Fraud Risk in Self-Built Systems: When Generative AI Outpaces Internal Controls in Small Businesses

Adedoyin Akande[1]*, Shalom Alugwe[2]

[1]Independent Researcher, Washington, DC, United States
[2]Independent Researcher, USA

Abstract

Purpose: Generative artificial intelligence (GenAI) is making it practical for small businesses to build their own operational and financial systems without a vendor or implementation team. This paper examines the fraud risks that arise when such systems become a firm's book of record, and it develops a framework that fraud examiners and auditors can use to evaluate them.

Design/methodology/approach: The paper combines conceptual analysis grounded in fraud theory, internal-control frameworks and audit-evidence standards with an illustrative practitioner case: the development, by a Certified Fraud Examiner, of a GenAI-built enterprise resource planning (ERP) system for a family-owned industrial sewing-machine business in Lagos, Nigeria.

Findings: Self-built systems start with no inherited controls. Five mechanisms amplify fraud opportunity: concentrated access, mutable records without change history, untested business logic, unvalidated data migration, and key-person dependency on the builder. Because GenAI produces polished outputs, these weaknesses can be harder to see, since the system looks more formal than the process behind it. The paper proposes a five-question examination framework that links each mechanism to procedures, evidence and a graded reliance decision.

Research limitations/implications: The framework is derived from one build and from established theory; it has not yet been field-tested across examinations. Propositions for empirical testing are provided.

Practical implications: Examiners should not give system-generated reports more evidentiary weight because they resemble commercial software output, and should consider early preservation where one person controls the system.

Originality/value: The paper identifies a new category of evidence risk, the AI-generated, owner-built book of record, and translates existing fraud and audit principles into practical procedures for it.

Keywords: Occupational fraud; Internal control; Generative artificial intelligence; Small business; Audit evidence; Digital forensics; End-user computing; Nigeria

Journal of Science, Technology and Social Transformation (2026) Doi: 10.64235/215dfe52

Introduction

For most of its four decades, a family-owned industrial sewing-machine business in Lagos, Nigeria, kept records much as many small businesses do: notebooks, spreadsheets, and information that the owner simply knew. Purchasing records sat apart from inventory. Customer information was kept separately from supplier payments. Financial reporting meant assembling information after the fact. The owner was the link between the records.

I recently built an ERP system for the business using GenAI. My background is in finance, enterprise-systems implementation and fraud examination, so I could map the process, define the requirements and test whether the logic made sense. What I could not previously do alone was write the software. The system now connects supplier ordering, payments, inventory, customer records and financial reporting. As it took shape, I noticed something that changed how I viewed the project. No software vendor

Corresponding Author: Adedoyin Akande, Independent Researcher, Washington, DC, United States, Email: shalomalugwe@gmail.com

How to cite this article: Akande A, Alugwe S. (2026). Fraud Risk in Self-Built Systems: When Generative AI Outpaces Internal Controls in Small Businesses. *Journal of Science, Technology and Social Transformation* 2(3), 61-69.

Source of support: Nil

Conflict of interest: None

had designed the controls. No implementation team had reviewed the configuration. No independent person validated the system before it went into use. I had defined the requirements, built the application and checked the results myself.

Because of my training, I knew to ask about access, audit trails, reconciliations and the integrity of the underlying records. A business owner using the same tools to solve an inventory or payment problem may never ask those questions. That is where the fraud risk begins.

This paper addresses three questions. First, how does GenAI-enabled self-building change the control environment of small businesses? Second, through what mechanisms does it create or amplify fraud opportunity? Third, how should fraud examiners and auditors evaluate the reliability of records produced by such systems? It contributes (a) an extension of fraud-opportunity theory to self-built, AI-generated systems (Figure 1); (b) a taxonomy of five opportunity-amplifying mechanisms (Table 2); and (c) a five-question examination framework mapped to procedures, evidence and existing standards (Figure 2; Table 3). A companion paper examines the operational-capability side of the same case (Akande, 2026).

Background

From using AI to building with it

Small-business adoption of GenAI has grown quickly. The U.S. Chamber of Commerce reported that 58% of surveyed small businesses were using GenAI in 2025, up from 40% in 2024 and 23% in 2023, and that 84% planned to increase their use of technology platforms (U.S. Chamber of Commerce Technology Engagement Center, 2025). The National Federation of Independent Business, surveying a different population, found that 24% of small employers were currently using AI, rising from 21% among firms with fewer than 10 employees to 48% among those with 50 or more (NFIB Research Center, 2025).

The use cases matter more than the headline rates. In the NFIB survey, 29% of respondents were using or planning to use AI for communications and 27% for marketing, while only 4% cited accounting, 4% process automation and 4% cybersecurity or fraud detection (NFIB Research Center, 2025). Most small-business AI use still sits around individual tasks. That is unlikely to last. The same tools that draft an email can generate a database, a payment workflow or a reporting application, and a system that once required a developer can now be produced through an extended conversation with an AI tool. Fraud examiners know how to test spreadsheets, commercial accounting packages and established ERP systems. They will increasingly meet something different: internal systems built by the business itself, sometimes by one person, with no vendor review and no standard control environment behind them.

End-user computing, shadow IT and AI-generated code

Self-built systems are not new in kind. End-user computing (EUC) has long allowed non-specialists to build spreadsheets and small databases that become critical to reporting, and research documents that such artefacts carry high error rates that are rarely detected by their authors (Panko, 1998). Systems adopted outside formal IT governance, often called *shadow IT*, create control and security gaps precisely because no one designed them as part of the control environment (Silic & Back, 2014). Governance frameworks such as COBIT and ITIL exist to close those gaps, and their adoption has been linked to regulatory compliance outcomes in Nigerian firms (Fadero et al., 2018; ISACA, 2018).

GenAI changes the scale and sophistication of what end users can build. It also brings specific risks. Code produced by AI assistants frequently contains security weaknesses (Pearce et al., 2022), and users with AI assistance have been found to write less secure code while believing it to be more secure (Perry et al., 2023). This overconfidence is a form of automation bias, the tendency to accept automated outputs with less scrutiny than they warrant (Parasuraman & Manzey, 2010). Human-in-the-loop designs keep human validation at the points where AI outputs enter consequential processes (Ladapo et al., 2024).

Fraud theory and the opportunity dimension

The fraud triangle holds that occupational fraud requires pressure, opportunity and rationalisation (Cressey, 1953). The fraud diamond adds *capability*: the perpetrator's position, knowledge and skill to exploit an opportunity (Wolfe & Hermanson, 2004). Of these elements, opportunity is the one organisations can most directly control through internal control. The COSO framework treats control activities, information and communication, and monitoring as components that jointly constrain opportunity, with segregation of duties as a core control activity (COSO, 2013). Self-built systems bear on two of these elements. They can widen opportunity by omitting controls, and they can concentrate capability in the person who built the system and understands its internals. Research on insider threat similarly emphasises that privileged insiders with system knowledge present distinctive risk (Akeju et al., 2018; Onche et al., 2024).

The small-business control environment

Smaller organisations already operate with fewer anti-fraud controls. In the ACFE's *Occupational Fraud 2026* study of 2,402 cases, more than half of cases involved either a lack of internal controls or an override of existing controls (Association of Certified Fraud Examiners [ACFE], 2026). Organisations with fewer than 100 employees experienced a median loss of $126,000, the highest among the size groups reported (ACFE, 2026). The 2024 edition gives a clear comparison of control adoption by size: only 27% of organisations with fewer than

100 employees had a hotline, compared with 82% of larger organisations, and small organisations also lagged in internal audit, fraud training, proactive data monitoring and formal fraud risk assessment (ACFE, 2024). Work on SME financial governance likewise emphasises that accountability depends on how transactions are recorded, approved and reported (Bola-Sadipe et al., 2019; Eboh et al., 2025). AI-built systems are arriving in exactly this environment.

Reliability of information produced by the entity

Auditing standards require auditors to evaluate whether information produced by the entity is sufficiently reliable, including by testing its accuracy and completeness, before using it as evidence (IAASB, 2009; PCAOB, 2010). Digital-evidence guidance adds requirements for identification, collection and preservation that maintain integrity and chain of custody (ISO/IEC, 2012; Kent et al., 2006). These principles apply to any system. The difference with a self-built system is that the examiner cannot assume the baseline controls, such as audit logs, permissions and posting locks, that a commercial package would normally provide.

The operating context of the case business

The case business operates in Lagos, and three features of its operating environment bear on the analysis that follows.

The first is that supply and delivery are irregular for legitimate reasons. The movement of goods is affected by congested and poorly connected urban networks (Tiamiyu & Alaka, 2020), by loading and unloading at informal roadside motor parks that interferes with arterial traffic (Bolaji & Ajayi, 2021) and by flood-exposed road segments (Alaka, Bolaji, & Tiamiyu, 2022). Flood exposure is linked in turn to the condition of roadside drainage and culvert structures on urban arterials (Bolaji et al., 2019) and to the durability of the concrete used in them (Alaka & Tiamiyu, 2019). Between cities, road traffic crashes add to the uncertainty: their spatial clustering on intercity corridors has been analysed from national road safety records (Alaka et al., 2021), and emergency response coverage on intercity highways has documented gaps (Tiamiyu et al., 2021). Beyond the main centres, unpaved rural road networks constrain physical access to essential services (Alaka et al., 2020). In such an environment, late receipts, part deliveries, substituted carriers and ad hoc logistics payments are routine. That matters to an examiner because routine exceptions supply plausible explanations for irregular entries. Where a system keeps no change history, a legitimate exception and a concealed alteration can look the same in the records.

The second is exposure to external shocks, which bears on the pressure element of the fraud triangle. COVID-19 movement restrictions changed essential trip-making in Nigerian cities (Ajayi et al., 2020), and later fuel-price increases affected what low-income commuters were willing to pay for shared and digitally booked transport (Ajayi et al., 2023). Shocks of this kind raise costs for households and for the small businesses that employ them, and financial strain on an employee or owner is the condition Cressey (1953) identified as pressure.

The third is a thin information environment. Mobile network coverage and road surface condition jointly constrain digitally booked services beyond state capitals (Alaka, Ajayi, & Bolaji, 2022), and connectivity of that kind affects where a self-built system is hosted, how it is backed up and whether an independent party can reach it. Where formal records are incomplete, decision-support research in data-scarce regions has combined field survey with open data (Tiamiyu et al., 2023) and has used multi-criteria methods to rank competing priorities (Alaka et al., 2023). The examination framework in Section 5 follows a similar logic: system records are corroborated against independent sources, and procedures are scaled to assessed risk.

Approach

The paper is conceptual, with an illustrative case. The conceptual component applies fraud theory (Section 2.3), internal-control frameworks (Section 2.4) and evidence standards (Section 2.5) to the characteristics of GenAI-built systems. The case component draws on my experience designing and building an ERP system for the business described above, including design artefacts and working notes on which controls I had to specify explicitly. The case is used to illustrate and ground the mechanisms, not to test them. I am a family member of the business owner and the system's builder; this gives direct insight into design choices but limits independence, and I report the resulting limitations in Section 7. No fraud was identified or alleged in the case business, and the analysis concerns risk, not events.

How Self-Built Systems Change the Control Environment

The controls are there only if somebody designed them

Commercial accounting and ERP products usually come with familiar control features: user permissions, audit logs, approval workflows, period restrictions and rules governing how posted transactions can be changed. These controls may be imperfect, but they exist because the software was designed around recurring accounting and operational risks. A self-built application starts with a blank page. If an owner asks an AI tool to build an inventory tracker, the tool may do exactly that and nothing more. The application might not preserve deleted records or keep a history of changes, and the same user may be able to add a vendor, approve a payment and edit the transaction afterwards. Table 1 contrasts where control features come from in the two settings.

This is not necessarily evidence of bad intent. In many cases the owner was solving an operating problem and never thought of the application as part of the control environment.

Table 1: Provenance of key control features: commercial packages versus GenAI-built systems

Control feature	*Commercial accounting / ERP package*	*GenAI-built, owner-operated system*
User roles and permissions	Provided by default; configured at implementation	Exists only if specified; often a single all-powerful user
Audit trail / change log	Typically built in; posted entries logged	Absent unless requested; records often editable in place
Posting locks and period close	Standard feature	Rarely generated unless explicitly requested
Approval workflows	Configurable (e.g., purchase-to-pay approvals)	Must be designed and coded; easily bypassed by the builder
Vendor master controls	Change logging, dual control options	Vendor and bank details may be edited without trace
Independent review of logic	Vendor QA; implementer testing; user acceptance testing	Often none beyond the builder's own checks
Access to code and database	Separated from ordinary users	Builder can change code, schema and data directly
Continuity and support	Vendor documentation and support	Knowledge concentrated in the builder

Note. Author's synthesis. Commercial packages vary in default settings, and poorly configured commercial systems can share several of the weaknesses listed in the right-hand column.

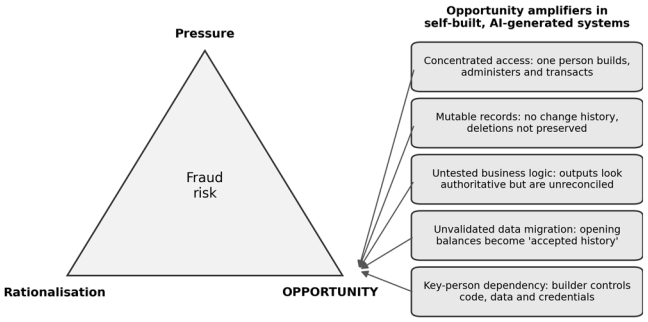
Examiners must still assess the consequences of that design. In my own build, access restriction, change logging and reconciliation were implemented because I specified them. The GenAI tools did not propose them unprompted.

A polished report can still be wrong

GenAI is very good at producing work that looks finished. A dashboard can be clean, a financial report can balance and a calculation can return an exact answer. None of that tells the examiner whether the underlying logic is sound. While building the system, I found that an inventory calculation could produce a precise reorder quantity and still miss a supplier constraint that changed the decision, and that a financial output could look reasonable until I traced it back to the underlying transactions. Presentation quality is not evidence quality. If a report comes from a self-built system, the examiner should establish who designed the logic, who tested it and whether anyone reconciled the result to source records. A professional-looking output should not receive more evidentiary weight because it resembles commercial software output. Analytical techniques such as variance analysis and revenue assurance can help detect anomalies (Aliliele et al., 2024; Sakyi et al., 2023), but only if the data they run on can be trusted.

Five opportunity-amplifying mechanisms

Drawing these observations together, Figure 1 extends the opportunity dimension of the fraud triangle with five mechanisms characteristic of self-built, AI-generated systems. Table 2 relates each mechanism to the schemes it can enable and to indicative red flags.



Note. Adapted from Cressey (1953) and Wolfe and Hermanson (2004). Concentrated access and key-person dependency also bear on the capability element of the fraud diamond.

Figure 1: Opportunity amplifiers in self-built, AI-generated systems: an extension of the fraud triangle

The system may be part of the evidence problem

Fraud examinations often depend on reconstructing events. If a vendor was added, who added it? If bank details changed, when did the change occur? If an invoice was edited, what did the original say? A self-built system may not be able to answer those questions. The person who wrote or maintains the application may be able to alter records, change the code or edit the database without leaving a reliable trail. In that situation, the examiner must assess the integrity of the system before relying on the reports it produces. This matters most when the builder is also responsible for the underlying transactions. In a five-person business that concentration may

Table 2: Opportunity-amplifying mechanisms, schemes enabled and red flags

Mechanism	*How it arises in a self-built system*	*Schemes it can enable*	*Indicative red flags*
Concentrated access	Builder is also administrator and transaction processor; no role separation	Fictitious vendors; unauthorised payments; concealment by record alteration	One account with rights to create vendors, approve and edit payments; no second approver
Mutable records	No change history; deletions not retained; posted entries editable	Altered invoices or bank details; deleted sales (skimming); backdated entries	Gaps in document sequences; no "created/ modified by" fields; balances that change retrospectively
Untested business logic	Calculations generated by AI and accepted on appearance	Manipulated margins, ageing or inventory values; errors exploited to conceal theft	Outputs that cannot be reperformed; unexplained rounding or classification patterns
Unvalidated data migration	Opening balances and masters loaded from spreadsheets or notebooks without reconciliation	Inflated receivables or inventory; fictitious historical transactions becoming "accepted history"	No migration reconciliation; opening balances without supporting schedules
Key-person dependency	Only the builder understands the code, data location and credentials	Obstruction of examination; destruction or alteration of evidence	Credentials held by one person; undocumented hosting; no backups under independent control

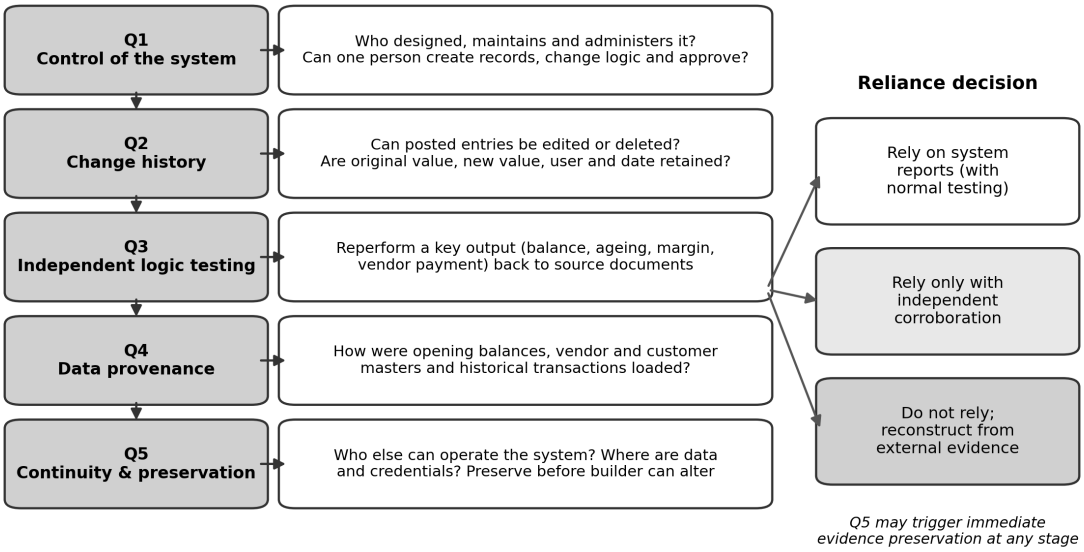
Note. Author's synthesis drawing on fraud-scheme categories in ACFE (2024, 2026) and the case build. The mechanisms raise opportunity; they do not by themselves indicate that fraud has occurred.

be normal, but from an examination standpoint it changes how much independent support is needed. It also reflects the insider-threat problem, in which technical knowledge and privileged access coincide (Akeju et al., 2018), and it parallels lessons from assessing security-critical directory systems offline, where the integrity of the evidence depends on how the system is captured (Ladapo et al., 2018).

An Examination Framework for Self-Built Systems

Fraud examiners do not need to become programmers to examine these systems. The first questions are the ones they already ask about records, access and evidence. The difference is that the answers may be buried inside a system no one outside the business has reviewed. Figure 2 presents five questions as a sequence leading to a graded reliance decision, and Table 3 sets out the procedures, evidence and standards associated with each.

Q1. Who built the system and who controls it? Identify who designed the application, who maintains it and who has administrative access. Ask whether the same person can create records, change the system logic and approve the transactions that flow through it. Concentrated access does not prove fraud, but it should shape the rest of the examination. Principles of role-based and identity-centric access control provide the benchmark (Ladapo et al., 2019;



Note. The questions are ordered for a typical engagement, but Q5 (preservation) should be addressed first where the builder is a subject of the examination.

Figure 2: Five-question examination framework for self-built systems and the resulting reliance decision

Table 3: *Examination procedures, evidence and reliance implications for self-built systems*

Question	*Core procedures*	*Evidence to obtain*	*If the answer is unfavourable*	*Related standard / guidance*
Q1 Control	Walkthrough of roles; list users and privileges; identify who can change code and data	User and privilege listing; hosting and repository access records	Treat all builder-touched records as higher risk; expand independent corroboration	COSO (2013) control activities; COBIT (ISACA, 2018)
Q2 Change history	Select posted transactions; request change history; test whether edits and deletions are logged	Audit-log extracts; database schema showing history tables	Document the limitation; do not rely on the absence of changes as evidence	PCAOB AS 1105; ISA 500
Q3 Logic	Reperform key calculations from source documents; compare to external confirmations	Source invoices, bank statements, third-party confirmations	Rely only on independently reperformed figures	PCAOB AS 1105 (IPE); ISA 500 para. 9
Q4 Provenance	Reconcile opening balances to prior records; trace sample of migrated masters	Migration files, prior spreadsheets or ledgers, reconciliation schedules	Treat pre-migration history as unverified; reconstruct from external sources	ISA 500; ACFE examination practice
Q5 Continuity	Identify data location and credentials; secure backups; forensic imaging where warranted	Hash-verified copies of database, code and configuration; custody log	Preserve immediately; restrict builder access if legally permissible	ISO/IEC 27037; NIST SP 800-86

Note. IPE = information produced by the entity. Procedures should be scaled to the engagement and applied subject to legal authority and the engagement's terms of reference.

Ogbole et al., 2021), and weak authentication practices, such as shared passwords, should be noted (Onche & Ogbonna, 2022).

Q2. What happens when a record changes? Select a transaction and ask to see its history. Can a posted entry be edited or deleted? Does the system record the original value, the new value, the user and the date? If not, document that limitation before relying on system-generated reports.

Q3. Has anyone tested the business logic independently? Choose an important output and trace it back to source. Reperform a customer balance, an ageing calculation, a margin figure or a vendor payment. A functioning application can still produce unsupported numbers. This is the self-built analogue of testing the accuracy and completeness of information produced by the entity (IAASB, 2009; PCAOB, 2010).

Q4. Where did the opening data come from? Small businesses may migrate into these applications from spreadsheets, notebooks or older systems. Ask how opening balances, vendor records, customer information and historical transactions were loaded. Errors introduced at migration can become accepted history, and so can manipulated records. Vendor-master integrity deserves particular attention, given its central role in payment schemes (Wedraogo et al., 2025).

Q5. What happens if the builder is unavailable? Establish who understands the application, where the data are stored, how credentials are managed and whether another person can preserve or operate the system. This becomes urgent if the builder is the subject of the examination. Evidence preservation, including forensic copies of the database, code and hosting configuration with documented chain of custody, may need to happen before that person can alter the application or its records (ISO/IEC, 2012; Kent et al., 2006).

Discussion

Presentation quality versus evidence quality

The central risk identified here is not that GenAI creates fraud. The technology does not create fraud by itself. The risk is that it can make weak or missing controls harder to see, because the finished system looks more formal than the process behind it. This reverses a heuristic that examiners and auditors have long relied on: that system-generated output from a structured application is more reliable than a hand-prepared schedule. For self-built systems, that heuristic holds only after the system's controls have been evaluated. The combination of automation bias (Parasuraman & Manzey, 2010) and polished AI output makes this especially important.

Implications for fraud examiners and auditors

Examiners should add a short system-provenance step to engagements involving small businesses: establish whether core records live in a commercial package, a spreadsheet or a self-built application, and if the last, apply the Table 3 procedures before relying on its output. Risk-based assurance approaches, which scale procedures to assessed risk and to data availability, fit this setting (Fadayomi et al., 2019). Where the builder is a subject, preservation should precede interviews.

Implications for small businesses and their advisers

Owners who build systems should treat control design as part of the build, not as an afterthought. A minimum control set would include individual user accounts, separation of vendor creation from payment approval, an immutable change log, a reconciled migration, and backups and credentials held by someone other than the builder. Fraud-awareness training,

which the ACFE associates with lower median losses (ACFE, 2026), and insider-threat awareness (Onche et al., 2024) complement these technical measures.

Implications for AI tool providers

Because users rarely request controls they do not know they need, tools that generate business applications could default to including audit trails, role separation and posting locks when the prompt concerns financial records. This would move part of the control burden from users' knowledge to design defaults.

Propositions for future research

The framework suggests testable propositions: (P1) GenAI-built financial systems in small businesses contain fewer default control features than commercial packages of comparable scope; (P2) examiners give greater evidentiary weight to polished system output than to equivalent hand-prepared schedules, independent of underlying control quality; (P3) the probability that a self-built system includes change logging depends more on the builder's control knowledge than on the AI tool used; and (P4) applying the five-question framework improves examiners' identification of unreliable system records.

Limitations

The framework derives from established theory and from one build by a trained examiner, which may make the case unrepresentative of typical owner-builders, who are likely to specify fewer controls. I have a family relationship with the case business, and no independent review of the system is reported here. The ACFE statistics are based on cases reported by Certified Fraud Examiners rather than on a random sample of organisations. The framework has not yet been validated across examinations; the propositions in Section 6.5 are intended to support that work.

Conclusion

Building the system for my father's business made the benefits of GenAI concrete. It let me turn knowledge of the business, finance and systems design into working software without a development team. For a small business that has relied for years on memory, spreadsheets and personal oversight, that can be a major improvement. It also made the control problem concrete. The AI did not tell me where access should be restricted, which changes needed to be logged, which financial relationships needed to reconcile or which inventory recommendation did not make sense. I had to know to ask.

Fraud examiners will see more systems built by people who were solving legitimate business problems rather than designing accounting software. By the time an examiner arrives, such an application may hold the vendor master, customer balances, transaction history and financial reports that everyone in the business treats as authoritative. The response does not require a new branch of computer science. It requires applying the fundamentals: establish who controls the records, find out whether changes leave a trail, trace important outputs to source evidence, understand where the data came from, and preserve the system early when one person has unusual control over it. GenAI has made it easier for small businesses to build their own systems. For examiners, the question is what they would need to see before trusting the records those systems produce.

Declarations

Funding. This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Conflict of interest. The author is a family member of the owner of the case business and designed and built the system described. The author declares no financial interest in any software product or vendor mentioned.

Ethics and consent. The business owner consented to the case description. No fraud was identified or alleged, and no personal data of customers, suppliers or employees are reported. [Confirm whether institutional ethics review or exemption applies.]

Data availability. Case materials contain commercially confidential information and are not publicly available.

Use of generative AI. Generative AI tools were used to build the software artefact discussed. [Disclose here any use of GenAI in preparing the manuscript, per the target journal's policy.]

Related manuscript. A companion manuscript on the operational-capability implications of the same case (Akande, 2026) has been submitted separately. The papers address distinct research questions and literatures; overlapping material is limited to the case description and a small number of adoption statistics.

References

[1] Ajayi, O., Alaka, O. B., & Tiamiyu, R. (2020). Essential trip making and mode substitution during COVID-19 movement restrictions in Nigerian cities. *IRE Journals, 4*(4), 442–465. https://doi.org/10.64388/IREV4I4-1722673

[2] Ajayi, O., Alaka, O. B., & Tiamiyu, R. (2023). Willingness to pay for shared and digitally booked transport among low-income commuters after fuel price increases. *International Journal of Advanced Multidisciplinary Research and Studies, 3*(6), 3059–3070.

[3] Akande, A. (2026). *From task assistance to operational infrastructure: Generative AI and the expansion of operational capabilities in small and medium-sized enterprises* [Manuscript submitted for publication].

[4] Akeju, B., Edivri, J., Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., & Abolaji, T. O. (2018). Conceptual model for insider threat classification and risk modeling in complex digital systems. *IRE Journals, 1*(9), 476–492. https://doi.org/10.64388/IREV1I9-1713778

[5] Alaka, O. B., Ajayi, O., & Bolaji, O. (2020). Geospatial assessment of access to health facilities over unpaved rural road networks. *International Journal of Multidisciplinary Research and Growth*

Evaluation, 1(5), 1199–1214. https://doi.org/10.54660/.IJMRGE.2020.1.5.1199-1214

[6] Alaka, O. B., Ajayi, O., & Bolaji, O. (2022). Mobile network coverage and road surface condition as joint constraints on digitally booked transport beyond state capitals. *International Journal of Engineering and Modern Technology, 8*(5), 142–168. https://doi.org/10.56201/ijemt.v8.no5.2022.pg142.168

[7] Alaka, O. B., Bolaji, O., & Tiamiyu, R. (2022). Mapping flood-exposed road segments from freely available satellite imagery during the 2022 flood season. *IIARD International Journal of Geography and Environmental Management, 8*(2), 117–143. https://doi.org/10.56201/ijgem.v8.no2.2022.pg117.143

[8] Alaka, O. B., & Tiamiyu, R. (2019). Repeated-load performance of concrete produced with locally sourced aggregates for road and drainage structures. *IRE Journals, 2*(10), 673–691. https://doi.org/10.64388/IREV2I10-1722671

[9] Alaka, O. B., Tiamiyu, R., Ajayi, O., & Bolaji, O. (2023). Multi-criteria prioritization of rural road rehabilitation using surface condition, population, and market-access indicators. *International Journal of Advanced Multidisciplinary Research and Studies, 3*(6), 3047–3058.

[10] Alaka, O. B., Tiamiyu, R., & Bolaji, O. (2021). Spatial clustering of road traffic crash locations on intercity corridors using national road safety records. *International Journal of Multidisciplinary Research and Growth Evaluation, 2*(6), 1086–1101. https://doi.org/10.54660/.IJMRGE.2021.2.6.1086-1101

[11] Aliliele, C., Eboh, E. E., & Oluwo, K. (2024). Advances in variance analytics for cost control in manufacturing and industrial enterprises. *International Journal of Advanced Multidisciplinary Research and Studies, 4*(6), 3163–3185. https://doi.org/10.62225/2583049X.2024.4.6.6012

[12] Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*. ACFE.

[13] Association of Certified Fraud Examiners. (2026). *Occupational fraud 2026: A report to the nations*. ACFE.

[14] Bola-Sadipe, D., Aliliele, C., & Eboh, E. E. (2019). Conceptual model for strategic accounting systems strengthening financial transparency and regulatory compliance. *IRE Journals, 3*(6), 535–564. https://doi.org/10.64388/IREV3I6-1715327

[15] Bolaji, O., & Ajayi, O. (2021). Loading and unloading activity at informal roadside motor parks and its effect on arterial traffic flow. *IIARD International Journal of Geography and Environmental Management, 7*(2), 54–77. https://doi.org/10.56201/ijgem.vol.7.no2.2021.pg54.77

[16] Bolaji, O., Alaka, O. B., Ajayi, O., & Tiamiyu, R. (2019). Field condition assessment of roadside drainage and culvert structures on urban arterials in southwestern and north central Nigeria. *IRE Journals, 3*(1), 663–683. https://doi.org/10.64388/IREV10I2-1722674

[17] Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control—Integrated framework*. COSO.

[18] Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.

[19] Eboh, E. E., Aliliele, C., & Odihi, F. (2025). Advances in financial governance and accountability systems in small and medium enterprises. *International Journal of Advanced Multidisciplinary Research and Studies, 5*(6), 2223–2245. https://doi.org/10.62225/2583049X.2025.5.6.6013

[20] Fadayomi, O., Abolaji, T. O., Edivri, J., Ogbole, J. I., Okoruwa, P. O., & Akeju, B. (2019). Risk-based cybersecurity assurance and data availability: Limitations, advances and future research opportunities. *IRE Journals, 2*(12), 602–617. https://doi.org/10.64388/IREV2I12-1713779

[21] Fadero, S., Oyesiji, S. O., Nwakamma, S., & Jooda, D. (2018). IT governance frameworks (COBIT/ITIL) and their impact on regulatory compliance in Nigerian insurance firms. *IRE Journals, 2*(5), 478–496. https://doi.org/10.64388/IREV2I5-1722619

[22] International Auditing and Assurance Standards Board. (2009). *International Standard on Auditing 500: Audit evidence*. IFAC.

[23] ISACA. (2018). *COBIT 2019 framework: Introduction and methodology*. ISACA.

[24] ISO/IEC. (2012). *ISO/IEC 27037:2012 Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence*. International Organization for Standardization.

[25] Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86

[26] Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2018). Lessons learned from offline assessment of security-critical systems: The case of Microsoft Active Directory. *IRE Journals, 2*(6), 277–299. https://doi.org/10.64388/IREV2I6-1717205

[27] Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2019). Implementation of Active Directory for efficient management of enterprise networks. *IRE Journals, 3*(4), 608–627. https://doi.org/10.64388/IREV3I4-1717206

[28] Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2024). Keeping humans in the loop: Human-centered automated annotation with generative AI. *International Journal of Multidisciplinary Futuristic Development, 5*(1), 81–95.

[29] National Federation of Independent Business Research Center. (2025). *Small business and technology survey*. NFIB Research Center.

[30] Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., Abolaji, T. O., Edivri, J., & Akeju, B. (2021). Conceptual model for identity-centric Zero Trust Architecture in enterprise security governance. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7*(5), 393–415.

[31] Onche, V. O., & Ogbonna, C. S. (2022). Password practices, authentication behaviour, and data-protection compliance among secretarial professionals in higher education. *International Journal of Multidisciplinary Research and Growth Evaluation, 3*(6), 1001–1015. https://doi.org/10.54660/.IJMRGE.2022.3.6.1001-1015

[32] Onche, V. O., Ogbonna, C. S., & Adegbite, M. P. (2024). Effectiveness of cybersecurity awareness training on insider-threat behavior among university administrators: An integrative academic review. *International Journal of Computer Science and Mathematical Theory, 10*(2), 117–144. https://doi.org/10.56201/ijcsmt.v10.no2.2024.pg117.144

[33] Panko, R. R. (1998). What we know about spreadsheet errors. *Journal of End User Computing, 10*(2), 15–21.

[34] Parasuraman, R., & Manzey, D. H. (2010). Complacency and bias in human use of automation: An attentional integration. *Human Factors, 52*(3), 381–410. https://doi.org/10.1177/0018720810376055

[35] Pearce, H., Ahmad, B., Tan, B., Dolan-Gavitt, B., & Karri, R. (2022). Asleep at the keyboard? Assessing the security of GitHub Copilot's code contributions. In *2022 IEEE Symposium on Security and Privacy* (pp. 754–768). IEEE. https://doi.org/10.1109/

SP46214.2022.9833571

[36] Perry, N., Srivastava, M., Kumar, D., & Boneh, D. (2023). Do users write more insecure code with AI assistants? In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2785–2799). ACM. https://doi.org/10.1145/3576915.3623157

[37] Public Company Accounting Oversight Board. (2010). *AS 1105: Audit evidence*. PCAOB.

[38] Sakyi, J. K., Nnabueze, S. B., Filani, O. M., & Okojie, J. S. (2023). Revenue assurance strategies leveraging artificial intelligence and big data in service-intensive organizations. *International Journal of Multidisciplinary Evolutionary Research, 4*(2), 58–75. https://doi.org/10.54660/IJMER.2023.4.2.58-75

[39] Silic, M., & Back, A. (2014). Shadow IT – A view from behind the curtain. *Computers & Security, 45*, 274–283. https://doi.org/10.1016/j.cose.2014.06.007

[40] Tiamiyu, R., & Alaka, O. B. (2020). Routing of motorcycle dispatch deliveries on congested and poorly connected urban networks in Lagos. *International Journal of Multidisciplinary Research and Growth Evaluation, 1*(5), 1183–1198. https://doi.org/10.54660/.IJMRGE.2020.1.5.1183-1198

[41] Tiamiyu, R., Alaka, O. B., & Ajayi, O. (2021). Emergency response coverage gaps on intercity highways in Kwara State: A network service-area analysis. *International Journal of Multidisciplinary Research and Growth Evaluation, 2*(6), 1102–1118. https://doi.org/10.54660/.IJMRGE.2021.2.6.1102-1118

[42] Tiamiyu, R., Alaka, O. B., Bolaji, O., & Ajayi, O. (2023). Combining field survey and open geospatial data for transport infrastructure decision support in data-scarce regions. *International Journal of Advanced Multidisciplinary Research and Studies, 3*(6), 3071–3084.

[43] U.S. Chamber of Commerce Technology Engagement Center. (2025). *Empowering small business: The impact of technology on U.S. small business*. U.S. Chamber of Commerce.

[44] Wedraogo, L., Essandoh, S., Sakyi, J. K., Ibrahim, A. K., Okafor, C. M., Babalola, A. S., & Adenuga, M. A. (2025). Analysis of vendor management practices and their effects on supply chain performance. *International Journal of Multidisciplinary Futuristic Development, 6*(1), 42–54. https://doi.org/10.54660/IJMFD.2025.6.1.42-54

[45] Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal, 74*(12), 38–42.