ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb554

An IT Audit Framework for Quality, Security, and Compliance in Integrated Biomedical Imaging Systems: A Case Study in a Saudi Arabian Clinical Environment

Hazel Galas Lampitoc[1]; Dr. Reagan Recafort[2]

[1]AMA University, Quezon City, Philippines
[2]Doctor of Information Technology, Dean, Graduation School, AMA University, Quezon City, Philippines

Publication Date: 2026/02/21

Abstract: Biomedical imaging systems have proven to be relevant for current clinical practice; on the other hand, increasing complexity has resulted in substantial challenges in system quality, cybersecurity, and regulatory compliance. This study examines these challenges in a Saudi Arabian clinical context, in addition to presenting an IT audit framework for integrated imaging systems. The study, underpinning its methodological approach, using General Systems Theory (GST), used a qualitative case study design with semi-structured interviews, document reviews, and non-intrusive observations. Thematic analysis yielded four major issues identified: challenges to the quality/performance of the system, security risks and vulnerabilities involved, compliance deficiencies and inconsistencies between different components, and the interdependency between imaging subsystems. Here we highlight a few limitations of traditional IT audit methodologies, which are still unable to cope with imaging-specific operational and technical realities. Consistent with this demand, the IT audit framework proposed by this study refers to those four core dimensions: quality assessment, security evaluation, compliance verification, and subsystem interdependency. It provides healthcare providers with a structured and practical method for enhancing the reliability, cybersecurity preparedness, and the alignment of the imaging system with the requirements set by the national and international standards. By focusing on the governance of biomedical imaging systems, it provides a significant advance in Saudi Arabia's digital ecosystem transformation based on evidence.

Keywords: *Biomedical Imaging Systems; PACS; RIS; HIS; IT Audit Framework; Cybersecurity; System Quality; Regulatory Compliance; General Systems Theory; Saudi Arabia; Digital Health; Interoperability; Imaging Informatics.*

How to Cite: Hazel Galas Lampitoc; Dr. Reagan Recafort (2026) An IT Audit Framework for Quality, Security, and Compliance in Integrated Biomedical Imaging Systems: A Case Study in a Saudi Arabian Clinical Environment. *International Journal of Innovative Science and Research Technology*, 11(2), 1202-1214. https://doi.org/10.38124/ijisrt/26feb554

I. INTRODUCTION

➢ *Background of the Study*

Biomedical imaging is now an essential part of modern medicine. Instead of single machines capable of manually generating images and interpreting them, technologies like X-ray, CT, MRI, and ultrasound work in highly connected virtual landscapes. Picture Archiving and Communication Systems (PACS) as well as Radiology Information Systems (RIS), Electronic Health Records (EHR) systems, and advanced digitalisation diagnostic instruments are collaborating to offer clinical guidance to aid in diagnostics, avoid delays and improve clinical outcomes. Such a move toward a unified imaging ecosystem has also rendered radiology data-hungry and technology-dependent. At present, digital transformation is underway in Saudi Arabia with healthcare modernization one of the national goals of Vision 2030. The Ministry of Health (MOH), Saudi Health Council, Saudi Data and AI Authority (SDAIA), etc. are driving strong initiatives to harmonize health information infrastructures to underpin cybersecurity and promote interoperability between hospitals. Therefore, many health facilities in the Kingdom are implementing advanced imaging software, cloud storage, AI diagnostics for high-quality service delivery and operational efficiency. However, the advantages of integration are easily negated by significant challenges. Biomedical imaging has to handle sensitive patient data and are therefore

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb554

susceptible to cybercrimes. These vulnerabilities introduced by the former PACS server, lack of authentication mechanism, insecure network environment, and the absence of encryption may lead to the hospitals becoming exposed to information breach, the failure of systems, and patient safety being compromised. AI tools start being deployed as well (which is even more challenging) (data governance, algorithm reliability, regulatory compliance and so forth). These realities highlight the need for solid IT audit systems to evaluate integrated imaging systems for compliance needs, security, and standards. Even with traditional audit frameworks such as COBIT, ISO/IEC 27001 or the NIST Cybersecurity Framework being valuable, these frameworks do not take into account the inherent technical and clinical subtleties of the environment of imaging. Imaging regimes must be DICOM in combination with modality-specific flows and clinical safety requirements, real-time conditions on imaging. Consequently, the audit framework is required to be a specific guideline, so that the imaging systems are to work in a secure, reliable and responsible manner locally and internationally.

➢ *Problem Statement*

Biomedical imaging systems are vital in the clinical environment; however, there is currently no IT audit framework emphasizing quality, security, and compliance of integrated imaging environments. Current audit models provide broad direction but fail to meet imaging-specific requirements such as modality flows, interoperability frameworks, real-time performance, and clinical safety concerns. This gap is significant in the case of Saudi Arabia, which has advanced faster than its national counterparts in digital transformation with added complexity, particularly around systems and cybersecurity. Healthcare providers are bound by national requirements including SeHEP and NCA guidance, but little formalized audit tool is available that focuses on imaging systems. In absence of structured audit systems, hospital services may fail to identify threats, support system safety, regulatory compliance, and compromises may occur that compromise the safety and integrity of the patient and data.

➢ *Purpose of the Study*

The purpose of the study is to develop an IT Audit Framework pertaining to Quality, Security and Compliance of the integrated biomedical imaging system used in a Saudi Arabian clinical study. Applying a qualitative case study methodology, this paper reviews operational, security and imaging system issues, examines state-of-the-art imaging systems that exist and synthesizes observations about international audit standards and national legislation to actual clinical practice. This new approach will support the healthcare leadership team, IT auditors, and clinical administrators on diagnosing and monitoring imaging systems performance to ensure regulatory compliance.

- *Research Objectives*

Our study is focused on the following objectives:

✓ Evaluate the quality of integrated biomedical imaging systems across a Saudi Arabian clinical hospital.
✓ Pinpoint challenges with Quality, Security and Compliance in Imaging System Integration.
✓ Estimate what IT audit practices exist and see if its applicability to biomedical imaging is feasible through assessment of systems or applications.
✓ To provide an integrated IT audit framework for integrated imaging facilities.
✓ To recommend how to improve audit readiness, system reliability and regulatory compliance.

➢ *Significance of the Study*

The academic contributions and practical implication of this study to the healthcare operations are the result of its contributions. In terms of research aspect, this research contributes to light literature on an insufficient number of studies on IT auditing in dedicated clinical systems, in specific imaging systems lack of the research in governance, security and compliance related. At real-time level, this systematic audit framework is intended to help health care facilities to enhance a system's quality and cybersecurity in addition to adhering to national legislation (e.g. SeHEP and NCA regulations). The findings complement the wider objectives of Saudi Arabia in designing its Vision 2030: building an efficient and digitally empowered and effective healthcare system.

➢ *Scope and Delimitations*

This study focuses on integrated biomedical imaging systems (i.e., PACS, RIS and associated imaging systems) from one single Saudi Arabian clinical environment. The study takes into account aspects such as quality and security of the system, compliance techniques taken over and the level of service rendered. Although it's an absence, this approach does not include financial audits or clinical results reviews. Assessment of non-imaging systems is not covered by current reports such as the laboratory or pharmacy systems. Penetration tests were not conducted for ethical and operational reasons.

➢ *Definition of Key Terms*

Biomedical Imaging Systems: Software that collects, stores and transmits medical images on digital media. PACS: Picture Archiving and Communication System for image storage and retrieval. RIS: A Radiology Information System that manages your radiology workflow. IT Audit Framework: An established set of standards for judging quality, security and compliance of systems. The worldwide IS control standard is ISO 27001. IT regulation and control; COBIT 2019. SeHEP: The Saudi Health Information Exchange Policy on Data Protection and sharing.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb554

➢ *Conceptual Framework Diagram*

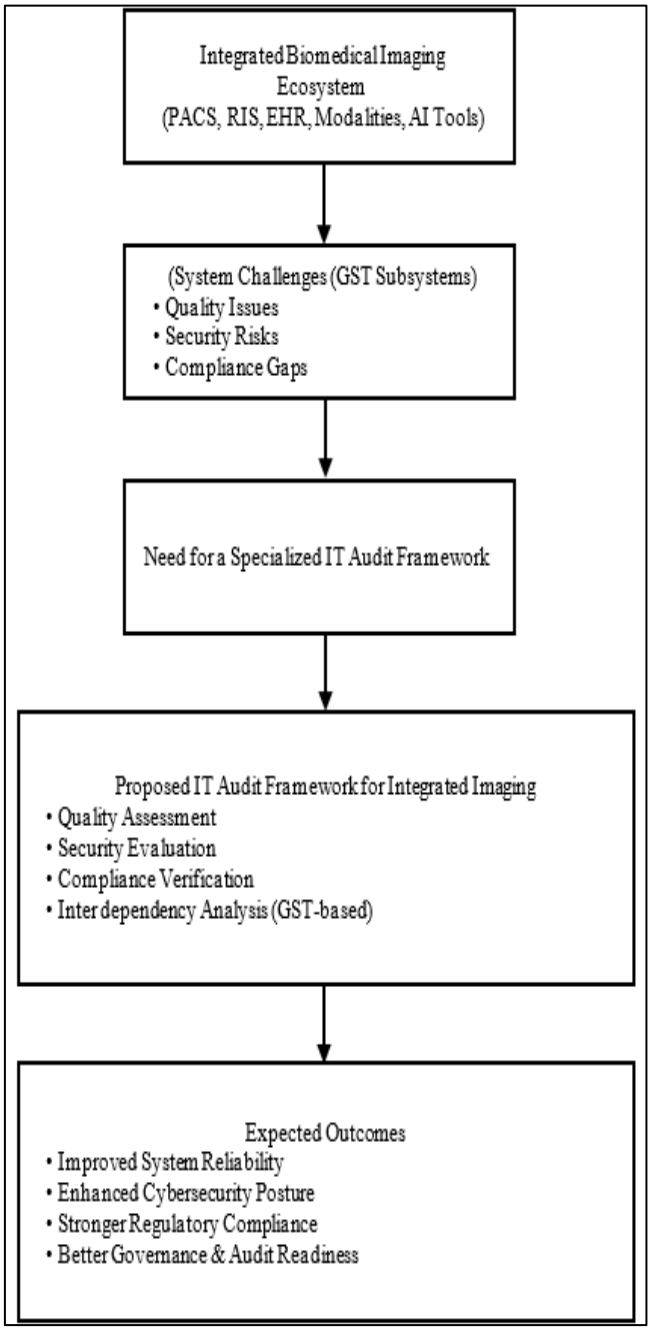

Fig 1 Conceptual Framework Diagram

II. NARRATIVE EXPLANATION

Based on General Systems Theory (GST), the conceptual model that is proposed views integrated biomedical imaging systems as a network of interconnected subsystems whose interdependencies mutually impact the reliability, security, and compliance of the system. Quality assurance, cybersecurity requirements, and regulatory compliance present challenges for the imaging ecosystem, which is comprised of PACS, RIS, EHRs, different imaging modalities, and AI technology. The challenges raised show the limitations of general IT audit frameworks and the need for an imaging environment-specific framework. The proposed IT Audit Framework evaluates imaging systems on four levels: quality assessment, security evaluation, compliance verification, and interdependency analysis. The framework hopes to improve system reliability, strengthen cybersecurity capabilities, and enable more robust compliance to relevant regulations throughout Saudi Arabia's burgeoning digital health community by delivering a comprehensive approach to these domains. As hospitals move beyond independent imaging systems to connected, online entities, there is an urgent need for governance, quality assurance, cybersecurity, and regulations to be implemented. The literature review in this chapter covers the literature of integrated biomedical imaging systems, IT auditing systems, quality assurance (QA) requirements, cybersecurity vulnerabilities, and compliance. The objectives of the study are to make an integrated biomedical imaging environment in healthcare. For Saudi Arabia, the digital health context becomes even more significant, which has been explored; as the conceptual basis is laid down through GST, it is used to give an insight into the interactions among imaging subsystems. The chapter ends with a summary of the research gap that this study addresses.

➢ *Integrated Biomedical Imaging Systems*

Integrated biomedical imaging systems integrate different technologies (PACS, RIS, EHRs, varied imaging modalities, and AI-guided diagnostic tools) to streamline clinical workflows. Such systems are reliant on interoperability standards, such as DICOM for image-to-image communication and HL7 for clinical data sharing. Working at its best, this integration improves diagnostic accuracy, reduces delays, and enables collaboration between healthcare workers. But that integration also brings with it operational and technical challenges: the best imaging workflows depend on network capability, storage availability, and system configurations. Moderate disruptions—slow image retrieval or inconsistent communication between the modalities—can lead to suboptimal clinical decision-making. Integrated imaging environments require continuous tracking with organized governance and a detailed audit process to ensure quality and patient safety, they claim.

➢ *IT Auditing in Healthcare*

IT auditing plays a very fundamental role in securing the security of healthcare services, maintaining compliance with efficiency standards and regulations. Frameworks such as COBIT, ISO/IEC 27001, NIST recommendations as well as ITIL also provide systematic guidelines for the assessment of governance structures as well as risk management processes and security controls. However, it has been noted, by the literature that there is a longstanding weakness: the generic IT audit frameworks frequently are unwilling to comprehensively account for the unique characteristics of biomedical imaging systems. Imaging contexts represent a set of specialized data formats, modality-

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb554

dependent, real-time performance-oriented and highly-risky clinical workload workflows. An example of how PAC performance directly impacts radiology turnaround times is that missed DICOM communications can cause diagnostic work-in-progress in a patient care system to be interrupted. Given the unique nature of integrative imaging settings, however, there exists an urgent need for clinical audit frameworks within domains—primarily imaging systems—firm by the nature of integrated imaging scenarios and the need for specialized audits.

➢ *Imaging Systems Quality Assurance*

Quality assurance (QA) establishes the precision of imaging systems and their clinical reliability. Traditional QA initiatives emphasise calibration of the devices in combination with image quality assessments and the regular maintenance tasks; however, in systems that are built with hardware integrated in the simulation, this scope is more than limited to the individual devices.

Numerous other QA considerations are cited in the literature:

- Capacity/performance of the network.
- Data transmission integrity
- PACS/RIS/EHR systems are interoperable.
- Access control over user and workflow.
- Handling of software patches and updates

Poor quality assurance (QA) practices can cause diagnostic imperfections and also bottlenecks in workflow that increase risks regarding patient safety outcomes, therefore it is emphasized by many researchers that the QA aspect must be included in IT audit processes so as to provide a complete analysis of all image system performance.

➢ *Imaging Environment Cybersecurity Threats*

Biomedical imaging systems, being sensitive and playing significant roles in clinical operations, are high-value targets for cyberattacks, and researchers found multiple vulnerabilities, including:

- Outdated PACS servers.
- Legacy operating platforms
- Weak or shared authentication methods
- Unencrypted data transfer
- Misconfigurations in network segments

Cybersecurity incidents impacting these systems can lead not only unauthorized access, but ransomware attacks with extended downtimes and compromising patient safety standards--the literature points out continuous security audits alongside vulnerability assessments plus adherence to established cybersecurity standards as key measures against threats that are only growing. These findings highlight the importance of an audit framework in which cybersecurity evaluations form the core competencies.

➢ *Compliance and Compliance Requirements in Healthcare IT*

Healthcare organizations must balance these aspects of protecting their data standards with a series of national and international regulations, in addition to maintaining the quality standards for clinical quality. Mainly from literature, this includes:

- HIPAA (an international standard regarding protection of health data).
- ISO 27799 (health information security guideline).
- Joint Commission International (JCI) benchmarks.
- NCA directives in respect of Saudi Arabia.
- The Saudi Health Information Exchange Policy (SeHEP).

By compliant these imaging infrastructures uphold patient privacy whilst being in line with data integrity; this contributes to seamless security in clinical practice; non-compliance can result in legal action impacting brand, and operational disruption thus placing structured auditing mechanisms critical to verify that regulatory expectations are fulfilled.

➢ *Integrated Imaging Systems in Saudi Arabia*

The rapid growth in the health industry in Saudi Arabia (which is being fast tracked by Vision 2030 and digital health programmes at national level to modernise), with a growing interest in cloud-based services combined with AI-enabled image processing tools to manage medical records, is supplemented by harmonized health information systems (including NPHIES), in pursuit of homogeneity of data exchange among health-care firms, and SDAIA is a commitment within clinical practice to responsible use of AI. However, with a lot of progress made to date there remain some noticeable challenges that are also evident, such as:

- Differences between hospitals on digital maturity levels
- Partial interoperability between older systems and new ones
- Readiness to risk mitigation against cyberattacks
- Inconsistent application prevailing surrounding IT audit methodologies
- Lack of qualified auditors with specialisation in images.

These challenges underscore the urgent need for tailored audit frameworks that represent Kingdom's regulatory environment and technological progress informed by operational realities in its healthcare ecosystem.

➢ *Background Theory: General Systems Theory (GST)*

Integrated imaging environments can be thought of in terms of General Systems Theory (GST). The General Systems Theory (GST) considers systems as interconnected, with total effectiveness being

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb554

determined by their interactions. This approach is in line with the imaging ecosystem design, which considers PACS, RIS, EHRs, networks, and cybersecurity controls as interdependent subsystems. GST also emphasizes that no subsystem exists in a vacuum. So auditing one subsystem like security would have an effect on the whole imaging environment. A system security audit reveals security weaknesses such as weak authentication, aging PACS servers, and unencrypted data transmission, which should be fixed to enhance the complete security of the entire system. Improved security reduces the likelihood of cyber-attacks, resulting in less image loss, workflow chaos, and loss of patient data. On the negative side, if security vulnerabilities go unresolved, the process can be compromised, which may slow down the delivery of the imaging protocol, degrade the accuracy of the data, and may lead to a failure in diagnosis. GST refers to this as a "ripple effect" and says a subsystem doesn't work, causing a ripple effect throughout the system. Thus, this theoretical foundation leads to an audit system that ensures to evaluate the imaging systems comprehensively and not based towards a technical analysis in a vacuum.

➢ *Research Gap*

Despite the literature providing a vast potential in integrating imaging system integration, IT auditing, cybersecurity and compliance across different research areas, there is an overall lack of audit frameworks that are tailored to integrated biomedical imaging systems. Even fewer recent studies in the recent scope are still based on the Saudi Arabian environment where dynamic digital changes have created both a risk limitation and an opportunity to develop. This gap suggests the criticality of an IT audit framework that is thorough with a practical component on systems quality, security controls, compliance with regulatory requirements, compliance standards, interoperability and operability which can be put into practice within a systematic context. This study has set out to create an audit framework for integrated imaging environment systems of patient care in healthcare systems in Saudi Arabia.

➢ *Synthesis*

The chapter provides a literature review that covers the rising intensity of integrated biomedical imaging systems and their growing demand for governance, quality assurance, cybersecurity or regulation compliance structures. As healthcare organizations transition from fragmented imaging systems to integrated digital ecosystems, PACS, RIS, EHRs, imaging modalities, and AI-driven tools operate as an integrated component of a clinical ecosystem. This interconnectivity improves diagnostic efficiency but presents new vulnerabilities and operational problems that require systematic monitoring. Current IT audit tools and techniques, including COBIT, ISO/IEC 27001, NIST, and ITIL, are useful in general information systems but have the most common shortcomings in imaging settings according to the literature. Therefore, digital information system tools in imaging settings can be used well for non-intraspecific information systems (e.g., EHRs, MRI, and CTAs). Biomedical imaging relies heavily on proprietary data formats, protocols tied to specific modalities, issues facing real-time performance, and high levels of clinical safety. Such special elements need an audit approach, which shouldn't simply use a traditional IT control approach but needs to be customized to the specific technical and patient context of the imaging process. Considered among the main points, in addition to analysis of image quality and equipment performance, it is the reliability of networking, integrity of data transmission, interoperable process and workflow productivity. Cyber risk information is also good and often pointed, with imaging equipment being a target of cyber attacks because it is a highly sensitive resource that delivers high-quality care to patients. Compliance with national and local and international legislation (e.g. HIPAA, ISO 27799, JCI, NCA, and SeHEP guidelines) is essential to ensure both patient safety and the safe operation of the system. In the Saudi context, the literature shows an accelerated penetration of digital transformation as envisaged by Vision 2030 and national health agendas. While these technology advancements have accelerated use of modern imaging solutions, they have identified shortcomings with interoperability, cybersecurity preparedness and special IT auditing capabilities. It emphasizes the need for a national audit framework which is in line with the Kingdom regulatory framework and the technology sector. These difficulties can be explained through the General Systems Theory (GST) which is a solid theory. GST demonstrates that imaging systems act as interconnected subsystems and that vulnerabilities in any unit, such as security, could spread throughout the system. It adds to the value of an audit system that factors in quality, security, compliance, relationships and so on and works with rather than in isolation of other parts of the process. The literature is generally very sparse: there is no such IT audit framework specifically in the integrated biomedical imaging system domain, especially in the case of the Saudi Arabia health sector. The lack of data in this area so far justifies the study in formulating a dedicated audit framework to aid in meeting operation, technical and regulatory needs of imaging ecosystems in this sector.

III. METHODOLOGY

➢ *Research Design*

This study used qualitative case study methodology to understand the quality, security, and compliance features of integrated biomedical imaging systems in a clinical environment in Saudi Arabia. Since quantitative data frequently fails to capture the richness of human experience and insights related to common workflows, the qualitative method has been chosen for this study as it is said to provide a holistic and detail-oriented understanding. This research primarily focuses on the construction of an IT audit framework, thus, the

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb554

need for obtaining the detailed insights of those directly involved with imaging systems is imperative. The case study approach is most appropriate because it looks at a single institution as an example of the imaging ecosystem at the institution level, including processes, policies, system and human aspects. And since this method closely follows General Systems Theory (GST), which emphasizes the relationships among subsystems in a wider context, it is particularly well-suited to investigating large imaging infrastructures.

➢ *Research Setting*

The study was conducted within a healthcare facility in Saudi Arabia that boasts a fully integrated biomedical imaging ecosystem. This context encompasses PACS, RIS, multiple imaging modalities such as CT, MRI and ultrasound, and EHRs associated through centralized infrastructure. The hospital is part of a national digital health cluster that also adheres to statutory requirements and regulations as defined by the Ministry of Health (MOH), the Saudi Health Council and National Cybersecurity Authority (NCA). This environment was selected since it shows real challenges encountered by healthcare organisations during digitalization, in the form of interoperability issues, cyber risks on a system and compliance requirements. An exploration of this context can therefore shed light on the operational requirements of a framework for audit.

➢ *The Participants and the Sampling*

The participants in this study were professionals working in the operation, management, or oversight of biomedical imaging systems. These professions were PACS administrators, IT security staff, technologists, radiologists, compliance officers, and health information management workers. Their functions also provide insight into system quality, security, and compliance related processes. Conviction was reached by purposively sampling the participants who had specialist knowledge and experience of the topic of this study. This approach provides for a meaningful and personally relevant data set; participants were invited at data saturation—interviews extended until there were no new ideas.

➢ *Data Collection Methods*

The data collection was achieved through three principal qualitative approaches, including semi-structured interviews, document examination, and unobtrusive observations. Semi-structured interviews allowed participants to express their experiences, while granting researchers the flexibility to delve into the 'emerging themes' and investigate new emerging issues—ideal for sensitive issues, such as systems vulnerabilities or workflow bottlenecks. Document review involved reviewing relevant documentation i.e. imaging practices, audit records, workflow diagrams and process diagrams, security practices, and compliance reports and documents were examined, providing information and information for interpretation, which provided background context to findings from interviews. Using non-intrusive observation to develop an understanding of how imaging systems function in practice, such as how staff accessed PACS, RIS platforms, and modalities, revealed workflow bottlenecks or system dependencies that were not clearly articulated by participants.

➢ *Data Collection Instruments*

The principal tools used in this study included an interview guide, a document review checklist, and an observation notes template. I used an interview guide with open-ended questions to capture participants' experiences with terms of system quality assurance practices and security controls and compliance measures that were embedded in their workflows. Using the document review checklist, for each of the materials reviewed, it provided a structured approach to ensuring policies, system logs, standards etc. and relevant workflow documentation were thoroughly examined to ensure that they were in-line with study objectives. The observation notes template allowed for patterns of recording during site visits about what type of workflows or potential issues employees encountered using these systems.

Table 1 Summary of Data Collection Instruments

Instrument	Purpose	Purpose
Interview Guide	Explore experiences and insights	Explore experiences and insights
Document Review Checklist	Validate and supplement interview data	Validate and supplement interview data
Observation Notes Template	Capture real-world system interactions	Capture real-world system interactions

➢ *Data Analysis*

For this study, thematic analysis was implemented as the main method to assess qualitative analysis—a method widely adopted to identify significant patterns in deep descriptive data. Since our current objective is to develop a theoretical IT audit framework based on grounded experiences, the thematic analysis offers both structure as well as flexibility in interpreting professional opinions in an imaging context. Analysis was performed by familiarization in which transcripts of interviews and observation notes were read several times and in conjunction with documents to ensure understanding, followed by identification of recurring thoughts or issues in participant comments. Open coding, or linking phrases from responses to a question, an experience, a concern or experience to support an overall quality assurance practice, or for a subsystem interaction, emerged from participant responses and documentation evidence gathered in prior stages—the codes were the critical insights that emerged

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb554

immediately from participant perspectives. These first codes were axially coded following—grouping similar codes into higher order categories (e.g., categorizing delayed image retrieval alongside inconsistent modality communication into "system performance challenges"). This structure revealed connections among concepts, pointing to where themes converged and where many issues crossed. Final stage was a process of Selective Coding wherein core themes which represented the overall importance of the dataset were selected and based on the basis of these themes the proposed IT audit framework is introduced consisting of "interdependency among subsystems," "legacy component vulnerabilities," "compliance documentation gaps" and "workflow disruptions stemming from systemic misalignment." Analysis with interpretative lens guided by GST highlighted the interrelation of subsystems implying weaknesses in these systems have a ripple effect throughout an ecosystem helping to interpret specific themes, including weak authentication flows affecting systems such as PACS/RIS/EHR environment which confirms the systemic nature of the issues found (local). The final themes were transformed into actionables that serve as the foundation for an IT audit framework which provides for empirical grounds of the model that are consistent with the operational complexities that characterise the studied settings and add credibility to findings as it was proven that the findings from the study were underpinned through a systematic, theory-driven method, which not only resulted in practical implications but also the contextual relevance for that.

➢ *Trustworthiness of the Study*

To ensure reliability alongside rigor whilst conducting each step in its study implementation Lincoln & Guba's four criteria was followed: credibility; transferability; dependability, as well as confirmability principles which upheld rigorously through process: This included documenting all decisions used in our study through established audit trails, being open for transparency, maintaining fidelity in evidence and ensuring our findings rest strictly on participant-derived data avoiding researcher bias affecting results presented hereon thereby strengthening trustworthiness credentials through conducting substantial scholarly processes described above while enhancing the depth validity of the validity of findings achieved through collaborative research that took place among groups different stakeholders engaged in mutual investment in working together to progress them collectively toward the same objectives through rigorous methodologies to be defined in detail already outlined for this study outlined extensively here in detail and explicitly structured articulately recording essence behind foundational goals pursued painstakingly in all inquiry completed diligently following the steps taken for the sake of excellence striving to reach high quality standards consistently demonstrated absolute dedication commitment dedication professionalism, which is exemplified thoroughly presented vividly described concisely described clearly articulate, presented in a clear structure logically aligned in accordance to coherently structured structure, ensuring to deliver insightful contributions helping increase overall knowledge base in understanding greatly and improving in depth and expanding the generalizability gained, helping to deepen and broaden general scholarly discussion and debate concerning intricately interlinked fields, which has been covered this study in detail at great detail in detail with great success, successfully addressing complexities encountered through the research process successfully facing challenges faced, overcoming challenge successfully and perseveringly focusing with clarity achieving goals of achieving the purpose that were established commendably completed as promised, end product realized within scope, contributing significantly to the study enriching the discipline on the global literature, enriching the literature in ways that open up new realms or fields, inspiring others to explore further, encourage future research, and facilitate collaborative conversations among those who engage and work together and promote collective advancement leading the field to progress in our understanding of subject matter to lead to great growth as well!

➢ *Ethical Considerations*

Ethical considerations were adhered to and adhered to at every stage of the research. Subjects were made aware of the study objectives, informed that their participation was voluntary and that they had the right to withdraw at any time. Consent for any interviews or observation was obtained. To protect identities and privacy no ID was collected in order to keep confidentiality of research participants. All the recorded data were kept in a secure place and were used strictly on student research. The research was conducted according to the institutional and national ethical guidelines associated with studies of human subjects, and its ethical guidelines were approved by the hospital ethics committee prior to data collection.

➢ *Research Procedures*

It began with the identification of the research problem and wide-ranging literature review of relevant literature. The data collection methodology was developed and validated based on these observations. After gaining ethical clearance, the researcher conducted interviews, examined documents, and conducted observational research. Data were transcribed and coded and analysed thematically. The findings guided the creation of an IT audit framework evaluated by experts for validation. Such systematic approach made it to be done transparently, rationally and professionally.

➢ *Limitations of the Methodology*

There were several limitations of this study. This was done in one hospital and it raises concern with terms of generalizability and findings across other healthcare facilities. Purposive sampling means that findings represent the experiences of individual

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb554

participants, not a wide spectrum of the population. Furthermore, time constraints limited the number of interviews and observations that could be conducted. Additionally, technical penetration testing was excluded from this research for both ethical and operational reasons. Nonetheless, with these challenges looming the door open to the development of a specialized audit methodology for the context of integrated biomedical imaging systems.

➢ *Data Flow Diagram of the Research Process*

This is a high-resolution diagram that uses a digital transformation pipeline format. It reflects a diagram that demonstrates a data flow of data as it traverses different phases of this study (the imaging ecosystem to the development of the audit framework in detail).

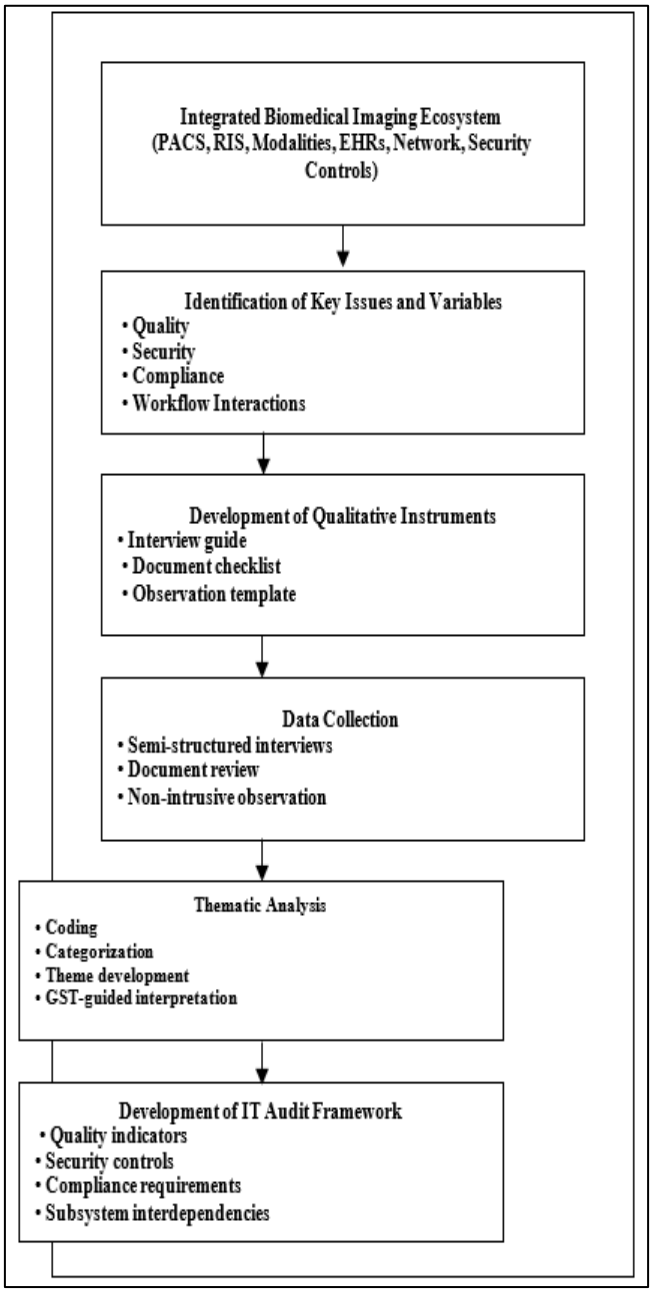

Fig 2 Narrative Explanation of the flow diagrams for the Data Flow Diagram

The chart depicts how information is conveyed throughout the duration of the investigation - how each step serves to drive the overall IT audit framework. It begins with a summary of the integrated biomedical imaging platform of the study on which the research was based (PACS (Picture Archiving Communication System), RIS (Radiology Information System), imaging modalities, EHRs (Electronic Health Records), supporting network and security infrastructure for the study). Once people understand this landscape, they will be able to make sense of it as the foundation of concerns about quality assurance, security management and of compliance, and recognize how subsystems related to one another may interact along lines of General Systems Theory (GST). Following this process the researchers identify system quality attributes, security capabilities established, compliance policies that workers follow and interactions between workflows within these systems as major problems and variables needing investigation. By early detection, focus on the critical, closely linked domains of audit needs is maintained at this stage. Next, there are qualitative instruments; they provide a tool kit for conducting interviews and document review checklists and observation templates aimed at providing thorough accounts of their findings from diverse angles—enabling understanding of the subtleties of phenomena within imaging ecosystems and aligning methodologies with overarching goals validated earlier by experts. The next steps are data collection and obtaining information drawn primarily from semi-structured interviews and document reviews and other methods and supplemented with unobtrusive observations of different methods with different perspectives: firsthand narratives from interviews provide a subjective lens while documents provide formal historical perspectives, observations allow you to capture live interactions between systems, in order to end up with triangulated datasets that will give greater credence to the findings generated thereafter. To build thematically, this involves coding—the coding acts as an exercise in thematic analysis where data is coded into categories in which recurring patterns emerge along relationships between things encountered all explored, largely informed by GST explaining how subsystems behave toward each other—as an example, highlighting possible implications where areas of compromised security can render workflows less efficient overall, regulations' compliance, finally arriving at final evaluations against overarching themes that drive us to manifest concrete aspects of compliance including quality thresholds and security controls, ensuring that frameworks truly reflect operational realities as real practitioners experience day to day and interact with vastly diverse contexts across their fieldwork activities thus strengthening sound evidence-based outputs rooted by contextual relevance presented at every level of development leading towards audit frameworks based primarily on lived experiences collected through systematic methods outlined through logical pathways taken by the team, all the results adopted to the end of achieving a shared understanding, formed within

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb554

processes and illustrated visually in complementary diagrams drawing out strong qualitative methods adopted that naturally follow holistic frameworks reflecting successful objectives accurately and effectively captured across multiple dimensions across a whole investigation carried out to something satisfactory here clearly outlined above delineated to demonstrate robust adherence across these dimensions examined clearly delineating roads walked down and yielding meaningful results organized to ensure validity required enabling effective implementations that are developed collaboratively and forward looking allowing real contributions to be made around us as yet unrealized dormant depths to be charted down the map in the future.

IV. PRESENTATION OF FINDINGS

➢ *Introduction*

This chapter presents data from this qualitative case study that investigates the quality, security, and compliance status of integrated biomedical imaging systems in an enterprise-level hospital in Saudi Arabia. These are based on semi-structured interviews and document reviews, in addition to non-intrusive observations. The researcher identified major themes through thematic analysis, which illustrate how imaging professionals navigate or may find themselves navigating the complexities of PACS, RIS, imaging modalities, EHRs and other relevant subsystems. The results of the datasets provided a glimpse into the imaging ecosystem and laid out the basis for the IT audit framework described in this paper.

➢ *Overview of Data Sources*

We used three complementary data sources to establish depth and validity for this study. Semi-structured interviews covered PACS administrators, radiology technologists, radiologists, IT security officers and compliance staff. Document reviews provided us insight into policies, audit logs, workflow diagrams and cybersecurity guidelines at the time. Non-intrusive observations were able to observe real-time system interactions and workflow behaviour. The collation of all of these sources provided a triangulated dataset as well as enhanced the general credibility.

Table 2 Summary of Data Sources

Data Source	Description	Contribution
Interviews	12 participants from imaging, IT, and compliance roles	Experiences,insights, challenges
Documents	Policies, logs, standards, workflow charts	Verification, context, evidence
Observations	Real-time imaging workflows	Practical behaviors, system interactions

➢ *Emergent Themes*

Thematic analysis revealed four key themes that describe the status quo of the imaging ecosystem:

- Quality and Performance of the System
- Exposure to Security Risk and Vulnerabilities
- Disparities in Compliance and Documentation
- Imaging Subsystems were inextricably linked within the system.

We discuss each of these themes below with narrative explanation and evidence.

➢ *Theme 1 System Performance and Quality:*

The challenge lies in system quality. Problems with the performance, reliability, and workflow efficiency of the system were all identified by participants as problematic. (Multiple radiologic technologists noted that image transmission time lags were frequent in peak hours during time pressure, especially if several modalities were transmitting large studies at the same time.) As one tech put it, on occasion, “the system just slows down, so much so that reporting gets delayed,” demonstrating the operational impact of performance problems. Observation confirmed that retrieval of images often took longer than expected for high-resolution CT and MRI studies. Documents indicated high traffic and the presence of frequent modality-to-PACS mismatches indicative of interoperability issues between older devices and newer PACS versions were found to be common. In general this theme has the importance of QA Indicators in the audit framework in system responsiveness, interoperability, uptime, workflow.

➢ *Theme 2: Security Holes and Risk Exposure*

Issues on the theme of security popped up again and again in each interview and document review. The legacy imaging devices still run on outdated operating systems. As one participant said, “some machines can’t be patched anymore because the vendor no longer supports them,” leaving those machines vulnerable for long periods. The enforcement of access controls was occasionally inconsistent, they noted. Some imaging workstations continued to be logged in for long periods of time, putting them at risk for unauthorized access. The documents reviewed did not cover all systems fully conforming with the National Cybersecurity Authority (NCA) Essential Cybersecurity Controls. These security factors highlight the need for a security assessment element that should be embedded in the audit method, such as: access management, vulnerability mitigation, network protection, and device lifecycle management.

➢ *Theme 3: Mismatches and Documentation Problems in compliance*

The extent of conformity with national and international standards differed from department to department. Some units had new policies which met the MOH and NCA requirements and others had out-of-date (have not been updated in years) and old documentation

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb554

that they were to follow. A compliance officer said "documentation is not always updated until the issue has occurred," signaling a reactive attitude and not an anticipatory one. The discrepancies between documented processes and actual practices were apparent in observations. For example, policies required audit logs to be reviewed regularly, however document review indicated that some logs remained unreviewed for several months. Such inconsistency suggests gaps in policy implementation and monitoring. This theme reflects the requirements to introduce one of the two elements of the audit, which is a compliance verification aspect, to ensure compliance with policy and to ensure consistent documentation and execution of the policies.

➢ *Theme 4: Interdependency of Imaging Subsystems*

In line with General Systems Theory, participants remarked that imaging subsystems are by their nature interrelated. For example, a temporary RIS outage delayed modality worklists, which slowed PACS ingestion and reporting workflows. "When RIS goes down, all else slows down," a radiologist said. The findings confirmed that imaging workflows are dependent on PACS, RIS, modalities and EHRs communicating synchronously for full integration. Document reviews also showed that sub-system dependencies are not consistently mapped and when we do manage it well, it can be easier to predict what changes, disrupts or fails. This argument adds weight to the necessity of an interdependency analysis capability as one part of accounting infrastructure to consider subsystem relatedness in a holistic manner.

➢ *Theme Map Diagram (Text-Based)*

(This shows a picture (diagram) of the themes developed and their interconnection in the audit framework, which is a visual representation of the emergence of themes.)

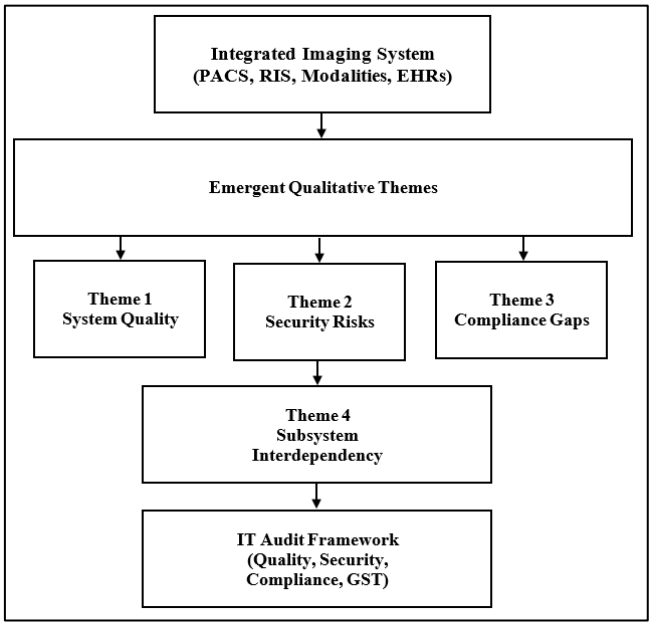

Fig 3 A Narrative Description for the Theme Map Diagram.

The theme map diagram offers a visual sense of how the primary themes emerged from the data and how they connect to the information from the broader imaging environment. At the top of the diagram is the holistic imaging system, PACS, RIS, imaging modalities, EHRs, and inter-service support systems. It is this system that forms the basis of the study as it is the ecosystem where all quality, security as well as compliance challenges occur. According to the diagram, the imaging ecosystem is an integrated and interdependent network of subsystems whose interactions contribute to the performance of the department as a whole. Out of this central system are the four major themes identified via thematic analysis and branches them out. Theme 1, System Quality and Performance Challenges, demonstrates the operational concerns over workflow efficiency, image dissemination, system response time and interoperability. The aforementioned issues were evident consistently throughout the interviews, documents and on the spot workflow. Theme 2, Security Vulnerabilities and Risk Exposure, showcases cybersecurity defects in legacy systems and subpar access control protocols as well as the failure to satisfy national cybersecurity standards. This theme emphasizes the growing need for protection of imaging systems against cyber threats. Theme 3: Compliance Gaps and Documentation Inconsistencies, which describes the discrepancy between documented policies, and current practice. It also demonstrates the uneven implementation of regulatory requirements per department. This theme highlights that compliance is more than setting policies; it is regularly applying and updating the policies. Theme 4, the Involvement of Imaging Subsystems shows that in particular each time one subsystem gets an error—like RIS is down or PACS delayed—there is a domino effect on the entire IM journey. This theme echoes General Systems Theory which describes that subsystems in a larger system may influence each other. The bottom of the diagram depicts how these four themes intersect to determine the nature of the IT audit framework presented in this study. Each theme brings an important view: quality indicators, security controls, compliance requirements, and subsystem interdependency. Collectively, they provide a basis for a holistic audit framework designed for the needs of biomedical imaging environments.

➢ *Summary of Findings*

This study indicates that, in the imaging ecosystem, system performance, security vulnerabilities, compliance inconsistency, and subsystem dependencies are among the many interconnected challenges. By and large, these themes point to the necessity for a tailored IT audit framework which addresses the distinct properties of biomedical imaging environments.

- *Introduction*

The Chapter then synthesizes the findings presented in Chapter 4 and explores their implications in terms of the study's objectives, the literature

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb554

reviewed, and the principles of General Systems Theory (GST). Thus, the chapter will conclude and give proposals as to the key steps taken for the optimization of the security, quality and regulatory aspects of integrated biomedical imaging systems in Saudi Arabia. Lastly, it provides research recommendations to enhance the imaging informatics and healthcare technology governance domain.

The purpose of this study was to examine the quality, security and compliance status of integrated biomedical imaging systems and to create a targeted technical audit framework to support imaging context. Its findings identify four principal themes—system quality issues, security weak points, compliance gaps, and subsystem relationships—that together describe the present state of the imaging system ecosystem. These topics relate to literature and GST as proposed below.

- *Quality and performance obstacles in the system*

System performance related issues like slow image transmission, nonuniform interoperability, and minor downtimes caused major workflow efficiency issues, the study found. This was in agreement with other studies highlighting that imaging systems need to be high-quality systems and high-transmission systems, which help ensure timely diagnosis and patient care. Such delays in PACS retrieval and modality-to-PACS communication, the same as reported at other healthcare providers, in which bandwidth constraints and obsolete devices prevent reliable operations, are also in place. From a GST point of view, these quality issues illustrate how an issue in a single subsystem (whether that be network bandwidth or modality support) could disrupt the quality of an entire imaging workflow. The results of the study also support continuous performance control and a proactive approach to system optimization that form an integral part of the design of future auditing framework.

- *Security Threats and the Dangers of Potential Risk Vulnerability and Exposure to Risk*

Security became a major issue, mainly because old machines often come with unsupported operating systems and less uniform access control enforcement is lacking in their control infrastructure. Such vulnerabilities make imaging systems susceptible to cyber attacks, including ransomware, which has been increasingly being exploited on an international scale against healthcare institutions that include hospital and other medical entities. The literature consistently cautions that medical imaging devices are some of the most vulnerable components of a hospital network for their long operational lifespans and limited patching capability. The results have also demonstrated a lack of compliance with NCA Essential Cybersecurity Controls, indicating imaging facilities may be better protected through improved security governance standards in place, which require special security scrutiny. GST (Cyber Security Model) is helpful in understanding how one security vulnerability, such as the unpatched modality, can damage the entire imaging system! This reminds us by implication of the importance of building the security assessment framework with strong and rigorous evaluation criteria into the audit process.

- *Compliance Gaps and Inconsistent Documentation in the Compliance Requirements*

The discrepancy in policy update process, verbatim evidence and compliance with regulation was identified through the study. Certain departments had good and transparent compliance practices, while others depended on obsolete documents or poor audit trails. In accordance with this, the study was compared to previous studies that have reported that the level of adherence to compliance in healthcare frequently varies across different departments because of differences in leadership, training, and resources. The discrepancy between the written procedures and the practice is worrisome and indicates that compliance may have not yet become institutionalized. GST also reinforces the lesson learned of the need to create a seamless integration of compliance across operations through all subsystems, and avoid siloing compliance responsibilities across areas (e.g., one department cannot comply alone in any one department), and also in different subsystems for consistency with the operations across the departments. Hence, this should logically become a stand-alone auditing compliance verification component.

The research emphasized the interrelatedness of PACS, RIS, modalities and EHRs - the imaging subsystems. Disruption in one subsystem always causes ripple effects throughout the workflow. This finding is particularly supported as argued by GST, which stresses on the importance of seeing systems as interdependent wholes rather than isolated modules. The literature further recognizes the need to map subsystem dependencies to anticipate system changes or failures impact. Results from this study bolster this need with participants often detailing how system outages via RIS, PACS delays, or modality communication issues impacted various stages of an imaging experience. This concept directly aligns with the implementation of interdependency analysis in the audit methodology.

V. CONCLUSION

This study aimed to explore the quality, security, and compliance issues on embedded biomedical imaging systems in a specific imaging setting in a Saudi healthcare establishment and to work on the provision of an IT audit framework for imaging facilities and to design the infrastructure audit framework for imaging environment. Findings also reveal significant difficulties on the performance of the system, security risks, noncompliance and inter-subsystem interdependency issues. These challenges show, in its own way, the inherent difficulties of generic IT audit models, but also demonstrate the importance of a framework that is tailor-made for imaging systems. That

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb554

is illustrated in the study, guided by General Systems Theory, the need to assess an imaging environment holistically as deficiencies in one subsystem can impact the entire ecosystem. This should have an in-depth knowledge of security and compliance landscape — the IT audit framework proposed has 4 major dimensions; quality assessment, security evaluation, compliance verification, and interdependency analysis. Overall findings and results will provide a structured foundation to analyze the impact of a new digital imaging initiative. Additionally, the research will enable digital platforms/informatics software vendors to pinpoint the most prevalent root causes of data asymmetry, enable auditing and audit the proposed auditing approach can be systematic and based on the evidence, or to test the validity of the proposed audit approach by following well established scientific principles. Overall, the study aligns with national digital health initiatives in Saudi Arabia through enhanced system trustworthiness, improved cybersecurity posture and higher regulatory compliance with the system. Recommendations The conclusions drawn from this study bring up the following recommendations.

RECOMMENDATIONS

- *Increase the availability of Performance Monitoring*

Real-time monitoring tools are necessary to monitor PACS, RIS, and modality performance by health care organizations' end users: a measure of continual monitoring tools and modality performance. Routine performance audits could be performed to avoid bottlenecks/blocking and improve system responsiveness to facilitate smooth performance of the system.

- Strengthening of Cybersecurity Measures Legacy devices can be isolated, replaced, upgraded, or separated from them as necessary. Strong access controls and regular vulnerability assessments and NCA cybersecurity regulations are essential.

- Improved Compliance Documentation Policies and procedures also need to be reviewed and updated regularly, with an eye to the policy. For compliance officials, it is the responsibility of their compliance officers to ensure that these workflows are indeed recorded as the written procedures conform to work. And audits need to ensure what workflows must be recorded as the actual practice and audit logs.

- *Map SubService Interdependencies of Sub-Services Dependence*

Institutions will develop graphical diagrams and documentation of the interaction between imaging subsystems and use imaging subsystems that illustrates the connection between different subsystems by documenting the system with graphical diagrams and documentation of the relationship between them. That'll be useful early on to understand the impact of a system change and improve incident response.

- *Implement a proposed IT audit framework*

It is also recommended that hospitals use the proposed framework for the internal audit of imaging environments, beyond the imaging images in this study to guide the process of conducting internal audits of imaging environments.

- *Conduct standardised Routine Integration audits for PACS, RIS, HIS*

Routine integration audit needs to be performed in order to proactively identify and rectify those communication gaps in PACS, RIS and HIS. These audits can be employed to ensure that the information exchange remains uninterrupted, to prevent any bottlenecked processing and to provide stable integration among imaging subsystems.

- *Frequent audits to address the communication bottlenecks*

It is recommended with regards to healthcare organizations there should be a regular auditing to identify and rectify the communication difficulties between PACS, RIS and HIS in the context of integration. These audits should be neutral to evaluate the flow of data, performance of interfaces, consistency of messages and information interoperation, with respect to every imaging environment.

Through ongoing integration checks the organization is also able to track down slow down instances, separated fields of data, lost messages, and workflow interruptions before they impact workflow significantly. Regular audits keep tracking and ensuring interface engine tuning and HL7 configurations and modality worklists align with changing clinical conditions. The overall system responsiveness will be massively improved as reporting will become much more timely as well as ensuring the overall quality of imaging ecosystem.

SUGGESTIONS FOR POLICY

- National Standards for Imaging System Audits. To enable the audit of imaging systems and compliance to MOH and NCA, regulatory authorities will examine the implementation of audited national guidelines.

- Vendors of the Cybersecurity Certification of Imaging Devices may be required to meet minimum standards of security prior to selling them to the clinic.

FUTURE RECOMMENDATIONS FOR RESEARCH

- *Multi-Site Studies*

Future studies that examine environmental imaging in other hospitals would substantiate & build on the proposed audit frame.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb554

➢ *Quantitative Verification*

This is likely to be a quantitative measurement with a quantitative study upon the implementation of the model.

AI-assisted Imaging System integration

Given the growing utilization of AI in radiology, a comprehensive research on AI tools and the safety (quality, security and compliance) should be conducted.

➢ *Final Reflection*

Here we demonstrate that integrated biomedical imaging systems are complex and interrelated ecosystems requiring dedicated oversight. It adds immense value for the governance of Saudi Arabian imaging systems under the theoretical framework grounded in real-world experience of General Systems. The proposed IT audit framework provides practical, evidence-based tools, which can help healthcare organizations reach an even higher level of reliability, security, and compliance for their digital transformation.

REFERENCES

[1]. Alahmadi, A., & Drew, S. (2020). *Cybersecurity challenges in Saudi Arabian healthcare systems:*

[2]. *A review of threats and mitigation strategies*. Journal of Health Informatics in Developing Countries, 14(2), 1–12.

[3]. Altuwaijri, M. M. (2019). *E-health in Saudi Arabia: Current trends, challenges, and recommendations*. Journal of Infection and Public Health, 12(6), 761–765.

[4]. American College of Radiology. (2021). *PACS and imaging informatics: Best practice guidelines*. ACR Press.

[5]. Arshad, J., Azad, M. A., & Khan, M. (2021). *Security vulnerabilities in medical imaging systems: A systematic review*. Computers in Biology and Medicine, 134, 104458.

[6]. COBIT 2019 Framework: Governance and management objectives. (2019). ISACA.

[7]. Health Sector Cybersecurity Framework. (2022). Saudi National Cybersecurity Authority.

[8]. ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization.

[9]. Khan, R., & Al-Sadi, A. (2020). *Digital transformation in Saudi healthcare: Opportunities and challenges*. International Journal of Medical Informatics, 141, 104241.

[10]. NIST. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). National Institute of Standards and Technology.

[11]. Saudi Health Information Exchange Policies (SeHE). (2016). Saudi Ministry of Health.

[12]. Smith, T., & Kessler, R. (2020). *IT auditing in healthcare: Ensuring data integrity and system reliability*. Health Information Management Journal, 49(3), 145–155.

[13]. Van der Putten, W., & Riley, J. (2019). *Medical imaging informatics: Principles and applications*. Springer.

[14]. Zhang, Y., & Zhao, L. (2021). *Assessing the security posture of PACS and RIS systems in modern hospitals*. Journal of Digital Imaging, 34(5), 1200–1212.