Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Mobile-Web Platform for Private Security Workforce Onboarding, Job Allocation, Attendance Verification, and Compliance Management

Wajahat Murtaza[1]
[1]VIGILOX Limited; info@vigilox.co.uk

ARTICLE INFO

Received: 04 Nov 2025

Revised: 25 Dec 2025

Accepted: 04 Jan 2026

ABSTRACT

Introduction: The tools used in staffing, rostering, attendance monitoring, and licensing compliance are usually fragmented and this makes visibility across deployments low and payroll conflict and compliance risks high. This paper introduces VigiloX which is an end-to-end mobile-web application that brings together guard onboarding and verification, job posting and assignment, roster assignment, evidence-based attendance (geographically contextual and photographic), and audit compliance records. We employ a design science research approach to come up with a domain-specific workflow model of guarding operations and traceability-by-design data model, which connects job slots, guard identities, attendance events, and compliance artefacts across modules. The artefact was tested at a module level with functional test cases and end-to-end workflow scenario, such as job posting and approvals, all the way to check-in/out and payroll-ready time summaries. The findings indicate that VigiloX is capable of sustaining integrated workforce security operations and enhancing the auditability and downstream payroll and reporting preparedness.

Objectives: To present VigiloX as an integrated, auditable platform for private security workforce operations and to propose a domain-specific workflow and traceability-by-design data model.

Methods: Design science research with iterative build–evaluate sprints; requirements mapping and modular decomposition; implementation with role-based access and shared data entities; functional and end-to-end scenario validation.
Results: The platform supported end-to-end workflows from job posting and approvals through attendance evidence capture and payroll-ready summaries; scenario tests and stakeholder walk-throughs indicated consistent traceability across modules.
Conclusions: Integrating onboarding, rostering, attendance and compliance in a single platform improves auditability and reduces ambiguity created by fragmented tools.
Keywords: private security, workforce management, attendance verification, GPS/photo check-in, role-based access control, compliance, mobile application.

INTRODUCTION

The security activities of a private nature are usually based on the geographical distribution of employees, shifts, and time constraints and strict customer demands. Practically, staffing and timekeeping are frequently handled in other sets of tools (e.g., messaging applications, spreadsheets, and manual sign-in sheets), which makes assignment of staff to a particular place visible and attendance checking difficult. These deficiencies are also typical in the broader literature on mobile attendance systems, with the traditional/manual methods being reported as prone to inaccuracies inaccuracies and being time-intensive, particularly when a large number of people need to be monitored in multiple sessions or locations or when workers are located in several different locations (Nordin and Fauzi 2020).

All these situations lead to operational recurrent problems: (i) sluggish onboarding and documenting, (ii) low levels of recognisability of the guard who will be assigned to a particular place and slot, (iii) disagreements about modifications in the attendance including breaks and working hours, and (iv) lack of traceability of licensing and verification documentation. Previous systems have addressed a part of this problem with smartphone-based attendance that integrates identity authenticating with location tracking (e.g., fingerprint and GPS), which shows that an identity check linked with location reporting can reduce human error and increase monitoring strength (Soewito et al. 2015). In the meantime, mobile job sites emphasise the benefits of organised job posting, application processes, and in-app communication to facilitate distributed workforces through formalisation of matching and minimised ad-hoc arrangements (Asa et al. 2023).

VigiloX has been developed to align these processes on a single platform that connects employment creation and guard matching, approvals, assignment to a roster, trusted capture of attendance, and compliance records which are auditable. The paper suggests a domain specific workflow model of guarding operations, a reference architecture of a mobile-web implementation and a validation of the architecture that was done in terms of functional validation and scenario validation. Section 2 describes the methodology, Section 3 describes the system design and architecture, Section 4 presents main modules and implementation, Section 5 the conclusions and reports about the results and observations and the last part of the paper is described in Section 6 future work.

Contributions and novelty: There are three contributions of this work. To begin with, it suggests a domain-specific workflow architecture of private security operations that will combine the onboarding, job distribution, attendance checking, and compliance control into one operational cycle. Second, it proposes a traceability-by-design data model where the entities of job slots, guard identities, attendance evidence and compliance artefacts are explicitly connected, which allows end-to-end auditability across modules. Third, it illustrates that evidence-based attendance capture may be systemically linked with states of licensing and verification in order to assist in administration and decrease administrative conflicts. Combined, these contributions widen the current workforce management practices to incorporate accountability and compliance into operational processes.

METHODOLOGY

The design-science research (DSR) approach was used and focused on design, development, and testing of an artefact to solve a real-life organisational issue in private security operations (Holopainen et al. 2020). The implementation process was in iterative sprints, which involved building and evaluating the artefact, which is in line with the known logic of DSR build-evaluate (Hevner et al. 2024). There were four steps in the research process:

2.1 Elaboration of the requirements and workflow mapping

The three main user roles (guards, clients/admins, and subcontractors) were first identified and what each of the groups required of the system was figured out. With those needs, we have captured the complete flow of operation starting to the end: onboarding and identity checks, job creation and applications, shift approval and rostering, attendance capture, and, lastly, dashboards and reports to monitor and support payroll.

2.2 System decomposition

The functional requirements were subdivided into the following modules: Authentication and profiles, Jobs and applications, Approval, Roster, Attendance, Messaging and SOS, licensing and verification, and Payroll-ready time summaries.

2.3 Implementation approach

Role-based permissions and a common data model were used to implement modules so that traceability could be made between a job slot, an assigned guard and attendance evidence. Established principles of data minimisation, integrity/confidentiality, and accountability were taken into consideration as security and privacy controls.

2.4 Validation

The platform was tested with (i) module-level functional (CRUD, permissions, edge cases) and (ii) scenario-based testing (posting a job, approving applicants, assigning slots, check-in/out, and generating summaries) testing.

SYSTEM ARCHITECTURE AND DESIGN

VigiloX is designed as a multi-purpose workforce system, comprising three interlinked components: (a) a mobile app used by guards, (b) a web dashboard by clients and administrators and (c) a set of services handled by the backend and managing identity records and job and roster assignments, attendance and timecard evidence, and notifications.

This system will ensure that there is end to end traceability. Practically, it implies that all attendance records will be linked to a certain guard profile and a certain job slot, which will leave a trail that can be audited to facilitate operational control and reporting. Unlike generic workforce platforms, the proposed architecture is developed according to a security-specific operational lifecycle in which traceability between assignments, personnel and compliance artefacts is enforced at data-model level and not at an afterthought level.

3.1 Roles and access control

Robust role-based invitations of the access. Guards are able to see and apply to available jobs and turn in attendance. Clients and administrators are able to post job, check applications, deny or accept applications, allocate rosters and track attendance and compliance data. Subcontractor functionality is restricted to the tasks that role is meant to perform by making the user only see and do what is pertinent to them.

3.2 Core data entities

The platform is structured around a set of core records based on real objects of operation. They are guard and client profile, job posting, shift slots, job applications, job assignments, and job attendance events. The support of compliance and onboarding is also facilitated with the help of licence records and verifying artefacts, i.e. with passport or visa papers and uploaded certifications.

3.3 Verifying the attendance process

Check-in and check-out actions with time-stamps and supported by evidence capture like a photo are used to take the attendance. Location context may also be accessed as needed to validate a site. The system breaks worked time, deducts the breaks and generates adjusted hourly totals in such a way that the attendance records are directly converted into payroll summaries and performance reporting.

3.4 Communication and safety

In-app messaging among pertinent users enables operation coordination. In safety-sensitive scenarios, an SOS feature enables a rapid escalation process, which assists organisations to react rapid on situations when a guard requires immediate help.

3.5 Technology Stack and Implementation Environment

VigiloX is deployed as cross platform mobile-web application. The client application is developed in the Unity Engine using the Mono scripting runtime and released on Android and Windows platforms with a common codebase with platform specific integrations.

Firebase offers the backend services, such as Firebase Authentication (identity, role-based access control), Realtime Database (live synchronisation of operational data e.g. profiles, assignments, attendance events) documents and media evidence and Firebase Cloud Messaging (notifications).

Real-time operational communication is facilitated through Photon stack (Photon Realtime/PUN, Photon Chat, and Photon Voice), allowing low latency messaging, presence, and optional voice communications in the platform. Firebase/Photon provides encrypted communication channels, which are combined with other cryptographic tools (e.g., BouncyCastle) and secure PDF generation of reports (e.g., iTextSharp) and QR/barcodes scanning (e.g., ZXing) are provided where necessary.

SYSTEM MODULES AND FUNCTIONAL WORKFLOWS

4.1 Onboarding and verification

The mobile app has a well-organized and user-friendly point of entry to the guards and administrative users, where they are guided to create an account and securely log in (Figure 1). The system also records mandatory identity and contact related data used to facilitate the downstream staffing, communication, and compliance procedures during onboarding. This strategy guarantees that users have a valid and stable profile at the time they are registered to the platform.

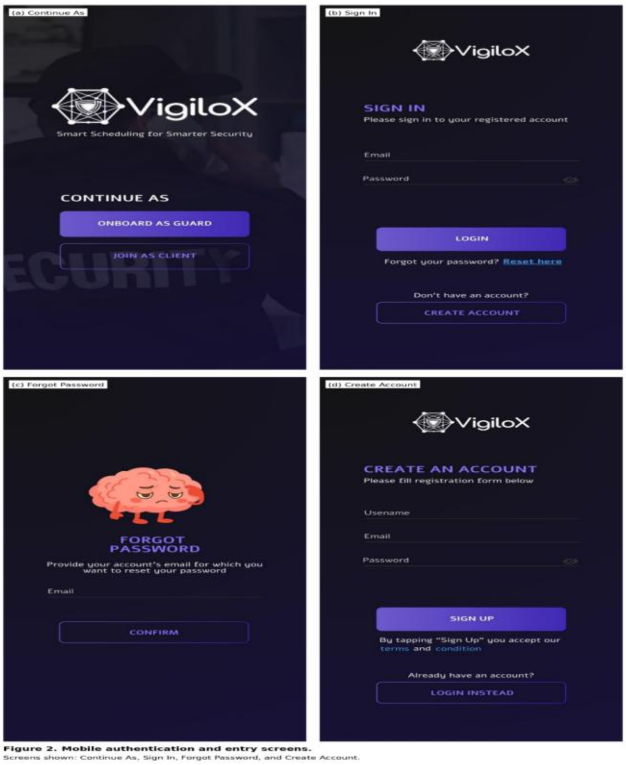


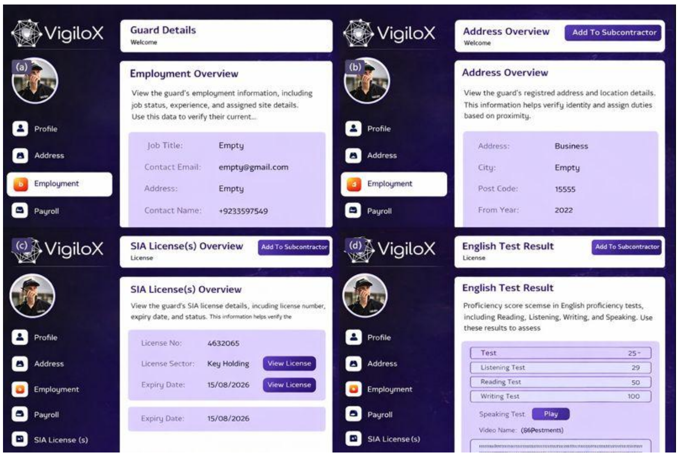
Figure 2. Mobile authentication and entry screens.
Screens shown: Continue As, Sign In, Forgot Password, and Create Account.

Figure 1. Authentication and entry screens

It shows the Composite view of the VigiloX mobile app with (a) role-based entry selection, (b) secure sign-in screen, (c) password recovery screen and (d) account creation process of a new user.

4.2 Guard profile and self-service

Each and every guard will have a dedicated profile dashboard that aggregates main operational data into one simple-to-use dashboard (Figure 2). Through this display, the guards have the capability of knowing their current status of activity, viewing the assigned work done and being able to use the in-built tests and also enjoy the safety features such as the SOS feature. One of the fundamental aspects of this self-service design is an in-app English proficiency test: every guard will be able to complete the test inside the platform, and the results will be held on the profile of the guard to facilitate the ability to assess the skills and assign the right roles to the guard. The platform allows greater transparency by allowing a guard to view and update his or her profile information, which decreases supervisory user administrative workload.



Employment Overview

View the guard's employment information, including job status, experience, and assigned site details. Use this data to verify their current...

Job Title: Empty
Contact Email: empty@gmail.com
Address: Empty
Contact Name: +9233597549

Address Overview

View the guard's registred address and location details. This information helps verify identity and assign duties based on proximity.

Address: Business
City: Empty
Post Code: 15555
From Year: 2022

SIA License(s) Overview

View the guard's SIA license details, incuding license number, expiry date, and status. This information helps verify the

License No: 4632065
License Sector: Key Holding
Expiry Date: 15/08/2026
Expiry Date: 15/08/2026

English Test Result

Proficiency score scemse in English proficiency tests, including Reading, Listening, Writing, and Speaking. Use these results to assess

Test	25
Listening Test	29
Reading Test	50
Writing Test	100

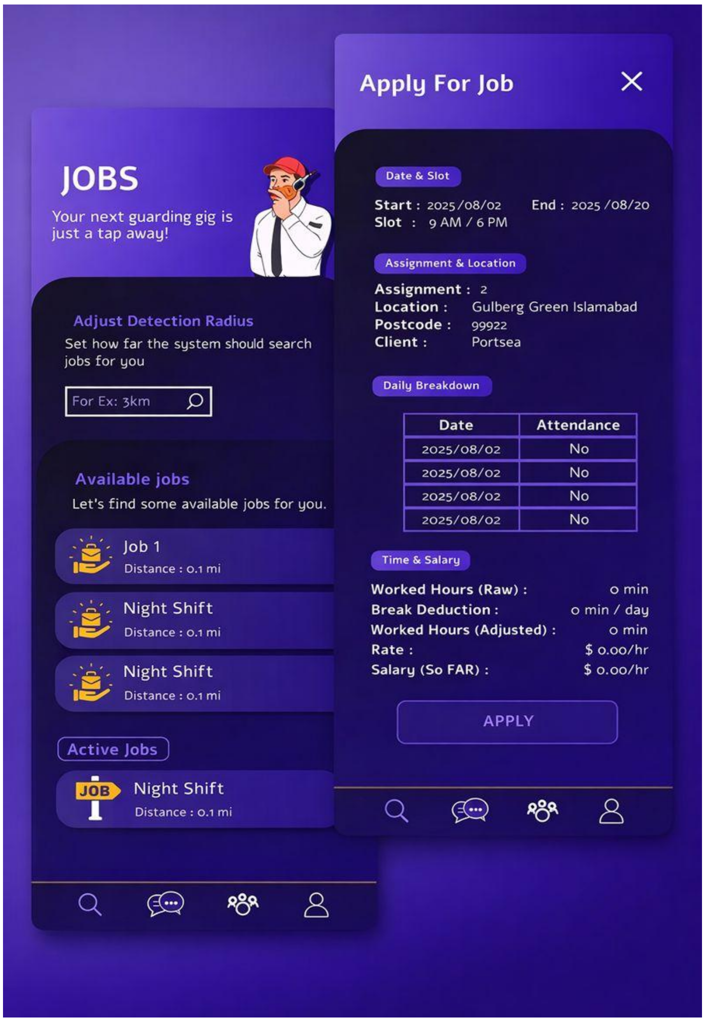
Speaking Test
Video Name: (66Pestments)

Figure 2. Guard profile dashboard

Figure 2 shows composite view of the VigiloX guard interface with employment, address, regulatory licensing (SIA), and English proficiency test. These modules underpin self-management of guards, verification on compliance and assessment of the skills in the platform.

4.3 Jobs and applications

Clients or administrators create jobs that have very specific site details and shift parameters. Guards are able to surf through the available opportunities, filter results with a customized search radius, and apply to particular assignments. The application detail view offers the display of the job dates, location, and time-and-pay on the same screen, which helps the guards make informed decisions and minimizing misunderstandings during the point of acceptance (Figure 3).



JOBS

Your next guarding gig is just a tap away!

Adjust Detection Radius

Set how far the system should search jobs for you

For Ex: 3km

Available jobs

Let's find some available jobs for you.

Job 1
Distance : 0.1 mi

Night Shift
Distance : 0.1 mi

Night Shift
Distance : 0.1 mi

Active Jobs

Night Shift
Distance : 0.1 mi

Apply For Job

Date & Slot

Start : 2025/08/02 End : 2025/08/20
Slot : 9 AM / 6 PM

Assignment & Location

Assignment : 2
Location : Gulberg Green Islamabad
Postcode : 99922
Client : Portsea

Daily Breakdown

Date	Attendance
2025/08/02	No
2025/08/02	No
2025/08/02	No
2025/08/02	No

Time & Salary

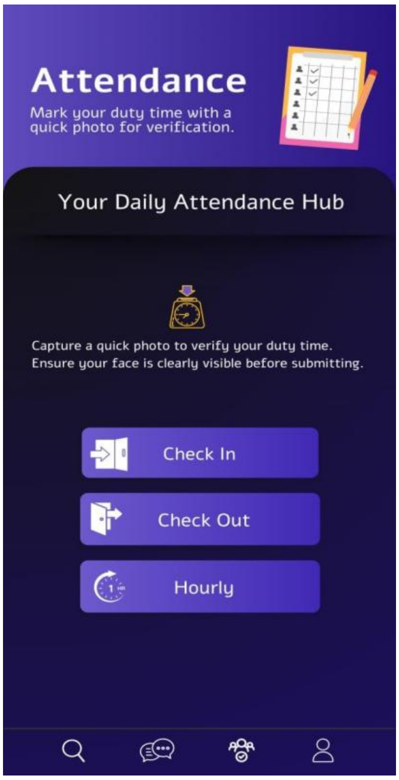
Worked Hours (Raw) :	0 min
Break Deduction :	0 min / day
Worked Hours (Adjusted) :	0 min
Rate :	$ 0.00/hr
Salary (So FAR) :	$ 0.00/hr

Figure 3. Job discovery and application flow

Figure 3 shows job listings, job details, and the guard application interface that is used to view and apply to assignments.

4.4 Attendance verification

The check-in and check-out is recorded in a well-organized system, which involves a fast photo release as a verification tool, which is accompanied by regular notifications in case of a longer shift (Figure 4). Both raw and adjusted working hours are recorded by the system with standardised rules on breaks where needed. This gives regular, payroll ready time summative and verifiable record of attendance.



Attendance

Mark your duty time with a quick photo for verification.

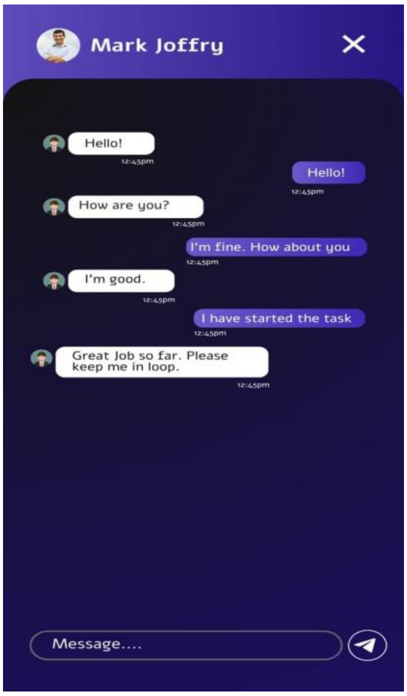
Your Daily Attendance Hub

Capture a quick photo to verify your duty time.
Ensure your face is clearly visible before submitting.

Figure 4. Attendance hub

4.5 Message and operations coordination

Designed to support the daily processes, the platform also has in-built the messaging technology enabling guards and supervisory users to directly converse in the system (Figure 5). Taking operational instructions and updates within the platform enhances traceability and minimises on the need to use external messaging tools, which are more difficult to trace.



Mark Joffry

Hello!
12:45pm

Hello!
12:45pm

How are you?
12:45pm

I'm fine. How about you
12:45pm

I'm good.
12:45pm

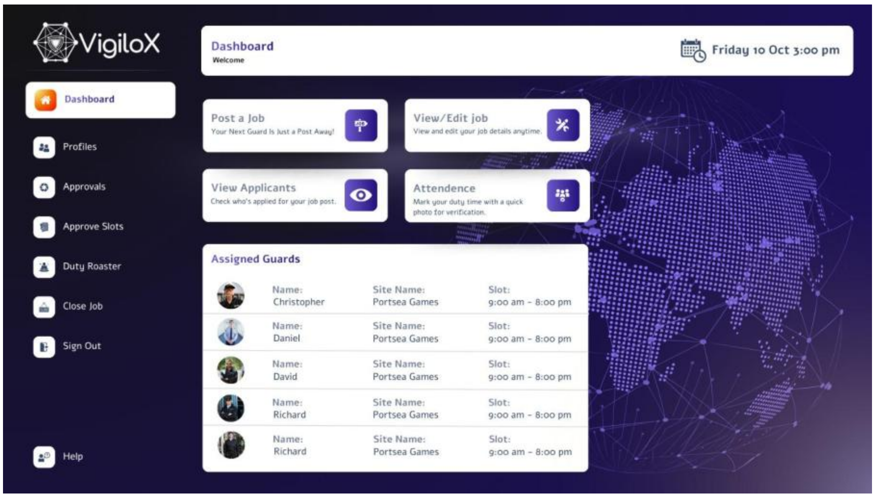
I have started the task
12:45pm

Great Job so far. Please keep me in loop.
12:45pm

Figure 5. In-app messaging screen

4.6 Management of administration and job life-cycle stage

The web-based dashboard can be viewed as the main point of control on the side of the administrators. It offers direct access to the basic functions like job creation and editing, reviewing applicants, assigning guards and attendance control (Figure 6). This centralized perspective facilitates effective administration of the entire job lifecycle through posting up to the end.


VigiloX
Dashboard
Profiles
Approvals
Approve Slots
Duty Roaster
Close Job
Sign Out
Help
Dashboard
Welcome
Friday 10 Oct 3:00 pm
Post a Job
Your Next Guard Is Just a Post Away!
View/Edit job
View and edit your job details anytime.
View Applicants
Check who's applied for your job post.
Attendence
Mark your duty time with a quick photo for verification.

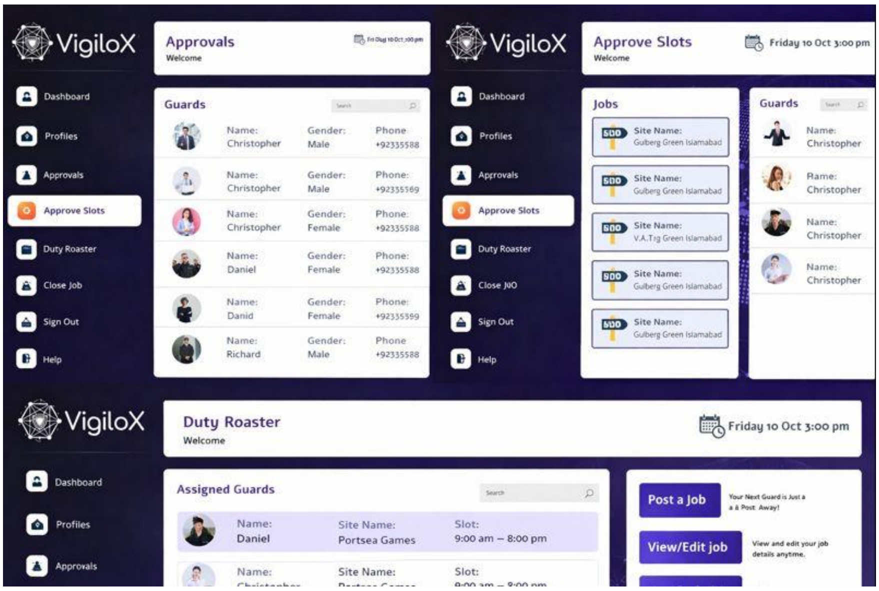
Assigned Guards

Name:	Site Name:	Slot:
Christopher	Portsea Games	9:00 am - 8:00 pm
Daniel	Portsea Games	9:00 am - 8:00 pm
David	Portsea Games	9:00 am - 8:00 pm
Richard	Portsea Games	9:00 am - 8:00 pm
Richard	Portsea Games	9:00 am - 8:00 pm

Figure 6. Administrative dashboard overview

4.7 Approaches and allotment of slots

Accepting of the applicants and assigning slots are managed via a special interface where jobs and candidate guards are shown (Figure 7). This design allows prompt and knowledgeable making of assignments to ensure that administrators pair staffing requirements with availability of guards and retain control over coverage levels at each site and shift.



Guards

Name:	Gender:	Phone
Christopher	Male	+92335588
Christopher	Male	+92335569
Christopher	Female	+92335588
Daniel	Female	+92335588
Danid	Female	+92335599
Richard	Male	+92335588

Jobs

	Site Name:
500	Gulberg Green Islamabad
500	Gulberg Green Islamabad
500	V.A.T.g Green Islamabad
900	Gulberg Green Islamabad
500	Gulberg Green Islamabad

Guards

Name:
Christopher
Christopher
Christopher
Christopher

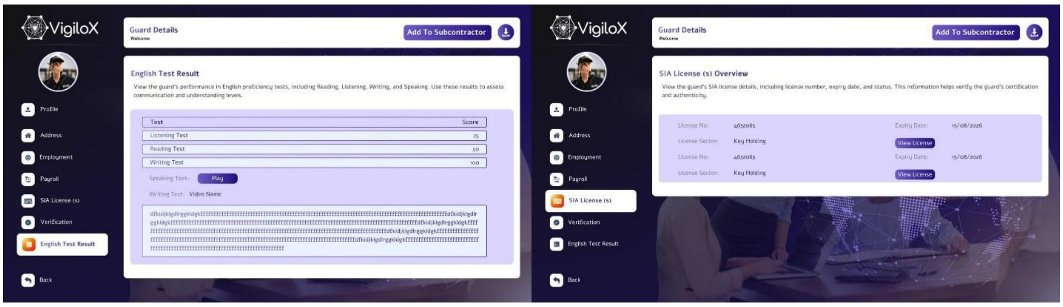
Assigned Guards

Name:	Site Name:	Slot:
Daniel	Portsea Games	9:00 am – 8:00 pm
Christopher	Portsea Games	9:00 am – 8:00 pm

Figure 7. Approvals and slot allocation interface

4.8 Compliance and verification

Address history, employment records, licensing such as SIA licences and supporting documents such as passports, visas and certificates are all combined in the detailed guard records (Figure 8). By having these materials centralised in the platform it would be easy to check compliance routinely and minimise chances of missing or out of date records.



English Test Result

View the guard's performance in English proficiency tests, including Reading, Listening, Writing, and Speaking. Use these results to assess communication and understanding levels.

Test	Score
Listening Test	25
Reading Test	50
Writing Test	100

Speaking Test:

Writing Test: Video Name

SIA License (s) Overview

View the guard's SIA license details, including license number, expiry date, and status. This information helps verify the guard's certification and authenticity.

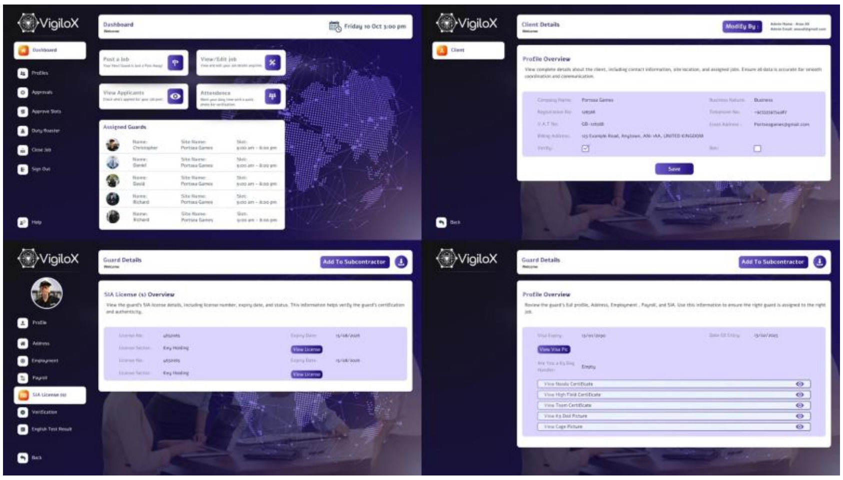
License No: 4632065 Expiry Date: 15/08/2026
License Sector: Key Holding

License No: 4632065 Expiry Date: 15/08/2026
License Sector: Key Holding

Figure 8. Guard compliance and verification modules

4.9 Client governance

Client profiles are identified as organisational identifiers including company registration number, VAT, billing address, primary contacts, etc. Governance controls The governance controls such as verification and account restriction options enable the administrators to be responsible when it comes to controlling client activity and reducing the possibility of fraudulent or inappropriate job postings (Figure 9).



Company Name: Portsea Games
Billing Address: 125 Example Road, Anytown, AN1 1AA, UNITED KINGDOM
Verify: ☑ Ban: □

Figure 9. Client profile and governance controls

RESULT AND DISCUSSION

5.1 End-to-End Validation Outcomes

Functional validation revealed that VigiloX is capable of performing the entire operational cycle that is necessary in private security uses: a customer posts a job, guards apply, an administrator authorizes and assigns shift slots, the assigned guard logs attendance with evidence, the system produces time summaries that are associated with the corresponding assignment. The key design deliverable is traceability-by-design - records are interconnected globally instead of stored as disconnected artefacts - accountability is achieved through the capability of reconstructing the decisions of who was assigned, who attended, where under which approval are based on the record of the system itself (Kroll 2021). Table 1 is an overview of the end-to-end scenario-based testing, which was done to verify that the platform can support core guarding workflows and generate auditable operational records.

Scenario	Steps	Expected output	Evidence	Result
S1 Guard onboarding and verification	Guard registers → uploads ID docs → admin reviews → account activated	Guard profile is verified, ID/licence status marked approved	Guard profile entry, uploaded document metadata, admin approval log	Pass

S2 Job creation and application	Client creates job → adds location/slot/requirements → guards apply	Job is visible to eligible guards, applications attach to that job	Job record, application list with timestamps	Pass
S3 Approval and roster assignment	Admin reviews applicants → approves → assigns guard to slot/shift	Guard-slot assignment created, roster updated	Roster record, assignment ID linked to guard + job	Pass
S4 Attendance check-in	Guard arrives → checks in → photo + time recorded	Check-in record stored with evidence	Attendance log, image file, timestamp entry	Pass
S5 Attendance check-out	Guard checks out → hours calculated	Completed attendance session with total hours	Attendance summary, duration calculation record	Pass
S6 Compliance verification before deployment	System checks licence/verification status before assigning	Guard is blocked if documents missing/expired	Compliance status flag, audit log entry	Pass
S7 Payroll-ready summary generation	System aggregates attendance → generates time summary	Payroll-ready report per guard/job	Time summary report, exportable record	Pass
S8 Traceability across modules	Trace guard → job → slot → attendance → summary	Audit trail can be followed across modules	Linked IDs across profile/job/roster/attendance	Pass

Table 1. End-to-End Scenario-Based Evaluation of the VigiloX Platform

The results as reported in Table 1 do not just indicate correctness of individual modules, but the integrity of cross-module dependencies which is vital in personal security operations. Specifically, the situations S3, S4, and S5 indicate that roster assignment, capturing attendance evidence and generating time-summaries are always associated with the usage of common identifiers. This connection makes it less ambiguous who does a shift (e.g. who did which slot) and more powerful in managing working disagreements within the organisation in regard to coverage or breaks or hours of pay. Scenario S6-S8 build on previous argument that governance status checks and audit trails can be verified using the same operational records as opposed to using external spreadsheets, messaging threads, or unmonitored document folders to enhance preparedness during allocation decisions and periodical compliance checks.

5.2 Stakeholder Walk-through Feedback

Besides scenario-based validation, informal feedback of stakeholders was also gathered by conducting guided walk-throughs with the targeted user roles. The participants were 3 users: 1 admin and 2 guards, who were required to undertake core workflows corresponding to Table 1, which comprised job posting and approval, roster assignment, attendance check-in/out and time summary review. The general feedback indicated that the overall end-to-end connection between approvals, roster assignments, attendance evidence and payroll-ready summaries were consistent with current operational practice and less ambiguity than fragmented tools. This is especially helpful when participants were reviewing hours or resolving disputes as the participants highly treasured the capability to get back to a specific job slot and approval decision to track attendance records. Recommendations were made in terms of interface refinements, as opposed to workflow logic, suggesting that the process model underlying the interface was suited to the real world security operations. Though the scale of this feedback is limited and exploratory, it offers some preliminary face validity that the site is able to accommodate more than technical correctness as to operational requirements.

Role	Tasks Performed	What Worked Well	Suggestions / Observations
Admin / Dispatcher	Job posting, approvals, roster assignment, attendance review	Clear linkage between approvals, roster, and attendance, audit trail useful for review	Faster bulk approvals, clearer filters
Guard	Profile review, check-in/out, shift viewing	Attendance flow easy to follow, evidence capture straightforward	Clearer prompts at check-in
Compliance / Supervisor	Document review, licence status checks, summary review	Centralised compliance records reduced manual checking	Retention rules should be configurable

Table 2: Summary of Stakeholder Walk-through Feedback

5.3 Usability and Operational Implications

The division of modules (profiles, approvals, roster, attendance, compliance) into operational roles and tasks is more usable based on operational roles and tasks, which helps to reduce information that a user needs to process on a step-by-step basis (i.e. it can reduce extraneous load by deconstructing the workflow systematically) (Schreiber, Abbad-Andaloussi, and Weber 2024). Operationally, the primary value is generated at process handoffs where manual processes often fail: breaking approvals into slot assignments, accumulating evidence against the proper slot, discretizing attendances into payroll-ready reports and maintaining provenience. The additional advantage of you maintaining such transitions in a single platform is so that you can eliminate duplication which will be caused by maintenance of records and also earned agreement in reporting.

5.4 Governance, Privacy and Data Protection

The issue of privacy and data protection is also relevant due to the fact that the site keeps identity documents and photo-based evidence related to attendance. Practically, deployments ought to use encryption in transit and stored records, role based access control with log history about happened sensitive records as well as deploy explicit retention/deletion regulations on the evidence of identity after accomplishing the objectives of verification and the standing of retention have been achieved. Such controls put into effect accepted principles of data protection like purpose limitation, data minimisation and storage limitation (European Data Protection Board (EDPB) 2020).

5.5 Limitations and Future Evaluation Metrics

Although the positive results were obtained after the validation, the analysis is restricted to the level of functional and scenario-based tests and is not yet able to measure operational results in the field. Specifically, the existing outcomes fail to quantify the time savings, the decrease in the number of disputes, or the change in compliance performance in comparison with the current manually practiced methods. A more rigorous analysis would involve field trials in several locations and positions, which would record both efficiency ratios (e.g. time-to-onboard, time-to-fill) and quality ratios (e.g. dispute frequency, correction rates), to measure the actual impact.

The operational metrics that should be used to quantify the benefits in the future include time-to-onboard, shift-fill rate, attendance dispute rate, and payroll cycle time. It would also be necessary to conduct field trials in a variety of locations that would allow comparing processes between manual and platform-based.

CONCLUSION

As a part of this paper, a mobile-web platform VigiloX was introduced, which was aimed at digitalising the main private security workforce activities, onboarding and verification, job placement, roster placement, evidence-based attendance registration, and compliance records management. The platform has a fundamental contribution of a traceable operational lifecycle where approvals, assignments, attendance evidence, and payroll-ready time summaries are connected through modules to enable auditability of the operational control and compliance review. The validation (scenario-based) and feedback (stakeholders walk-throughs) point to the fact that the workflow model is a workable concept that reflects practical security operations, and also helps to minimize the use of fragmented tools and disconnected records.

FUTURE WORK

The future will also be geared towards enhancing the intelligence of operations as well as governance. Intended improvements are: (i) customizable geofencing and anomaly detection (e.g., late arrivals, off-site check-ins, missing check-outs) (ii) more extensive payroll, invoicing and export integrations to enable end-to-end administration (ii) supervisor and client facing dashboards on performance and compliance and (iii) enhanced security controls in line with industry-best practice, such as stricter access controls (e.g. access controls) and improved evidence retention management. Further testing will focus on trial in the field by multiple sites to measure the impact of operations in terms of time-to-onboard, the rate of shift-fills, the rate of dispute, and payroll cycle time.

REFERENECES

[1] N. Nordin and N. M. Fauzi, “A web-based mobile attendance system with facial recognition feature,” 2020, Accessed: Jan. 10, 2026. [Online]. Available: https://www.learntechlib.org/p/216424/

[2] B. Soewito, F. L. Gaol, E. Simanjuntak, and F. E. Gunawan, “Attendance system on Android smartphone,” in *2015 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)*, IEEE, 2015, pp. 208–211. Accessed: Jan. 10, 2026. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7337046/

[3] J. S. Asa, O. Bumma, D. Tamara, and C. M. Sarungu, “Android Based Job Search Application ‘Megawe’ For The Segment Of Workers With An Education Level Below A University Degree,” *Procedia Computer Science*, vol. 227, pp. 194–203, 2023.

[4] J. Holopainen, O. Mattila, E. Pöyry, and P. Parvinen, “Applying design science research methodology in the development of virtual reality forest management services,” *Forest Policy and Economics*, vol. 116, p. 102190, 2020.

[5] A. R. Hevner *et al.*, “Transparency in design science research,” *Decision Support Systems*, vol. 182, p. 114236, 2024.

[6] J. A. Kroll, “Outlining Traceability: A Principle for Operationalizing Accountability in Computing Systems,” in *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, Virtual Event Canada: ACM, Mar. 2021, pp. 758–771. doi: 10.1145/3442188.3445937.

[7] C. Schreiber, A. Abbad-Andaloussi, and B. Weber, “On the cognitive and behavioral effects of abstraction and fragmentation in modularized process models,” *Information Systems*, vol. 125, p. 102424, 2024.

[8] European Data Protection Board (EDPB), “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default | European Data Protection Board.” Accessed: Jan. 10, 2026. [Online]. Available: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en