Institutionalising Digital Audit Capability Framework in the Malaysian Public Sector: Technology Readiness, Digital Governance and Auditor Competency

Zuraidah Mohd Sanusi[1], Yusarina Mat Isa[2*], Nur Aima Shafie[1], Fazlida Mohd Razali[1], Aziatul Waznah Ghazali[3], Soliha Sanusi[3], Mohd Daniel Mohd Nassir[1]

[1]Accounting Research Institute, Universiti Teknologi MARA, Shah Alam, Malaysia

[2]Faculty of Accountancy, Universiti Teknologi MARA Cawangan Selangor, Kampus Puncak Alam, Bandar Puncak Alam, Malaysia

[3]School of Accounting Studies, Faculty of Economics and Management, Universiti Kebangsaan Malaysia, Bangi, Selangor

***Corresponding Author**

DOI: https://doi.org/10.47772/IJRISS.2026.100700584

Received: 26 July 2026; Accepted: 31 July 2026; Published: 08 August 2026

ABSTRACT

Digital transformation is changing how governments process financial transactions, manage records, assess risk and demonstrate accountability. Public-sector internal audit functions are progressively replacing fragmented manual procedures with electronic working papers, data analytics, dashboards and audit management systems. However, technology implementation alone does not create an effective digital audit function because its value depends on reliable data, appropriate governance, competent auditors and organisational support. Drawing on institutional theory, this qualitative study examines the development of digital audit capability in Malaysian public-sector internal audit functions and proposes an integrated framework based on technology readiness, digital governance and auditor competency. The study draws on semi-structured interviews with senior public-sector internal audit representatives. Thematic analysis identifies system integration, data accessibility, trustworthy digital processes, multidisciplinary competency and management commitment as the main conditions supporting digital audit capability. The Malaysian context demonstrates a progressive but uneven transition among government internal audit departments towards audit management systems, online audit workflows and dashboard-based monitoring. The proposed framework positions digital auditing as an institutional capability-development process rather than a technology-acquisition exercise. The study contributes a context-sensitive framework that can guide government agencies in strengthening digital audit implementation, audit effectiveness and public accountability.

Keywords: digital auditing, public sector, technology readiness, digital governance, auditor competency, institutional theory, Malaysia

INTRODUCTION

Digital transformation has changed how governments administer public resources, maintain records and communicate financial information (Manita, Elommal, Baudier & Hikkerova, 2020; OECD, 2025). Payments, procurement, payroll, revenue collections and asset transactions are some of the activities increasingly processed through electronic platforms rather than physical documentation. This development provides public-sector organisations with faster processing, extensive digital records and greater opportunities for analytical monitoring (OECD, 2019). At the same time, it increases the volume, complexity and interconnectedness of the information that auditors must examine. Government audit functions must therefore adapt their methods to remain effective in a technology-intensive administrative environment.

Traditional public-sector internal auditing has depended substantially on document examination, interviews, manual calculations and sample-based verification (IIA, 2024; INTOSAI, 2019). These procedures remain necessary where evidence requires contextual interpretation, physical confirmation or professional evaluation. However, they are increasingly insufficient as the dominant audit approach when government agencies process millions of transactions through integrated systems (OECD, 2024, 2025). Auditors are now expected to analyse broader datasets, evaluate automated controls, identify unusual transaction patterns and communicate findings within shorter reporting periods (Alles

et al., 2006; Appelbaum et al., 2017; Earley, 2015). Digital auditing therefore offers a means of responding to these requirements across successive phases of the audit cycle.

Existing digital audit studies frequently focus on individual technologies, technology acceptance or quantitative associations between system use and auditor performance (Alles, 2015; Veerankutty et al., 2018). Such studies provide important evidence but may not sufficiently explain how auditors experience implementation challenges or how technology, governance and competency interact in practice (Salijeni et al., 2019). To address this gap, a qualitative approach is valuable because it captures institutional realities, professional interpretations and implementation conditions that cannot be adequately represented through numerical indicators alone (Creswell & Poth, 2018; Patton, 2015). Interviews with experienced public-sector auditors can reveal how access, system design, security and professional judgement shape actual audit work. Document review can complement these perspectives by identifying formal systems, policies and practices.

This study therefore aims to examine how digital audit capability can be developed within the Malaysian public sector through a qualitative inquiry. The inquiry is informed by institutional theory, which directs attention to the regulative, normative and cultural-cognitive conditions under which new audit practices become embedded in government organisations (DiMaggio & Powell, 1983; Scott, 2014). It draws on semi-structured interviews with internal auditors from government agencies supported by a review of documents relevant to digital audit implementation. The study seeks to identify the main technological, governance, competency and organisational conditions influencing digital audit implementation. It also develops an integrated qualitative framework that reflects both internal auditors' experience and documented public-sector practices. The framework is intended to support government agencies at different levels of digital maturity, particularly in performing internal audit engagements within those agencies. The remainder of the paper reviews the relevant literature, introduces the theoretical perspective, describes the research methodology, presents the findings and the proposed framework, and concludes with the implications of the study.

BACKGROUND OF THE STUDY

Digital auditing refers to the systematic application of digital technologies to audit planning, risk assessment, evidence collection, analytical testing, documentation, reporting and follow-up (Lewis, Neiberline & Steinhoff, 2014). Its applications include audit management systems, computer-assisted audit techniques, data-analytics software, business-intelligence platforms, electronic working papers, document-management systems and dashboards (Appelbaum et al., 2017; Earley, 2015; Moffitt et al., 2018). These technologies can automate routine procedures, extend transaction coverage and allow auditors to focus more directly on higher-risk matters (Leocádio et al., 2024; IIA, 2026a). Electronic review records and system-generated audit trails can also improve the traceability and consistency of audit work. Nevertheless, digital tools contribute to audit quality only when they are aligned with reliable information and professional judgement.

Digital auditing transformation is more extensive than converting physical documents into electronic files. It changes how evidence is accessed, how procedures are reviewed, how responsibilities are allocated and how findings are communicated to management and auditees (Kokina & Davenport, 2017; Leocádio et al., 2024). This transformation is described as a movement towards more efficient, transparent and evidence-based assurance supported by analytics, automation, artificial intelligence and cybersecurity (Manita et al., 2020; Salijeni et al., 2019). The auditor's role has also consequently moved beyond routine checking towards risk interpretation, control evaluation and governance improvement. Thus, this transformation is organisational, professional and methodological as much as it is technological.

Technology acquisition alone does not create digital audit capability (Almaqtari, 2024). A government agency may implement an advanced audit platform but obtain limited benefits when data are incomplete, systems remain disconnected or users lack relevant skills (OECD, 2020, 2024). A technically capable audit team may also be constrained when data ownership is uncertain, or system access requires lengthy administrative approval. Digital audit transformation should consequently be understood as the development of an organisational capability rather than the adoption of isolated software (Alles, 2015; Salijeni et al., 2019). This capability emerges through the alignment of technology, governance, professional competency and organisational support.

Digital audit capability refers to the ability of an audit function to use digital systems, reliable data, institutional controls and professional expertise to deliver timely and value-adding assurance (IIA, 2024, 2026a). It includes the capacity to access relevant information, apply suitable analytical procedures, protect sensitive evidence and document audit work consistently. It also includes the ability to monitor findings, identify recurring weaknesses and support timely corrective action. Capability should therefore be evaluated through audit outcomes rather than the number of applications acquired. An organisation demonstrates digital audit capability when digital resources strengthen audit coverage, evidence quality, reporting timeliness and management accountability.

The Malaysian public sector provides a relevant setting for examining this digital auditing transformation (Mokhtar et al., 2024; Shafie et al., 2023). Government processes are increasingly conducted through electronic systems, while internal audit departments are moving from disconnected manual procedures towards electronic working papers, online auditee communication and audit management platforms (IIA, 2024, 2026a). The level of implementation differs across ministries, departments, statutory bodies and related agencies. Some audit units have introduced dedicated systems, while others continue to use combinations of spreadsheets, shared drives and locally developed applications. The overall direction nevertheless indicates a progressive movement towards more integrated digital audit management that needs to be further understood. This movement does not occur in an institutional vacuum; central agencies, professional standards and government-wide digitalisation policies shape the pace and form of adoption across audit units (Agostino et al., 2022).

LITERATURE REVIEW

Digital Auditing

The evolution of digital auditing can be understood as a progression from manual verification towards integrated digital assurance (Knudsen, 2020; Lewis, Neiberline & Steinhoff, 2014). Traditional audit work depended on physical records, manual calculations and limited sample testing, while the emergence of computerised accounting systems required auditors to understand electronic records, automated controls and system-generated reports (Rezaee et al., 2002; Vasarhelyi et al., 2012). Computer-assisted audit techniques subsequently enabled audit teams to extract, filter and analyse digital information more systematically. More recent developments include automated exception testing, business intelligence, continuous monitoring and artificial-intelligence-assisted procedures.

Digital auditing represents a more advanced stage than basic audit automation. Automation transfers repetitive activities from human auditors to software, whereas digital auditing combines technology, governance, professional review and institutional accountability (Kokina et al., 2025; Leocádio et al., 2024). It enables the examination of larger datasets while preserving the auditor's control over evidence quality and final conclusions (Li & Goel, 2025; Moffitt et al., 2018). This development of digital auditing changes audit planning, work allocation, documentation and communication. It also increases collaboration among auditors, accountants, system owners, data analysts and information-technology specialists.

Digital audit capability differs from technology adoption. Technology adoption indicates that an organisation has introduced a particular tool or platform, while capability concerns whether the organisation can convert that investment into improved assurance outcomes (IIA, 2026a, 2026b). An audit unit may possess analytical software but remain unable to use it effectively because data are unavailable or inconsistently structured (Alles, 2015; Salijeni et al., 2019). An audit unit may also implement an audit management system that reproduces existing forms without improving risk assessment, evidence analysis or follow-up. Digital capability is therefore reflected in the effective application and integration of technological resources in performing audit work. Viewed in institutional terms, capability develops when digital tools are absorbed into the rules, routines and shared understandings of the audit function rather than remaining discretionary additions to established practice (Salijeni et al., 2019; Scott, 2014).

Technology Readiness

Technology readiness forms the operational foundation of digital audit capability. It includes audit management systems, financial information platforms, data extraction applications, electronic working papers, dashboards and secure storage. A suitable audit management system should support planning, risk assessment, fieldwork, review, reporting, auditee responses and monitoring (Appelbaum et al., 2017; Earley, 2015). It should also provide a consistent audit trail and preserve institutional records beyond individual assignments. Its effectiveness nevertheless depends on usability, data quality and interoperability with financial and operational systems.

Analytical technologies such as data analytics allow auditors to examine broader transaction populations and identify potential exceptions (Kokina et al., 2025; IIA, 2026a). Applications of data analytics may detect duplicate payments, unusual transaction amounts, repeated vendors, missing approvals or transactions processed outside expected conditions. These procedures can improve risk prioritisation and reduce the time devoted to repetitive checking (Cao et al., 2015; Earley, 2015; Richins et al., 2017). However, analytical results remain dependent on the completeness, accuracy and consistency of the underlying data. Poor data quality may create misleading alerts or conceal significant control weaknesses.

Interoperability of technology is particularly important in government because agencies frequently operate separate systems for finance, payroll, procurement, assets, revenue and programme administration (OECD, 2019, 2024, 2025;

Appelbaum et al., 2017). Auditors may need to obtain multiple extracts and reconcile inconsistent formats before conducting analysis. This process reduces efficiency and may affect the reliability of comparisons across agencies. Technology readiness therefore requires more than access to individual applications. It requires the ability to obtain and combine information from relevant systems within a controlled technological environment.

Digital Governance

Digital governance provides the institutional safeguards for technology-supported auditing (OECD, 2019). It determines who owns the data, who may access them, how extracts are validated and who remains accountable for system-assisted decisions. These matters are especially important in public-sector auditing because evidence may contain sensitive financial, operational and personal information (Almaqtari, 2024; IIA, 2024). Weak governance may expose agencies to unauthorised access, inappropriate use and unreliable findings. Strong governance enables legitimate audit work while protecting confidentiality, integrity and institutional accountability.

Cybersecurity, privacy and digital records management form important elements of digital governance (NIST, 2024). Audit systems may contain confidential findings and detailed information about control weaknesses. Access controls, authentication, encryption, system logs, backup and incident-response procedures are therefore necessary. Digital governance should treat cybersecurity, confidentiality, professional conduct and controlled records management as integral components of audit implementation (IIA, 2026c; OECD, 2019). These controls should be embedded in audit processes rather than treated as separate technical responsibilities.

Transparency and explainability are also important because audit conclusions must be reviewed, communicated and defended (Li & Goel, 2025; Almaqtari, 2024). Auditors should understand how an analytical output has been generated and should be able to trace it to the relevant data and decision rules. Responsibility should remain clearly assigned among auditors, system administrators, data owners and technical specialists (Issa et al., 2016; Kokina & Davenport, 2017; IIA, 2024). Technology may assist the assessment, but it cannot assume accountability for an inappropriate audit conclusion. Digital governance must therefore support innovation without weakening the professional responsibility of auditors.

Auditor Competency

Auditor competency represents the human dimension of digital audit capability (IIA, 2024, 2026b). Technology may identify patterns, but auditors must determine whether the resulting information is relevant, reliable and sufficient. Digital competency includes literacy in electronic audit processes, data validation, analytical interpretation, information-systems knowledge and cybersecurity awareness (Earley, 2015; Richins et al., 2017). It also includes ethical judgement, communication and professional scepticism. These competencies enable auditors to use technology without becoming excessively dependent on automated outputs.

Not every public-sector auditor needs to become a programmer or data scientist. However, all auditors should understand the origin, structure and limitations of the data used in their assignments. More advanced procedures may require multidisciplinary teams involving data analysts, information-systems auditors and cybersecurity specialists (Leocádio et al., 2024; Li & Goel, 2025; Appelbaum et al., 2017). Such teams combine professional audit knowledge with technical capability. This approach is more practical than expecting every auditor to possess identical specialised skills.

Professional judgement remains central to digital auditing (IIA, 2024). A system-generated exception may represent an error, a control weakness, non-compliance or a legitimate operational variation. The auditor must examine its context, materiality and supporting evidence before reporting a finding (Kokina et al., 2025; Issa et al., 2016; Kokina & Davenport, 2017). Technology expands the scope and speed of analysis but does not independently determine the significance of a transaction. The appropriate approach is technology-supported judgement rather than technology-replaced judgement. These expectations are reinforced by professional bodies and standard setters, whose guidance exerts the normative pressure through which digital skills gradually become part of what is required of a competent public-sector auditor (DiMaggio & Powell, 1983; IIA, 2024).

UNDERPINNING THEORY: AN INSTITUTIONAL PERSPECTIVE

This study is underpinned by institutional theory, which holds that organisational structures and practices are shaped not only by considerations of technical efficiency but also by the pursuit of legitimacy within an institutional environment (DiMaggio & Powell, 1983). The theory identifies three pillars through which practices become established. The regulative pillar comprises rules, mandates and sanctions; the normative pillar comprises professional standards and expectations;

and the cultural-cognitive pillar comprises the shared understandings and routines that members of an organisation take for granted (Scott, 2014). Organisations subject to common coercive, normative and mimetic pressures tend to adopt similar structures and practices, although the depth of adoption varies with their resources and internal routines (DiMaggio & Powell, 1983).

Institutional theory suits the present study for three reasons. First, public-sector internal audit functions operate within a dense institutional environment of central agency directives, government-wide digitalisation policies and professional auditing standards, so their uptake of digital practices depends on legitimacy conferred by these institutions as much as on technical merit (Agostino et al., 2022). Second, the three pillars map closely onto the conditions examined in this study: regulative arrangements correspond to digital governance, normative expectations correspond to professional competency standards, and cultural-cognitive routines correspond to the everyday use of technology within audit work. Third, the theory helps explain why implementation varies across agencies operating under a common policy direction, since agencies face similar pressures but differ in resources, routines and absorptive capacity.

Viewed through this lens, developing digital audit capability is a process of institutionalisation in which technology, governance and competency must be aligned and embedded so that digital auditing becomes a durable organisational practice rather than a discretionary project. This perspective informs the design of the study, the interpretation of the findings and the structure of the framework proposed in this study.

RESEARCH METHODOLOGY

This study adopts a cross-sectional exploratory qualitative design to examine the conditions influencing digital audit capability in the Malaysian public sector. A qualitative approach is appropriate because digital auditing involves institutional practices, professional experiences and implementation challenges that require contextual interpretation (Creswell & Poth, 2018; Patton, 2015). The study seeks to understand how public-sector internal auditors perceive current digital auditing practices, data-access issues, governance arrangements and competency needs. It also examines how institutional documents describe the systems and processes supporting digital auditing. The design of this study combines semi-structured interviews with document review to strengthen the depth and credibility of the analysis through methodological triangulation (Bowen, 2009).

The interview component draws on eleven senior public-sector internal auditors from various government agencies. The participants were selected purposively because they possessed direct knowledge of public-sector auditing, digital systems and institutional implementation issues, enabling the study to capture different professional perspectives. The use of purposive participants with direct audit experience strengthened the relevance of the evidence, although the findings are not intended to represent every Malaysian public-sector agency (Hennink & Kaiser, 2022; Guest et al., 2020; Patton, 2015). Semi-structured interviews were used to provide a consistent focus while allowing participants to explain their experiences in detail. The interview questions covered current digital audit practices, barriers to effective implementation, access to audit data, system transparency, responsibility, privacy and institutional readiness. Participants were also asked to identify factors contributing to successful digital audit implementation in Malaysia. The flexible format enabled the interviewer to explore relevant examples and clarify issues that emerged during each session. Interviews continued until the discussions no longer generated materially different information concerning the principal study questions, indicating that code saturation had been achieved. Participants received an information sheet explaining the purpose of the study, provided written informed consent and were assured of anonymity, with agencies and individuals identified only by generic role descriptions.

The interview evidence was analysed thematically (Braun & Clarke, 2006, 2021, 2022). A deductive, codebook-style approach was adopted, in which an initial coding template was derived from the literature on technology readiness, digital governance and auditor competency and was subsequently refined against the data, a variant that Braun and Clarke (2021, 2022) distinguish from fully inductive reflexive analysis. NVivo software was used to organise the transcripts and to support systematic word-based and code-based analysis of the qualitative evidence. Transcripts and interview notes were reviewed repeatedly to identify statements concerning technology, data, governance, competency, collaboration and audit outcomes. Initial codes were assigned to recurring issues such as system fragmentation, data availability, digital skills, security, responsibility and management support. Related codes were then grouped into broader themes representing the main dimensions of digital audit capability. Coding decisions and theme definitions were recorded throughout the analysis to maintain an audit trail, and emerging themes were discussed among the research team until agreement was reached, consistent with established trustworthiness criteria for thematic analysis (Lincoln & Guba, 1985; Nowell et al., 2017).

Document review was undertaken to triangulate and extend the interview evidence (Creswell & Poth, 2018; Bowen, 2009; Lincoln & Guba, 1985). One key document, the Digital Audit Manual, provided information on digital audit processes, audit systems, audit command language (ACL), Power BI, electronic records, continuous auditing and dashboard-based monitoring. Other documents related to the manual were further examined for evidence relating to technology infrastructure, data integration, competency, security and institutional coordination. These findings were compared with the internal auditors' interview themes to identify areas of convergence and difference. The resulting themes were then compared to determine whether documented systems and policies supported the experiences described by the internal auditors. Areas of convergence were used to strengthen the framework, while differences were interpreted as potential implementation gaps.

RESEARCH FINDINGS IN THE MALAYSIAN PUBLIC-SECTOR CONTEXT

Technology-Enabled Audit Operations

The qualitative analysis identified a progressive shift from manual and disconnected audit practices towards more integrated digital audit management. Interview participants recognised that digital systems can improve access to information, support broader testing and reduce repetitive audit work. They also viewed digital auditing as a means of enabling auditors to focus more closely on judgement, risk and higher-value analysis. However, the degree of implementation differed between institutions and audit activities. Digital audit transformation was therefore viewed as an ongoing process rather than a completed institutional change. This perception is consistent with the institutional view that new practices become durable only when they are embedded in organisational routines rather than introduced as discrete projects (Scott, 2014).

A central finding concerned the increasing role of audit management systems. Government internal audit departments are progressively using electronic platforms, shared databases and digital workflows for planning, working papers, findings and follow-up. Some agencies possess a dedicated audit management system, while others use combinations of spreadsheets, shared folders and electronic templates. Participants considered centralised audit documentation important for consistency, accessibility and continuity. They also recognised that electronic storage alone does not constitute full digital audit capability, but it does provide a beneficial tool for an integrated audit management system. The audit management system supports audit administration, audit management, self-assessment, reporting, feedback and monitoring dashboards. It allows audit activities, findings and auditee responses to be recorded and monitored through a structured digital process. It also supports management oversight by displaying planning information, audit progress, finding status and corrective actions. This represents a movement beyond basic electronic working papers towards institutional audit workflow management.

The findings nevertheless show that digital audit capability depends on an ecosystem rather than one application. An audit management system requires access to transaction data from financial, procurement, payroll, revenue and asset systems. Analytical applications such as ACL, Power BI and Excel applications support transaction analysis and visual reporting, while document-management systems support the retention of audit evidence. The effectiveness of this ecosystem depends on whether the systems are connected and whether information can be obtained in usable formats. A single platform cannot deliver comprehensive digital assurance when relevant data remain fragmented.

System fragmentation emerged as a major implementation challenge. Government institutions may use different applications, coding structures and data formats, making comparison and integration difficult. Auditors may need to obtain separate extracts and perform extensive reconciliation before conducting meaningful analysis. Such processes reduce timeliness and may create uncertainty about data completeness. The challenge is therefore not only the absence of technology but also the limited interoperability among existing systems.

Data accessibility was closely related to system fragmentation. Interview participants indicated that auditors require timely access to complete financial and operational information. However, responsibility for approving access may be distributed among system owners, information-technology units and operational departments. Concerns about confidentiality may further delay the release of data. Clear data-ownership and access protocols are therefore needed to balance legitimate audit requirements with privacy and security.

Accountable Digital Oversight

Transparency and accountability also emerged as important governance themes. Auditors need to understand how analytical outputs are generated and who is responsible for validating the information used. System owners, data

specialists and auditors may each contribute to a digital audit process, but the final audit conclusion must remain the responsibility of authorised audit professionals. Automated tools should support rather than obscure the reasoning behind a finding. Explainable procedures improve the ability of auditors to defend conclusions and communicate them to auditees.

The evidence also highlighted the importance of data quality. Digital audit tools may generate rapid results, but those results can be misleading when source data contain errors, missing fields or inconsistent classifications. Auditors must understand how data were produced and whether transformations occurred before extraction. Data validation should consequently form part of audit planning rather than a technical activity completed separately. Reliable digital auditing begins with reliable data.

Management support was consistently associated with successful transformation. Digital audit implementation requires investment, access approvals, training and cooperation between different organisational units. Senior leadership can resolve barriers that individual audit teams cannot address independently. Management also influences whether digital auditing is treated as a strategic accountability initiative or a limited information-technology project. Visible leadership support increases the likelihood that technological, governance and competency changes are implemented together. In institutional terms, visible leadership commitment also signals that digital auditing carries organisational legitimacy, encouraging units to align their routines with the new practices (DiMaggio & Powell, 1983).

Organisational resistance is recognised as another implementation issue. Auditors may be comfortable with established procedures and may view new systems as increasing administrative work. Auditees may also perceive continuous monitoring or data-driven testing as intrusive. Effective change management requires communication, participation and practical demonstration of benefits. Pilot projects can help users understand how digital systems reduce repetitive work and improve the consistency of follow-up.

Digitally Competent Auditors

Competency gaps represented another central challenge for public-sector internal auditors in the context of digital auditing. Participants recognised that auditors possess different levels of confidence and experience in using analytical and information-system applications. Basic system training may help officers navigate a platform but may not develop their ability to formulate analytical questions or interpret complex results. Digital auditing requires a combination of audit knowledge, technological understanding and professional judgement. Training should therefore be aligned with actual audit tasks rather than limited to software functions. The findings also support the development of multidisciplinary audit teams. General auditors contribute knowledge of controls, regulations and organisational processes, while technical specialists contribute analytics, systems and cybersecurity expertise.

Cybersecurity, privacy and confidentiality were also identified as essential implementation conditions. Digital audit records may contain sensitive financial information, personal data and evidence of institutional vulnerabilities. Participants recognised that wider access and remote auditing may increase exposure when controls are insufficient. Secure authentication, access restrictions, data-transfer procedures and approved storage are therefore necessary. Security should be incorporated into system and workflow design from the beginning.

The above findings indicate that public-sector agencies operate at different levels of digital maturity. Large central institutions may have integrated systems, specialised officers and stronger financial resources, while smaller agencies may rely on basic tools and limited technical support. Thus, government agencies require a phased approach that reflects their risk exposure, size and existing capability. A framework may provide guidance that establishes minimum standards while allowing flexibility in digital audit implementation. The uneven maturity observed across agencies also illustrates the institutional argument that organisations facing similar pressures respond differently according to their resources and routines (Scott, 2014), a pattern that the proposed framework seeks to accommodate.

Digital Audit Capability Framework

The findings indicate that technology alone cannot produce effective digital assurance. Digital auditing depends on the availability of reliable data, appropriate governance and control arrangements, and auditors who are capable of interpreting technology-generated evidence and exercising professional judgement. Digital audit capability therefore emerges from the alignment of three interrelated dimensions: technology readiness, digital governance and auditor competency. These dimensions are supported by two overarching enabling conditions: management commitment and organisational collaboration. In institutional terms, the framework interprets capability development as a process of institutionalisation in which governance supplies the regulative foundation, professional standards and training supply the normative foundation,

and routine technology use supplies the cultural-cognitive foundation of digital audit practice (DiMaggio & Powell, 1983; Scott, 2014). Figure 1 presents the proposed Digital Audit Capability Framework, which synthesises the findings discussed in the earlier section.

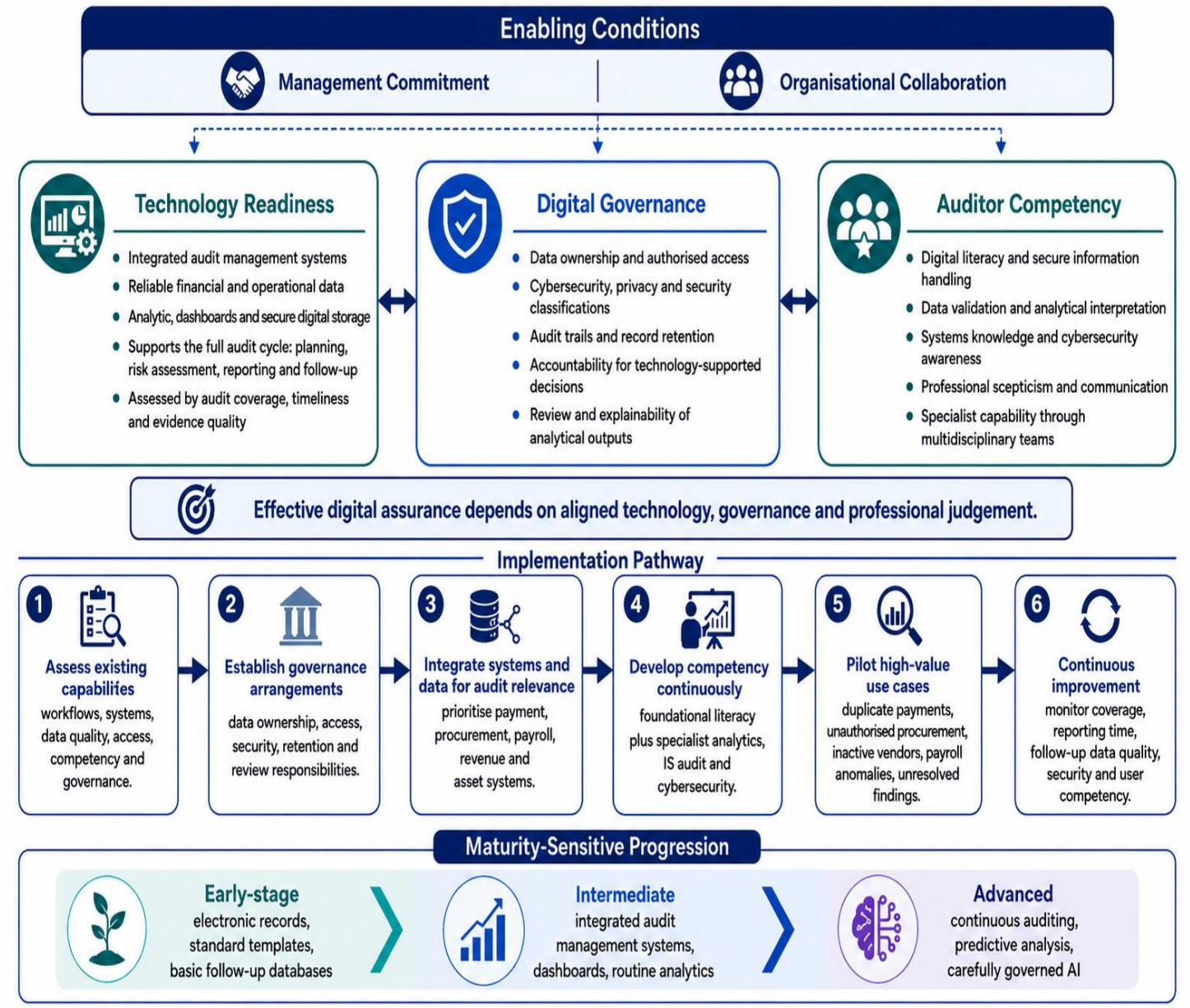

Figure 1: Proposed Digital Audit Capability Framework

At the core of the framework, technology readiness provides the operational foundation for digital audit implementation. It encompasses integrated audit management systems, reliable financial and operational data, analytical applications, dashboards and secure digital storage. These technological resources should support the entire audit cycle, including planning, risk assessment, audit testing, documentation, reporting and follow-up. They should also facilitate the controlled exchange of information across relevant government systems. However, technology readiness should not be assessed solely by the number of systems or applications introduced. Its effectiveness should instead be evaluated in terms of expanded audit coverage, improved timeliness and enhanced quality of audit evidence.

The second core dimension, digital governance, provides the institutional safeguards required for the responsible and trustworthy use of technology in auditing. It includes clear arrangements for data ownership, authorised access, cybersecurity, privacy, security classification, audit trails, record retention and accountability for technology-supported decisions. Governance arrangements should specify who is responsible for validating extracted data, approving analytical procedures and reviewing technology-generated outputs. They should also preserve the auditor's responsibility for the final audit conclusion. In addition, analytical processes should be sufficiently documented and explainable so that auditors can demonstrate how significant findings and exceptions were generated. These arrangements strengthen confidence in the reliability, transparency and defensibility of digital audit findings.

The third core dimension, auditor competency, converts technological resources and digital information into meaningful professional assurance. It includes digital literacy, data-validation skills, analytical interpretation, information-systems knowledge, cybersecurity awareness, communication and professional scepticism. Auditors must be able to determine whether a system-generated exception is valid, material and adequately supported by audit evidence. Competency development should therefore combine technical training with realistic audit cases, professional judgement and secure information-handling practices. While all auditors require foundational digital literacy, selected officers may develop specialist expertise in data analytics, information-systems auditing or cybersecurity. Managers also require the ability to interpret dashboards, review analytical outputs and oversee technology-supported audit decisions. More advanced capability may therefore be developed through multidisciplinary teams rather than through identical training for every auditor.

The three core dimensions are reinforced by management commitment and organisational collaboration. Senior management determines whether sufficient resources are allocated to audit systems, training, data access and technical support. Leadership also shapes whether digital auditing is treated as an institutional governance priority or merely as a technical initiative. Digital audit transformation is unlikely to succeed when it is assigned solely to information-technology personnel without clear audit ownership and professional oversight. Management should therefore position digital auditing as part of the organisation's broader governance, accountability and risk-management agenda. Organisational collaboration complements management commitment by facilitating cooperation among internal audit, finance, operations, information technology, data-management units and other relevant stakeholders. Such collaboration is essential because digital audit implementation depends on access to reliable data, shared definitions, technical assistance and coordinated responsibilities. Collaboration with universities, professional bodies and central government institutions may also strengthen the availability of relevant training, specialist expertise and implementation guidance. Together, management commitment and organisational collaboration create the enabling environment within which the three core dimensions can operate effectively.

The framework translates these dimensions into a six-stage implementation pathway. The first stage is to assess existing capabilities. Agencies should evaluate current audit workflows, available systems, data quality, access arrangements, staff competency and governance practices. The assessment should also identify high-risk audit areas in which digital procedures may generate the greatest value. Conducting this assessment before acquiring new technology allows agencies to identify capability gaps and reduces the risk of introducing systems without adequate organisational preparation. The second stage is to establish governance arrangements. Before wider data integration or automated testing is introduced, agencies should define data ownership, access rights, security classifications, retention requirements and review responsibilities. Analytical procedures should be properly documented and subjected to professional review. The respective responsibilities of auditors, system administrators and data specialists should also be clearly specified. Establishing these arrangements provides a controlled and accountable foundation for more advanced digital audit applications.

The third stage is to integrate systems and data according to audit relevance. Integration should be driven by audit objectives and risk exposure rather than by technical expansion alone. Priority may be given to systems relating to payments, procurement, payroll, revenue and assets because these areas typically involve high transaction volumes and significant control risks. Where feasible, agencies should develop common data definitions and standardised extraction procedures. Audit management systems should also connect planning, evidence, findings, auditee responses and follow-up activities. Effective integration can reduce repeated manual reconciliation, strengthen audit trails and improve management visibility over the audit process. The fourth stage is to develop competency continuously. Competency development should take place throughout implementation rather than being treated as a one-off activity. All auditors should receive training in foundational digital literacy, secure information handling and the appropriate use of analytical tools. Selected personnel may receive advanced development in data analytics, information-systems auditing and cybersecurity. Audit managers should also be equipped to interpret dashboards, challenge analytical results and supervise technology-supported audit decisions. Continuous competency development ensures that technological capability remains aligned with professional standards and audit judgement.

The fifth stage is to pilot high-value use cases. Initial implementation should concentrate on practical applications that can generate visible and measurable benefits. Suitable examples include the detection of duplicate payments, unusual procurement patterns, inactive vendors, payroll anomalies and unresolved audit findings. Pilot projects allow agencies to test data quality, system functionality, governance arrangements and staff readiness before wider implementation. They also provide practical evidence that can strengthen organisational support for further digitalisation. Lessons learned from pilot projects should be documented and incorporated into subsequent implementation. The sixth stage is continuous improvement. Agencies should regularly assess whether digital auditing has expanded transaction coverage, shortened reporting time, improved evidence quality and strengthened follow-up. They should also monitor recurring findings, data-

quality problems, security incidents, user competency and system performance. Governance arrangements should be reviewed as technologies, risks and regulatory requirements evolve. Digital audit capability should therefore be treated as a continuing organisational capacity rather than as a completed technology project.

The framework also recognises that government agencies operate at different levels of digital maturity. The maturity-sensitive progression allows agencies to move in a common strategic direction without requiring identical systems or implementation timelines. At the early stage, agencies may begin with centralised electronic records, standardised audit templates and basic follow-up databases. At the intermediate stage, they may introduce integrated audit management systems, dashboards and routine data analytics. At the advanced stage, agencies may progress towards continuous auditing, predictive analysis and carefully governed artificial intelligence. Overall, the framework emphasises that effective digital assurance results from the coordinated development of technology, governance and professional capability. Management commitment and organisational collaboration enable these dimensions, while the implementation pathway provides a structured process for operationalising them. The maturity-sensitive progression further allows agencies to advance according to their existing capabilities, risks and institutional circumstances.

CONCLUSIONS AND IMPLICATIONS

This qualitative study shows that digital audit transformation in the public sector depends on more than the acquisition of software. Interview and documentary evidence indicate that system integration, data accessibility, governance, competency and management support collectively shape digital audit capability. Malaysian public-sector audit institutions are progressively moving towards audit management systems, electronic evidence and dashboard-based monitoring. This integrated audit environment illustrates how planning, findings, auditee feedback and follow-up can be connected through a common platform (IIA, 2024; OECD, 2024). However, uneven maturity and fragmented systems continue to affect implementation across agencies.

The study contributes by developing a qualitative framework that integrates technology readiness, digital governance and auditor competency. The framework is grounded in internal auditors' experience and institutional documents rather than being derived solely from abstract technological concepts (Almaqtari, 2024; IIA, 2026a). It positions management support and organisational collaboration as enabling conditions that connect the three dimensions. This provides a more comprehensive interpretation of public-sector digital audit transformation. It also emphasises that professional responsibility remains central even where procedures are increasingly automated. Theoretically, the study extends the application of institutional theory to digital audit transformation in a developing-economy public sector, showing that capability emerges through the alignment of regulative, normative and cultural-cognitive conditions rather than through technology acquisition alone (DiMaggio & Powell, 1983; Scott, 2014).

The findings have practical implications for Malaysian government internal audit departments. Agencies should assess their existing capability before acquiring new applications and should establish data-governance arrangements before expanding analytics (IIA, 2026a, 2026b). Audit management systems should connect the full audit cycle rather than merely store electronic forms. Training should address data interpretation, cybersecurity, professional judgement and communication. Central institutions may support smaller agencies through common standards, shared platforms and coordinated competency programmes.

The findings also have implications for policy and management. Digital audit performance should not be evaluated only through the number of systems introduced or officers trained. More meaningful indicators include transaction coverage, reporting timeliness, evidence quality, issue-resolution rates and reduction in recurring findings (OECD, 2025). Management should also assess whether digital audit outputs contribute to better decisions and stronger internal control (IIA, 2026a). Such measures connect technological implementation with institutional accountability.

The study is limited by the small purposive interview sample and its focus on selected Malaysian public-sector institutions. The interviews provide informed internal auditors' perspectives but do not represent every ministry, statutory body, state administration or local authority. The reviewed documents also reflect particular institutional settings and stages of digital development. Future studies may expand the sample across different levels of government and include case studies of individual audit management systems. Longitudinal research may examine how capability changes before and after implementation.

Digital auditing should ultimately be evaluated through its contribution to public accountability and the protection of public resources. The objective is not merely to complete audits faster or introduce more sophisticated applications. The objective is to improve risk identification, strengthen evidence, accelerate corrective action and provide more useful

assurance. These outcomes require technology to be supported by governance, competency and professional responsibility. Digital audit transformation must therefore remain centred on public value.

Future research should empirically validate the proposed Digital Audit Capability Framework across a wider range of government agencies and administrative contexts using mixed methods, including surveys and case studies. Incorporating the perspectives of operational auditors, information technology specialists and senior management would provide more comprehensive evidence of its effectiveness and practical applicability, thereby further strengthening the novelty and contribution of this research.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the support of the Accounting Research Institute, Universiti Teknologi MARA, a Higher Institution Centre of Excellence (ARI-HICoE), and the Ministry of Higher Education Malaysia (KPT) for supporting the research and scholarly activities underpinning this article.

REFERENCES

1. Agostino, D., Saliterer, I., & Steccolini, I. (2022). Digitalization, accounting and accountability: A literature review and reflections on future research in public services. Financial Accountability & Management, 38(2), 152–176. https://doi.org/10.1111/faam.12301
2. Alles, M. G. (2015). Drivers of the use and facilitators and obstacles of the evolution of Big Data by the audit profession. Accounting Horizons, 29(2), 439–449. https://doi.org/10.2308/acch-51067
3. Alles, M. G., Brennan, G., Kogan, A., & Vasarhelyi, M. A. (2006). Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. International Journal of Accounting Information Systems, 7(2), 137–161. https://doi.org/10.1016/j.accinf.2005.10.004
4. Almaqtari, F. A. (2024). The role of IT governance in the integration of AI in accounting and auditing operations. Economies, 12(8), 199. https://doi.org/10.3390/economies12080199
5. Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big Data and analytics in the modern audit engagement: Research needs. Auditing: A Journal of Practice & Theory, 36(4), 1–27. https://doi.org/10.2308/ajpt-51684
6. Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27–40. https://doi.org/10.3316/QRJ0902027
7. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
8. Braun, V., & Clarke, V. (2021). One size fits all? What counts as quality practice in (reflexive) thematic analysis? Qualitative Research in Psychology, 18(3), 328–352. https://doi.org/10.1080/14780887.2020.1769238
9. Braun, V., & Clarke, V. (2022). Thematic analysis: A practical guide. SAGE.
10. Cao, M., Chychyla, R., & Stewart, T. (2015). Big Data analytics in financial statement audits. Accounting Horizons, 29(2), 423–429. https://doi.org/10.2308/acch-51068
11. Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE Publications.
12. DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160. https://doi.org/10.2307/2095101
13. Earley, C. E. (2015). Data analytics in auditing: Opportunities and challenges. Business Horizons, 58(5), 493–500. https://doi.org/10.1016/j.bushor.2015.05.002
14. Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. PloS One, 15(5), e0232076. https://doi.org/10.1371/journal.pone.0232076
15. Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. Social Science & Medicine, 292, 114523. https://doi.org/10.1016/j.socscimed.2021.114523
16. Institute of Internal Auditors. (2024). Global Internal Audit Standards. https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/
17. Institute of Internal Auditors. (2026a). Understanding data analytics for internal auditors. Global Practice Guide.
18. Institute of Internal Auditors. (2026b). Data analytics skills for internal auditors. Global Practice Guide.
19. Institute of Internal Auditors. (2026c). Auditing privacy and data protection risks. Global Practice Guide.
20. International Organization of Supreme Audit Institutions. (2019). ISSAI 100: Fundamental principles of public-sector auditing. INTOSAI.
21. Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation. Journal of Emerging Technologies in Accounting, 13(2), 1–20. https://doi.org/10.2308/jeta-10511

22. Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. Journal of Emerging Technologies in Accounting, 14(1), 115–122. https://doi.org/10.2308/jeta-51730
23. Kokina, J., Blanchette, S., Davenport, T. H., & Pachamanova, D. (2025). Challenges and opportunities for artificial intelligence in auditing: Evidence from the field. International Journal of Accounting Information Systems, 56, 100734. https://doi.org/10.1016/j.accinf.2025.100734
24. Knudsen, D.-R. (2020). Elusive boundaries, power relations, and knowledge production: A systematic review of the literature on digitalization in accounting. International Journal of Accounting Information Systems, 36, 100441. https://doi.org/10.1016/j.accinf.2019.100441
25. Leocádio, D., Malheiro, L., & Reis, J. (2024). Artificial intelligence in auditing: A conceptual framework for auditing practices. Administrative Sciences, 14(10), 238. https://doi.org/10.3390/admsci14100238
26. Lewis, A. C., Neiberline, C., & Steinhoff, J. C. (2014). Digital auditing: Modernizing the government financial statement audit approach. *Journal of Government Financial Management*, *63*(1).
27. Li, Y., & Goel, S. (2025). Artificial intelligence auditability and auditor readiness for auditing artificial intelligence systems. International Journal of Accounting Information Systems, 56, 100739. https://doi.org/10.1016/j.accinf.2025.100739
28. Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. SAGE Publications.
29. Manita, R., Elommal, N., Baudier, P., & Hikkerova, L. (2020). The digital transformation of external audit and its impact on corporate governance. Technological Forecasting and Social Change, 150, 119751. https://doi.org/10.1016/j.techfore.2019.119751
30. Moffitt, K. C., Rozario, A. M., & Vasarhelyi, M. A. (2018). Robotic process automation for auditing. Journal of Emerging Technologies in Accounting, 15(1), 1–10. https://doi.org/10.2308/jeta-10589
31. Mokhtar, N., Ismail, S., & Ahmad, H. (2024). Benefits and challenges of digital audit implementation in the Malaysian public sector: Evidence from the Accountant General's Department of Malaysia. IPN Journal of Research and Practice in Public Sector Accounting and Management, 14(1), 1–23. https://doi.org/10.58458/ipnj.v.14.01.01.0099
32. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
33. Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. International Journal of Qualitative Methods, 16(1), 1–13. https://doi.org/10.1177/1609406917733847
34. Organisation for Economic Co-operation and Development. (2019). The path to becoming a data-driven public sector. OECD Publishing. https://doi.org/10.1787/059814a7-en
35. Organisation for Economic Co-operation and Development. (2020). The OECD Digital Government Policy Framework: Six dimensions of a digital government. OECD Publishing. https://doi.org/10.1787/f64fed2a-en
36. Organisation for Economic Co-operation and Development. (2024). 2023 OECD Digital Government Index: Results and key findings (OECD Public Governance Policy Papers No. 44). OECD Publishing. https://doi.org/10.1787/1a89ed5e-en
37. Organisation for Economic Co-operation and Development. (2025). Government at a glance 2025. OECD Publishing. https://doi.org/10.1787/0efd0bcd-en
38. Patton, M. Q. (2015). Qualitative research & evaluation methods: Integrating theory and practice (4th ed.). SAGE Publications.
39. Rezaee, Z., Sharbatoghlie, A., Elam, R., & McMickle, P. L. (2002). Continuous auditing: Building automated auditing capability. Auditing: A Journal of Practice & Theory, 21(1), 147–163. https://doi.org/10.2308/aud.2002.21.1.147
40. Richins, G., Stapleton, A., Stratopoulos, T. C., & Wong, C. (2017). Big Data analytics: Opportunity or threat for the accounting profession? Journal of Information Systems, 31(3), 63–79. https://doi.org/10.2308/isys-51805
41. Salijeni, G., Samsonova-Taddei, A., & Turley, S. (2019). Big Data and changes in audit technology: Contemplating a research agenda. Accounting and Business Research, 49(1), 95–119. https://doi.org/10.1080/00014788.2018.1459458
42. Scott, W. R. (2014). Institutions and organizations: Ideas, interests, and identities (4th ed.). SAGE Publications.
43. Shafie, N. A., Sanusi, Z. M., Sanusi, S., Isa, Y. M., & Razak, N. A. (2023). Challenges of evolving digital auditing landscape among Malaysian government accountants and auditors. In J. Said, D. Daud, N. Erum, N. B. Zakaria, S. Zolkaflil, & N. Yahya (Eds.), European Proceedings of Social and Behavioural Sciences (Vol. 131, pp. 670–682). European Publisher. https://doi.org/10.15405/epsbs.2023.11.57
44. Vasarhelyi, M. A., Alles, M. G., Kuenkaikaew, S., & Littley, J. (2012). The acceptance and adoption of continuous auditing by internal auditors: A micro analysis. International Journal of Accounting Information Systems, 13(3), 267–281. https://doi.org/10.1016/j.accinf.2012.06.011

45. Veerankutty, F., Ramayah, T., & Ali, N. A. (2018). Information technology governance on audit technology performance among Malaysian public sector auditors. Social Sciences, 7(8), 124. https://doi.org/10.3390/socsci7080124