the asset inventory cannot be limited to computers and network equipment. Operational facilities and connected devices may affect both information security and physical services, while IoT and building-automation research has shown that these connected components expand both system functionality and attack surfaces (Minoli et al., 2017; Llaria et al., 2021; Graveto et al., 2022). Cameras, access-control terminals, parking devices, building controllers, environmental sensors, energy-management equipment, servers, applications, and cloud services may all participate in the same operational process.

The proposed architecture therefore uses a unified asset model while retaining the characteristics of different asset types. An asset record can contain its category, location, ownership or responsible department, operational status, network or system relationship, supplier information, and security-related attributes. Where relevant, relationships between assets are also maintained. This makes it possible to examine a risk not only at the level of an individual device but also in relation to the service or business process that depends on it.

Risk management is connected directly to these records. Identified risks are associated with relevant assets or processes and are recorded together with their treatment decisions, responsible roles, status, and related controls. The intention is to avoid maintaining a risk register that is disconnected from operational data.

When an asset is changed, transferred, replaced, or removed, its related security information can consequently be reviewed at the same time. This is particularly useful for property projects in which equipment and service providers change during long operating periods.

2.5 Workflow-Based Security Control Implementation

Some ISMS activities are technical, but many are organizational. This combination of organizational and technical controls is central to ISO/IEC 27001:2022 and ISO/IEC 27002:2022 (ISO/IEC, 2022a, 2022b). Training, authorization, supplier assessment, internal inspection, corrective action, emergency exercises, and management review all depend on people completing specific activities and leaving adequate records.

For this reason, workflow is used as a major implementation mechanism in the proposed architecture. A management requirement can be configured as a sequence of tasks involving initiation, assignment, approval, execution, verification, and closure, depending on the nature of the activity. Each task is associated with a responsible role and retains its status and relevant records.

Consider temporary access for an external maintenance engineer. The activity may begin with a maintenance request, followed by identity confirmation and authorization. Access is granted for a defined purpose and period, the maintenance activity is recorded, and authorization is subsequently withdrawn. From an operational perspective this is a normal maintenance procedure; from an ISMS perspective, it also provides evidence of supplier management and access control. The architecture treats these two views as parts of the same process.

Not every control requires a complex workflow. Simple controls may only require a status record, periodic confirmation, or evidence attachment. The implementation mechanism is selected according to the nature of the control rather than forcing all requirements into an identical process.

2.6 Supplier and Outsourcing Security Management

Outsourcing is especially relevant in property management. Supplier relationships and externally provided services are also recognized as important security-management concerns in ISO/IEC 27001:2022 and ISO/IEC 27002:2022 (ISO/IEC, 2022a, 2022b). Equipment maintenance, security services, cleaning, network support, elevator maintenance, parking systems, and specialized facility services may be provided by different external organizations. These suppliers can interact with physical facilities, information systems, or both.

Supplier security is therefore modeled as a life-cycle activity. Basic supplier information is linked with the services provided, relevant assets, responsible internal personnel, security requirements, assessment records, and access permissions. The architecture also records the period during which an external party requires access to a system or facility.

This approach is intended to address a common practical problem: authorization may be granted for legitimate maintenance work but remain active after the work has been completed. Linking access to a service activity and its validity period makes subsequent review and revocation easier to manage.

Supplier assessment records are retained in the same environment. When a supplier participates in multiple property projects, relevant assessment and security information can also be reused where organizational policy permits, reducing repeated collection of the same basic evidence.

2.7 Incident and Corrective-Action Management

Security incidents may originate from conventional information systems, connected devices, physical facilities, users, or external suppliers. In converged smart-building environments, this diversity of sources is one reason incident management must remain connected to asset and operational context (Graveto et al., 2022; Li et al., 2023). The proposed architecture uses a common incident record to maintain essential information about reporting, classification, assignment, handling, recovery, and closure.

Incident management is linked to assets and responsible roles. Supporting materials, handling records, and corrective actions can be attached to the incident as it progresses. Where an incident reveals a weakness in an existing control, a corrective action can be created and followed separately until completion.

The purpose of this design is not to implement a security information and event management platform or replace specialized detection technologies. Rather, it complements technical protection and detection mechanisms commonly discussed in IoT and building-security research by focusing on the management process that follows

(Bagaa et al., 2020; Kumar et al., 2021). Detection systems may continue to generate alarms and technical logs. The proposed architecture focuses on the management process that follows: who receives the issue, what action is taken, whether the problem is closed, and what evidence remains available for later review.

This distinction keeps the architecture applicable to property organizations with different technical infrastructures.

2.8 Evidence and Audit Traceability

Audit preparation can become labor-intensive when evidence is stored separately from the activities that produced it. Policies may be maintained in one location, approval records in another, device logs on individual platforms, and corrective actions in spreadsheets or communication records.

Evidence management in the proposed architecture is therefore process-oriented. Records generated during normal activities are associated with their corresponding processes and controls. Examples include approval records, supplier assessments, inspection results, incident records, corrective actions, training records, change histories, and system-generated logs.

A traceability chain can consequently be established: Control -> Process -> Task -> Responsible role -> Record -> Evidence.

The chain can also be followed in the opposite direction. An operational record can be traced back to the process and security requirement that caused it to be generated. This bidirectional relationship is useful when reviewing implementation status or preparing evidence for an internal or external audit.

Evidence validity also needs to be considered. Where appropriate, records include timestamps, responsible parties, status information, and change histories. The objective is not merely to increase the quantity of stored documents, but to make evidence understandable in its operational context.

2.9 Security Metrics and Continuous Improvement

The upper layer of the architecture provides a summarized view of security-management activities. This emphasis on governance and measurable improvement is consistent with the broader risk-management orientation of ISO/IEC 27001:2022 and the NIST Cybersecurity Framework 2.0 (ISO/IEC, 2022a; National Institute of Standards and Technology, 2024). Rather than defining a large number of indicators, the design focuses on measures that can be generated from operational processes and have a clear management meaning.

Examples include the number and status of unresolved risks, overdue corrective actions, supplier assessments, control implementation status, incident handling time, and completion of planned security activities. For incident management, commonly used measures such as Mean Time to Detect (MTTD) and Mean Time to Respond or Recover (MTTR) can be incorporated when the required timestamps are available.

Metrics are presented as management information rather than as independent performance objectives. A high closure rate, for example, does not by itself demonstrate effective security if issues are classified incorrectly or closed without adequate action. The dashboard is therefore intended to help managers locate exceptions and review trends while retaining access to the underlying records.

The architecture also supports a continuous improvement cycle, which is consistent with the continual-improvement principle embedded in ISO/IEC 27001:2022 (ISO/IEC, 2022a). Findings from incidents, audits, supplier assessments, or management reviews may generate corrective actions or adjustments to risk treatment. These changes return to the relevant processes and are subsequently recorded as new implementation evidence.

2.10 Prototype Implementation and Functional Verification

A prototype system was designed according to the architecture described above. Its purpose was to verify whether the proposed relationships among assets, risks, controls, workflows, suppliers, incidents, and evidence could be represented within an integrated information environment. The prototype was organized around functional modules corresponding to the major components of the architecture rather than around individual ISO/IEC 27001 clauses.

Verification focused on representative management scenarios. Typical tasks included registering and updating an asset, associating a risk with an asset, initiating an approval process, recording supplier-related activities, following an incident through handling and closure, and retrieving evidence associated with a management activity. For each scenario, the verification examined whether the required information could be entered, transferred between relevant functions, retained, and subsequently traced.

The verification was intentionally limited to functional feasibility. No attempt was made to use the prototype evaluation as a large-scale statistical comparison of security performance. This scope is consistent with the purpose of the study, which is to examine whether an ISMS-oriented architectural approach can translate information security management requirements into connected and traceable property-management activities.

Table 2. Functional verification design

Verification scenario	Main function examined	Verification focus
Asset registration and update	Asset management	Completeness and traceability of asset records
Risk identification and treatment	Risk management	Linkage among asset, risk, treatment and control
Contractor authorization	Workflow and supplier management	Authorization process and activity record
Security incident handling	Incident management	Assignment, handling, closure and retained evidence
Corrective action	Workflow management	Responsibility, status and closure tracking
Audit evidence retrieval	Evidence management	Traceability from control to supporting record

3. Results

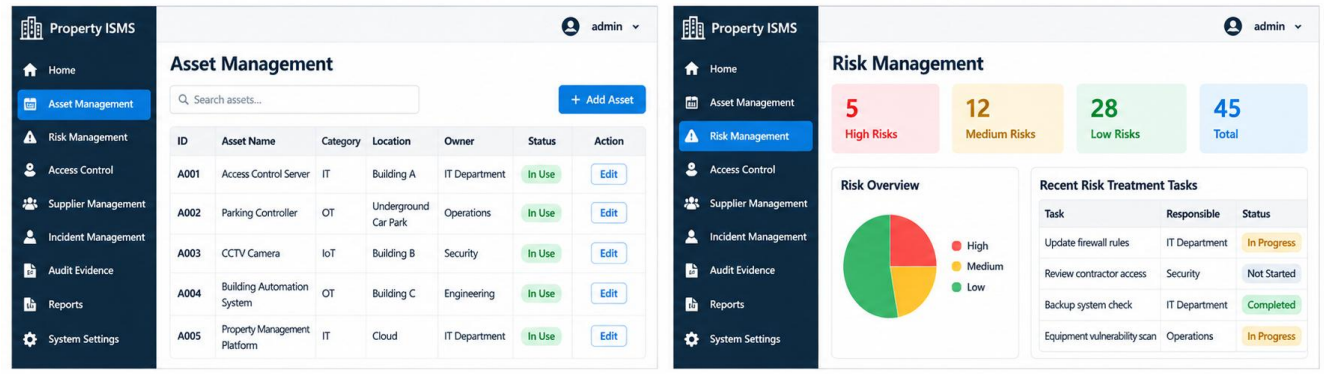
3.1 Prototype Realization

The prototype followed the architecture defined in Section 2 and was organized around a limited set of management functions rather than a large number of isolated ISO/IEC 27001 clauses. Asset and risk records, workflow-driven control activities, supplier and outsourcing management, incident and corrective-action handling, audit evidence, and management metrics were linked through shared identifiers and status records. In this way, the same asset, supplier, task, or incident could remain connected across several management activities.

A practical consequence of this arrangement is that security-related records do not need to exist as a separate document set. An asset entry can be associated with a risk item; the risk item can point to a treatment action; the treatment action can be assigned through a workflow; and the completion record can be retained as supporting evidence. The same logic applies to supplier access, incident handling, corrective actions, and periodic review. The prototype therefore represents the proposed standard-process-function mapping as connected operational records rather than as a static control checklist.

The interface design was intentionally simple. Functions were grouped according to the activities performed by users, including asset registration, risk handling, approval and review tasks, supplier records, incident tracking, evidence retrieval, and status overview. This reduces the need for users to understand the detailed structure of ISO/IEC 27001 before carrying out routine management work.

Fig. 2 presents representative interfaces of the prototype system, including the asset management and risk management modules. These interfaces illustrate how security-related information and management activities can be organized within the proposed architecture.



(a) Asset management interface

(b) Risk management dashboard

Fig. 2. Example interfaces of the prototype system.

3.2 Functional Verification

Functional verification examined whether typical property-management security activities could be represented as complete and traceable management paths. The focus was not algorithmic performance, but continuity: whether information could move from an operational event to the relevant control activity and then to a retained record.

Representative scenarios were selected from the processes described in Section 2. They included asset registration, risk treatment, contractor authorization, incident handling, corrective action, and audit evidence retrieval. For each scenario, the verification checked whether the relevant object could be created, connected to the responsible process, assigned to an appropriate role, updated during execution, and traced after completion. A contractor-authorization path, for example, was considered complete when the service request, identity information, approval, authorization period, activity record, and closure status could be followed as one chain. An audit-evidence path was considered complete when a reviewer could move from a control requirement to the related process, record, and stored evidence without relying on an unrelated document list.

3.3 Scenario-Based Results

The scenario-based review showed that different property-management activities can be handled through the same governance logic even when their operational starting points differ. Asset-related scenarios begin with an asset or risk record, while supplier and incident scenarios are triggered by service or event records. In both cases, the process ends with traceable records that can be associated with the relevant security requirement.

This is particularly useful in mixed IT/OT/IoT environments. A conventional server, an access-control terminal, a parking controller, or a building-automation device can be governed within the same management structure while retaining device-specific attributes. The architecture therefore separates the governance relationship from the technical details of individual platforms. Table 3 summarizes the main verification paths used in the initial prototype evaluation. The table is descriptive because the purpose of the present study is architectural feasibility rather than statistical comparison.

Table 3. Scenario-based functional verification of the proposed architecture

Scenario	Main functions involved	Traceability path	Verification focus
Asset registration and update	Asset management; risk management	Asset → risk → treatment → record	Whether changes remain linked and traceable
Contractor authorization	Supplier management; workflow management	Request → approval → authorization → activity →	Whether temporary access can be followed through its

Scenario	Main functions involved	Traceability path	Verification focus
		closure	life cycle
Security incident handling	Incident management; corrective action	Incident → assignment → handling → closure → evidence	Whether responsibility and handling records remain connected
Corrective action	Workflow management; evidence management	Finding → action → responsible role → verification → closure	Whether unresolved issues and closure evidence can be tracked
Audit evidence retrieval	Control mapping; evidence management	Control → process → record → evidence	Whether supporting evidence can be located from the control context

The verification paths were used only to check whether the architectural relationships could be represented and traced in the prototype. They were not treated as substitutes for long-term operational performance data.

3.4 Preliminary Internal Evaluation

The preliminary internal evaluation focused on usability and traceability. Particular attention was given to whether a user could identify responsibility, determine the current status of an activity, and retrieve the evidence generated during the process. The prototype supported these tasks across the representative scenarios described above, which was sufficient for an initial check of the proposed architecture.

This evaluation should nevertheless be interpreted cautiously. It does not provide long-term incident statistics, cross-site comparisons, or evidence of improved security performance over time. Those questions require a longer deployment period and a broader set of property-management environments. At the current stage, the result is limited to functional feasibility and traceability of the proposed management relationships.

4. Discussion

4.1 From Document-Based Compliance to Embedded Security Governance

The main value of the proposed architecture lies in the way it changes the position of information security within property management. In many organizations, ISMS activities are still handled as a parallel layer of work: policies are maintained separately, evidence is collected when an inspection approaches, and implementation status is often reconstructed from spreadsheets, email records, or individual business systems. Such an arrangement can satisfy documentation requirements, but it does not necessarily make security management part of normal operations. The architecture presented in this study addresses this gap by linking security requirements with operational processes and the system functions that support them, consistent with the process-based and continual-improvement orientation of ISO/IEC 27001:2022 (ISO/IEC, 2022a).

The standard–process–function mapping is especially important in this respect. A control requirement becomes more useful when it can be connected to an identifiable activity, a responsible role, and a record created during execution. The practical effect is modest but important: compliance information is no longer produced only for review. It becomes a by-product of routine work. An approval record, a supplier assessment, an incident closure record, or a change history can serve an operational purpose and, at the same time, provide evidence that a control has actually been performed.

This approach also changes the timing of audit preparation. Under a document-centered model, evidence may be collected retrospectively and its relationship to the original control has to be explained again. In the proposed architecture, the relationship is established earlier, when the process is configured and performed. This does not remove the need for human judgment. It does, however, reduce the amount of interpretation needed later to

determine who performed an activity, when it occurred, which asset or supplier it concerned, and whether corrective action was completed.

The distinction is relevant for property enterprises because their operating environment contains many repetitive but distributed activities. Access authorization, maintenance work, supplier entry, equipment changes, incident handling, and routine inspections occur continuously and are often managed by different departments. Embedding security requirements into these activities is more sustainable than asking staff to maintain a second, disconnected set of compliance records.

4.2 Integrated Governance of IT, OT, and IoT in Property Operations

Property management differs from a conventional office IT environment because operational services depend on a mixture of digital and physical systems. A resident application may interact with access control; parking services may depend on cameras, controllers, payment platforms, and network connections; equipment maintenance may require temporary access to a building automation platform. The security boundary is therefore difficult to define if IT assets, operational equipment, and IoT devices are managed independently, a challenge also identified in research on smart-building and building-automation security (Minoli et al., 2017; Graveto et al., 2022; Li et al., 2023).

The unified asset and risk view proposed in this study is intended to deal with this overlap. It does not assume that every device should be managed in exactly the same way. A camera, a database server, and a building controller have different operational characteristics and different consequences of failure. What they share is the need to be identified, linked to a responsible party, placed in an operational context, and considered when risks or changes are reviewed. Maintaining these relationships is more useful than forcing heterogeneous assets into a single technical classification.

This point becomes particularly visible in outsourcing scenarios. A maintenance contractor may need access to an OT platform but receive credentials through an IT account-management process. The work may concern a physical device while the evidence of authorization is stored in a business system. If these records remain separated, the organization has to reconstruct the relationship later. A common governance layer allows the activity to be viewed as one event with several technical components rather than as unrelated records.

The architecture therefore treats IT/OT/IoT integration primarily as a governance problem. Specialized security tools remain necessary for technical detection, monitoring, and device protection (Bagaa et al., 2020), but those tools do not by themselves establish responsibility, approval, treatment decisions, or evidence continuity. The proposed model is designed to sit above such technical mechanisms and connect them to management processes.

4.3 Practical Implications for Property Enterprises

The proposed architecture is most useful in organizations where security responsibilities are spread across several projects, departments, and external service providers. In these environments, the difficulty is often not the absence of security rules but the loss of context between a rule and the activity that should implement it. A structured mapping can make that context visible.

For day-to-day management, the architecture can support a clearer division of responsibility. Risks are attached to assets or processes, workflow tasks are assigned to named roles, supplier activities are linked to service periods, and corrective actions retain their own status until closure. Managers can therefore review outstanding work without relying entirely on informal follow-up. The same structure can also reduce repeated evidence collection. Where an operational record already contains the required information and can be traced to the relevant control, it can be reused for internal review or audit preparation rather than being reproduced in a separate format.

Multi-site organizations may benefit in a different way. Property companies often operate projects with similar business functions but different local equipment, suppliers, and staffing arrangements. A reusable process template

can provide a common control logic while still allowing local parameters to vary. This is particularly relevant to supplier review, temporary authorization, incident handling, routine inspection, and corrective-action workflows, which tend to recur across sites even when the underlying devices are different.

The model should not be understood as a claim that information security can be fully automated. Decisions about risk acceptance, control applicability, incident severity, or supplier suitability still require professional judgment. The contribution of the architecture is narrower: it provides a place where those decisions, their execution, and their supporting records can remain connected.

4.4 Limitations and Future Work

The present study is intentionally limited in scope. Its primary objective is to develop and examine an ISMS-oriented architecture rather than to establish statistical evidence of long-term performance improvement. The prototype and functional verification show how the proposed relationships can be implemented, but they do not demonstrate how the system will behave across a large number of property projects, organizations, or technology platforms over extended periods.

Several practical issues also require further investigation. Property environments contain heterogeneous OT and IoT devices, and the availability and quality of device interfaces vary substantially. Integration with legacy equipment may therefore require gateway services, manual data entry, or project-specific adapters. Data ownership and confidentiality may place additional limits on centralized evidence collection, especially when information is shared between a property enterprise and external contractors; related privacy and security concerns have also been reported for intelligent-building environments (Llaria et al., 2021).

Future work should extend the architecture in two directions. Broader deployment can be used to examine whether the proposed mapping remains manageable when the number of sites, suppliers, controls, and assets increases. Longitudinal evaluation would also allow more meaningful measurement of operational indicators such as audit preparation workload, corrective-action closure time, incident handling time, and repeated evidence reuse. These measures would be more informative after the architecture has been used through several normal operating and review cycles, rather than being estimated from a short prototype exercise.

A second area concerns interoperability. Further implementation work can explore standardized interfaces with building automation platforms, access-control systems, ticketing tools, log-management systems, and supplier portals. The architecture is intended to remain independent of a particular technology stack; testing that assumption across heterogeneous environments will be necessary before broader deployment can be recommended.

5. Conclusions

This study examined how the requirements of ISO/IEC 27001:2022 can be incorporated into intelligent property management without being separated from routine operations. The proposed ISMS-oriented architecture was developed for an environment in which conventional IT resources coexist with OT equipment, IoT devices, outsourced maintenance, and multiple operational roles. Its central idea is to connect security requirements with the processes through which they are carried out and with the system functions that record those activities. In this way, information security is treated as part of property management rather than as an additional set of documents prepared mainly for inspection.

The standard–process–function mapping provides the main methodological link in the architecture. It allows a control requirement to be associated with an operational process, a responsible role, and the records created during execution. On this basis, the architecture brings asset and risk management, supplier activities, access authorization, incident handling, corrective action, audit evidence, and management metrics into a common

structure. The value of the approach does not depend on introducing a new security algorithm. It lies in making existing management requirements easier to execute and trace across a mixed IT/OT/IoT environment. The prototype implementation further shows that these relationships can be represented through connected records and workflow-supported activities rather than through isolated control checklists.

The functional verification conducted in this work was intentionally limited in scope. It was used to determine whether representative management paths could be completed and traced within the prototype, not to establish a quantified improvement in organizational security performance. The results therefore support the feasibility of the architectural approach, while broader claims would require longer-term operational evidence.

Further work should focus on deployment in additional property projects and on integration with heterogeneous building and device platforms. Longitudinal use would also make it possible to examine whether the proposed approach reduces audit preparation effort, improves corrective-action follow-up, or changes incident-response efficiency over time. Such evaluation would complement the present architecture-centered study and provide a clearer view of how an embedded ISMS can operate across different property-management environments.

Acknowledgements

This work was supported by the 2025 Scientific Research Project of Wuhan Vocational College of Software and Engineering (Project No. SEA2025006).

Conflicts of Interest

The author declares no conflict of interest.

Data Availability

The data generated during the functional verification of the prototype are not publicly available because they contain internal system and operational information. Further information may be available from the corresponding author upon reasonable request.

References

[1] Affia, A. O., Nolte, A., & Matulevičius, R. (2023). IoT security risk management: A framework and teaching approach. Informatics in Education, 22(4), 555–588. https://doi.org/10.15388/infedu.2023.30

[2] Bagaa, M., Taleb, T., Bernabe, J. B., & Skarmeta, A. (2020). A machine learning security framework for IoT systems. IEEE Access, 8, 114066–114077. https://doi.org/10.1109/ACCESS.2020.2996214

[3] Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). IoT device cybersecurity capability core baseline (NISTIR 8259A). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8259A

[4] Graveto, V., Cruz, T., & Simões, P. (2022). Security of building automation and control systems: Survey and future research directions. Computers & Security, 112, 102527. https://doi.org/10.1016/j.cose.2021.102527

[5] International Electrotechnical Commission. (n.d.). IEC 62443 series: Security for industrial automation and control systems.

[6] International Organization for Standardization & International Electrotechnical Commission. (2022a). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements. ISO.

[7] International Organization for Standardization & International Electrotechnical Commission. (2022b). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection—Information security controls. ISO.

[8] International Organization for Standardization & International Electrotechnical Commission. (2022c). ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection—Guidance on managing information security risks. ISO.

[9] Kumar, A., Sharma, S., Goyal, N., Singh, A., Cheng, X., & Singh, P. (2021). Secure and energy-efficient smart building architecture with emerging technology IoT. Computer Communications, 176, 207–217. https://doi.org/10.1016/j.comcom.2021.06.003

[10] Li, G., Ren, L., Fu, Y., Yang, Z., Adetola, V., Wen, J., Zhu, Q., Wu, T., Candan, K. S., & O'Neill, Z. (2023). A critical review of cyber-physical security for building automation systems. Annual Reviews in Control, 55, 237–254. https://doi.org/10.1016/j.arcontrol.2023.02.004

[11] Llaria, A., Dos Santos, J., Terrasson, G., Boussaada, Z., Merlo, C., & Curea, O. (2021). Intelligent buildings in smart grids: A survey on security and privacy issues related to energy management. Energies, 14(9), 2733. https://doi.org/10.3390/en14092733

[12] Minoli, D., Sohraby, K., & Occhiogrosso, B. (2017). IoT considerations, requirements, and architectures for smart buildings—Energy optimization and next-generation building management systems. IEEE Internet of Things Journal, 4(1), 269–283. https://doi.org/10.1109/JIOT.2017.2647881

[13] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology.

[14] Qureshi, A., Afaqui, M. S. I., & Salas, J. (2021). IoTFC: A secure and privacy preserving architecture for smart buildings. In D. Wang, W. Meng, & J. Han (Eds.), Security and privacy in new computing environments (pp. 102–119). Springer. https://doi.org/10.1007/978-3-030-66922-5_7

[15] Wendzel, S., Tonejc, J., Kaur, J., & Kobekova, A. (2018). Cyber security of smart buildings. In H. Song, G. Fink, & S. Jeschke (Eds.), Security and privacy in cyber-physical systems: Foundations, principles, and applications. Wiley. https://doi.org/10.1002/9781119226079.ch16