******

**UGANDA CHRISTIAN UNIVERSITY**

**FACULTY OF ENGINEERING, DESIGN AND TECHNOLOGY**

**MASTER OF INFORMATION TECHNOLOGY**

**Advanced Information Security and Audit**

**EXAMINATION**

SUBMITTED BY OGABANIRUHANGA SEPTEMBER

REGESTRATION NUMBER: S24M10/006

ACCESS NUMBER: B30918

**Part A: Auditing Principles and Types of Audits**

1. **Explanation of Three Types of Audits and Justification for Suitability**  
   ISO 19011 clause 3.1 defines an audit as a process that is designed to gather objective evidence systematically, independently and in a documented form and evaluating it objectively in order to determine the degree to which the audit criteria are met [1]. In the case of SwiftHealth Uganda dealing with sensitive data of people in the healthcare industry, it is important to choose the right types of audits to evaluate ISMS maturity as well as implement compliance with the Uganda Data Protection and Privacy Act, 2019 and revelation-specific regulations. There are three principal categories of audits that are related to the topic of this context:
2. **First-Party Audit**  
   A first-party audit also called Internal audit is an independent and objective exercise that provides the organization with a sense that the degree of control on operations is adequate, it provides recommendations on how to make the organization operations better and it adds added value. The organization performs an internal audit itself with the objective of management reviews and with the other internal requirements such as the internal auditors perform in SwiftHealth to determine the conformance of ISMS with ISO/IEC 27001:2022 and internal policies [1]. Such audits are conducted by the employees or groups of internal auditors who understand the workings of organization yet are independent of the operations being audited.

The objectives of internal audits include self-assessment, to develop readiness to external audits and measures the gaps in the implementation of ISMS. Based on ISO/IEC 27001:2022 clause 8.2, they are concerned with continuous improvement and adherence to internal controls, access control and incident response [2].

1. **Second-Party (Supplier) Audit**  
   A second-party audit or supplier audit involves auditing of third-party vendors and service providers and their security practices (ISO/IEC 27001:2022, Annex A.15). Under ISO/IEC 27001:2022 Clause 8.1, such audits can ensure that the suppliers will deal with the security requirements of the organization and they are especially crucial when a sensitive data is dealt with through external vendors (ISO/IEC 27001:2022, Annex A.15). SwiftHealth completes a second-party audit of its third-party vendors like cloud hosting companies or providers of a telemedicine platform to certify that they meet the security requirements and contract compliance [2]. Supplier audits are carried out by those parties with interest in the auditee and not originally meant to be a certification audit [1]. Such audits are usually conducted by the audit or compliance team at SwiftHealth.

The objective is to ensure vendors conform to ISO/IEC 27001:2022 control (5.19 - information security in supplier relationship) and comply with Uganda Data Protection and Privacy Act, 2019 more specifically to data protection and privacy [3].

1. **Third-Party (External/Certification) Audit**  
   The third-party audit, also called external audit involves an independent and accredited certification body in certifying that the standards of ISO/IEC 27001:2022 are met [1]. They can give the stakeholders the confidence that their ISMS is operational and properly taken care of but at that, they serve to point out areas of possible risks that the internal audits may fail to pick out (ISO/IEC 27007:2020). These audits are carried out by outside auditors who are not under SwiftHealth and this ensures there is no biasness.

The objective is to do an objective and evidence-based evaluation of the maturity of ISMS and demonstrate conformance to international standards and certification [1]. They are also credible to the stakeholders including the patients and regulators.

**Justification for Suitability**  
To assess the maturity of the ISMS of SwiftHealth Uganda, a first-party (internal) and third-party (external/certification) audits are best suited with second-party auditing playing the second position.

* **First-Party Audits**: The first-party audits are best suited when there is an implementation phase of the ISMS as SwiftHealth can review the controls within the organisation, exploit the loopholes and perform mitigating actions at minimal costs. Such internal audits can be used to determine the effectiveness of the incident response processes (5.26) to assess the ability to detect breaches as prioritized by ISO/IEC 27001:2022 on continuous improvement [1]. They are also important in SwiftHealth, where such a complex data-sharing environment is essential to validate internal processes are resilient prior to external validation and to facilitate compliance with the Uganda Health Data Protection, Privacy and Confidentiality Guidelines (2025).
* **Third-Party Audits**: Third-party audits are essential to becoming certified to the ISO/IEC 27001:2022 standard and give a third party and formally recognized evaluation of ISMS maturity. An external audit will make sure that international standards and Uganda regulations are adhered to improving credibility to the patients, regulators and donors. As an example, third-party auditors may certify encryption controls in line with clause 5.31 to the extent that telemedicine platforms are aligned with ISO/IEC 27701:2019 requirements related to privacy [4]. The deadline to switch to these audits by October 31, 2025, demonstrates the expediency of preparing to such audits.
* **Second-Party Audits**: Even though significant in the context of third-party risks, these audits target vendors unlike the internal ISMS of SwiftHealth. They are not critical in evaluating the overall effectiveness of ISMS but critical in determining the effectiveness of the vendor as a component that indirectly promotes ISMS effectiveness under the Uganda Health Data Access, Sharing and Use Guidelines (2025).

The two-sided style takes advantage of the benefits of both kinds of audits: internal to foster continuous improvement and external to establish certification and credibility in line with both SwiftHealth aims of compliance and avoidance of leakage of sensitive patient data coupled with the Milestone One requirements of implementing audit expertise when managing ISMS.

1. **Application of Auditing Principles as an ISO 27001 Auditor**  
   As ISO 27001 Auditor the objective of implementing an unbiased, evidence-based and value added audit process is informed by principles as stipulated in ISO 19011:2018 that details the guidelines on auditing management systems [5]. As these data involve sensitive corporate health data, supply chain data and patient-related records, an ISO 27001 audit emphasizes strong information security-related practices, so we apply it to the SwiftHealth Uganda ISMS audit as follows:
2. **Integrity**

Integrity lies at the core of professionalism that urges auditors to be procedurally just, honest and fair in executing duties (ISO 19011:2018). Auditors should be professional, ethical and acting without bias based on a professional code of conduct that does not lead to conflicts of interest [5]. In order to have integrity, third-party audits will involve the external auditors to avoid internal bias because they are not affiliated to SwiftHealth.

When auditing SwiftHealth Uganda, I would use integrity in terms that I would display any such conflicts (past relationship with the suppliers of the pharmaceutical industry in Uganda) at the beginning and recuse myself when necessary to ensure bias. I would be truthful in the audit such as recording the ISMS controls to protect the data in medical supply chains without either over or under reporting to ensure such an exercise will be evidence-based by effectively analyzing of records like access logs [4]. This is a value addition in building confidence of the audit results that can see SwiftHealth Uganda make countable changes on information security such as better encryption of the patient data to end up in cutting risks of breach driving their healthcare management processes.

1. **Fair Presentation**

Fair presentation means that the auditors should positively, truthfully, accurately and objectively report, even when the results not to the favor of the organization (ISO 19011:2018). Findings of audits should be precise, objective and accompanied by verifiable evidence and nonconformity and improvement opportunities should be reported clearly [5].

In the case of SwiftHealth Uganda, my approach would be using fair presentation whereby all important findings as a result of the review of the ISMS (strengths in the supplier vetting processes and weaknesses in the incident response) would be captured objectively in the report including any disputes that could not be settled on the effectiveness of controls. This ensures objectivity in taking an unbiased approach to the assessments that avoids any possible favoritism on the part of self-evaluation within the organization is evidence based through its ability to back up with the references to documents such as risk assessment and also adds value by its clarity and actionable findings (time frames in enhancing vulnerability management) to the company in making it more compliant in its handlings and efficiency in the management of sensitive medical supplies information [3].

1. **Due Professional Care**

Auditors should be diligent in the application of professional skepticism in an effort to identify risks or nonconformities [5]. Based on this principle, auditors are required to employ diligence, prudence and exert judgment in any occasion bearing in mind the significance of the task and stakeholder trust. The auditors are also going to examine the ISMS controls by SwiftHealth with a critical eye, with high-risk zones such as third-party vendor integration and data encryption (5.31).

In SwiftHealth Uganda, the due professional care would include a comprehensive assessment of their ISMS documents such as data classification policies across pharmaceutical inventories and the practice of judgment to focus on high-risk areas such as the control of third-party access. This enhances objectivity with care in conducting systematic, non-biased reviews, evidence-based because cross-checks claims with audit trails (logs of healthcare facilities systems) and value addition like uncovering situation improvement gap for example through training programs to reduce safety risks posed by human factor hence helps in enhancing overall security in an organization as well as sustainable growth in Uganda health sector [3].

1. **Confidentiality**

Auditors need to guard sensitive information, including patient data in the course of audit [5]. This principle secures sensitive information that may have been obtained during audits using it inappropriately or revealing the same to other parties in a way that would waste the auditee right interest. It also complies with such standards as ISO 27001 in highlighting secrecy particularly to data that is proprietary or personal and also eliminates any personal benefit of the audit information. To protect the data of patients, all audit operations will comply with ISO/IEC 27001:2022 control 5.12 (classification of information) and ISO/IEC 27701:2019 privacy controls (PIMS 6.2.1.1) [4].

In the case of SwiftHealth Uganda audit, I would implement confidentiality following safe management of sensitive information such as health records of patients or supply chain agreements involving encryption of data storage and dissemination to only eligible recipients. This reflects both fairness against the touch of outside information and evidences an evidence-based process based purely on relevant, protected evidence beyond unauthorized access and value-adds-by being a strong security role model to the entire healthcare sector prompting the organization to implement similar measures (Non-disclosure agreements with suppliers) which contributes to higher trust to the organization among clients and its lower susceptibility to legal penalties in a regulated healthcare sector in Uganda.

1. **Independence**

Auditors should not be biased or influenced so as to achieve objectivity [5]. According to this principle, auditors need to have no conflicts of interest and be not under any external influence that constitutes the basis of objective conclusions. Independence guarantees the conclusion of findings depending not on affiliations or impacts, but the evidence only. Third party auditing will be carried out by external auditors of accredited certification bodies so as to be independent.

In the case of SwiftHealth Uganda, I would protect the independence of the company by choosing an external audit team which is not related to the company operation and competitors in the pharmaceutical market in Uganda to be avoided in positions of consultant and which may jeopardize independence. This direct implementation of impartiality makes the audit evidence-based since it can be based on the unbiased selection of ISMS components such as access controls and provides value in that it gives a third-party view of the risks (insider threats in facility management), allowing specific corrections that enhance security and operational integrity.

1. **Evidence-Based Approach**

The findings of an audit cannot be conclusions; it should be made out of evidence and not impression and estimates [5]. This principle requires that the conclusions will be based on sufficient verifiable evidence which includes relevant samples that give high levels of confidence in their results. It consists of collecting and analyzing information in a methodical manner to result to reproducibility and reliability based on facts than assumptions to validate sound audit result. The planned audit will be based on ISO/IEC 27002:2022 checklists to assess such controls as monitoring activities (8.16) or supplier relationships (5.19) [2].

When auditing SwiftHealth Uganda, I would use evidence-based as a way of gathering and checking samples of evidence such as logs of security incidents or training records of employees, to determine whether ISMS was being met. This provides independent reviews based on facts, automatically renders the process evidence-based and provides value as it facilitates the tracking of evidence-based gaps (an improper monitoring of medical equipment data) within the organization thus enabling it to focus remedies that avert breaches and enhance optimum resource deployment in their healthcare supply services [3].

1. **Risk-Based Thinking**

The audits need to focus on high risk areas to the organizations aims [5]. This principle guides auditors in allocating priority to risks and opportunities in auditing planning, conducting and reporting processes so as to focus on critical areas which may affect objectives. It does not get too involved in the inconsequential matters but on possible ways in which the management system could be compromised such as risks in quality of the procedures.

In the case of SwiftHealth Uganda, my approach to the risk-based audit should be narrowing down the scope of the audit to the heightened risk areas such as cyber threats to pharmaceutical data or supply chain disruption in Uganda, depending on their risk assessment. This keeps it unbiased by weighing risks in a non-biased manner, promotes evidence-based decisions by directly using evidence (control tests on risky assets), value-added to provide newer insights such as employing cloud security to achieve more scalability and improve the overall ability of the ISMS further contributing to the competitive advantage of the company in healthcare services [2].

**Conclusion**  
Combined first and third-party auditing is most suitable when assessing the maturity of ISMS of SwiftHealth Uganda with relevance in the provision of internal gap analysis and an external assessment to support certification to the standard ISO/IEC 27001:2022. The audit process is impartial, reliable and valuable through the application of auditing principles (integrity, fair presentation, due professional care, confidentiality, independence, evidence-based approach and risk-based thinking). These are appropriate measures that fall in line of the objectives of SwiftHealth in terms of protecting sensitive health data, accomplishing compliance, and gaining the confidence of stakeholders that form a foundation of a strong ISMS.

**Part B: Risk Management and Third-Party Security**

**a) Evaluation of Information Security Risks Associated with Integrating Third-Party Vendors for Cloud Hosting and Telemedicine Platforms**

Using third-party vendors in cloud hosting and telemedicine platforms in healthcare systems such as the SwiftHealth Uganda system poses a great risk to the information security of the organization. Such risks emerge as a result of dependence on the external parties to deal with vital processes, including data storage, transmission and processing of sensitive patients data, among others. According to peer-reviewed research and guidelines, the leading risks are divided into data privacy breach, vendor non-delivery, data loss or corruption and uncontrolled access through telemedicine.

1. **Data Breach Risk**

Data breaches happen due to exploitation of vulnerabilities in vendor systems by unauthorized actors that results in exposure of the protected health information (PHI). The conditions in cloud hosting, where there are improperly configured settings, unsafe APIs, or poor identity and access management may allow breaches. In the case of telemedicine, there is a possibility of risk due to unsecure data transfer when offering a remote appointment, like unencrypted video streams.

**Impact**: High risk because of the growing focus on healthcare suppliers; examples include the third party; the 2024 report is included in 41.2% of healthcare cases, most usually associated with ransomware [6]. The consequences are harsh such as regulatory fines or Uganda Data Protection and Privacy Act, 2019 (Section 26) reputational damages, and patient harm in case the leaked medical records are spread. The Personal Data Protection Office (PDPO) recently issued its 2025 enforcements showing punitive actions in cases of breaches that impose fines up to millions of UGX [7]. Research indicates that the average cost of a healthcare data breach is around 10.93 million dollars around the world and third party complications increase losses [8].

**Relevance to Standards**: This vulnerability breaks control ISO/IEC 27001:2022 Annex A 5.19 (information security in supplier relationships) and 8.30 (outsourced development) because vendors might not due to any weak encryption (5.31) or access (8.2) [1]. ISO/IEC 27701:2019 PIMS 6.10.2.3 (encryption of personal data) is of paramount importance in the protection of PHI [4]. According to peer-reviewed analysis of telemedicine systems, third-party systems cannot support end-to-end encryption as a feature leading to breaches [9]. In the case of SwiftHealth, a breach might undermine the capacity of the ISMS to uphold confidentiality and integrity that would undermine Clause 6.1.2 (risk assessment) [1].

1. **Vendor Non-Compliance Risk**

**Description:** Vendors will not comply with security standards or regulations, including the ISO/IEC 27001:2022 or the Uganda Data Protection and Privacy Act, 2019, resulting in indirect non-compliance in SwiftHealth. This involves subcontractors in the supply chain who do not have the right certifications or controls.

**Likelihood and Impact:** Medium to high likelihood due to the common presence of multiple tiers of vendors at different levels of security maturity with the healthcare supply chain [10]. The effects are regulatory breaches, loss of ISO/IEC 27001:2022 certification and industry credibility with stakeholders. Third-party non-compliance A 2025 PDPO decision resulted in the fining of a healthcare provider due to the emphasis on strong third party oversight [11]. According to a research on healthcare IoT systems, third party vendors create compliance gaps that lead to 90 per cent of the major breaches associated with the failure of supply chain [10].  
**Relevance to Standards**: The weakness violates the provision at ISO/IEC 27001:2022 Annex A controls 5.20 (treatment of information security in supplier contractual relationships), and 5.21 (management of information security within the ICT supply chain) [1]. ISO/IEC 27701:2019 PIMS 6.2.1.1 (access control to personal data) plays a crucial role in providing the vendor compliance with privacy requirements [4]. Peer-reviewed studies stress that insufficient vendor due diligence results in regulatory non-compliance that advocates to use ISO/IEC 27001-aligned assessments [8]. In the case of SwiftHealth, the threat would mean that ISMS certification may be threatened, as vendors processing or otherwise working with PHI are required to be in line with the Uganda Health Data Access, Sharing and Use Guidelines (2025).

1. **Data Loss or Corruption Risk**

**Description:** The possibility of missing data or corruption of data due to vendor system failure, poor backups or cyberattacks is real since telemedicine and cloud-hosted patient records would be involved. Typical causes include being poorly planned disaster recoveries or zero-day exploits in vendor software.

**Likelihood and Impact:** Medium likelihood and high impact in healthcare where a corrupted data set might interfere with the treatments or provoke misdiagnoses. Some studies have shown that 7 in 10 healthcare organizations encounter interruptions caused by third-party failures with millions on average being spent on paying them back [12]. Failure to comply with data retention requirements by the Uganda Health DataProtection, Privacy and Confidentiality Guidelines (2025) would attract regulatory penalties [13].

**Relevance to Standards:** This risk violates the standards of ISO/IEC 27001:2022 Annex A 8.13 (back-up) and 5.26 (information security incident response) [1]. The ISO/IEC 27002:2022 proposes the use of strong backup and recovery policies to avert loss of data [2]. A risk assessment conducted on point-of-care systems in healthcare cautions that third party telemedicine services easily experience ineffective backup controls which heightens corruption risks [12]. To SwiftHealth, this might deteriorate ISMS performance in Clause 8.1 (operational planning and control) [1].

1. **Unauthorized Access Risk via Telemedicine**

**Description:** Attackers can steal consultations or read records or intercept insecure platforms: phishing attack, man-in-the-middle attack, poor authentication. This is increased by the use of cloud hosting where vendors utilize shared environments without any suitable segregation.

**Likelihood and Impact:** The likelihood is high because of the use of remote access, and the evidence showcases phishing attacks targeting health care because according to an article published in 2024, such incidents increased by 35 percent [14]. The consequences are a breach of patient confidentiality, trust loss, and breaches of laws regulated by the Uganda Data Protection and Privacy Act, 2019 (Section 8, lawful processing) [3].

**Relevance to Standards:** This risk contravenes standard ISO/IEC 27001:2022 Annex A control 8.2 (privileged access rights) and ISO/IEC 27701:2019 PIMS 6.2.1.1 (access control of personal data) [1], [4]. Telemedicine security research points out that poor authentication methods are one of the major attack vectors [9]. To SwiftHealth, this risk poses a threat to ISMS goals of maintaining confidentiality and compliance with the Uganda Health Data Protection, Privacy and Confidentiality Guidelines (2025) [13].

**b) Propose Audit-Based Measures for Managing These Risks in Line with ISO 27001**

Audit-based action plans are recommended to address the identified risks to be able to comply with the ISO/IEC 27001:2022, ISO/IEC 27701:2019, and Ugandan laws and regulations and improve the effectiveness of ISMS within SwiftHealth.

1. **Vendor Risk Assessment (ISO/IEC 27001:2022, 5.19)**

**Measure:** Audit the vendors (second-party): Audit the vendors related similar controls as control and measures like encryption (5.31) uploading or authorizing the keys circumstances (8.2) and incident response (5.26) [1].  
**Implementation**:

* + Conduct audits twice a year with ISO/IEC 27002:2022 checklists to evaluate vendor controls, like secure configuration (8.9) and vulnerability management (8.8) [2].
  + Ensure vendors should offer evidence of ISO/IEC 27001:2022 certification or other security frameworks. Security assessment reports outside certified vendors are to be submitted as per the guidelines of healthcare supply chain research studies [10].
  + Reports on privacy-specific audits in accordance with ISO/IEC 27701:2019 PIMS 6.2.1.1 and 6.10.2.3 should be included, where applicable, to demonstrate compliance with the Uganda Data Protection and Privacy Act, 2019 (Section 8, data minimization) and the Uganda Health Data Protection, Privacy and Confidentiality Guidelines (2025) [4], [3], [13].
  + Implement vulnerability scanning tools such as Nessus to find possible vulnerabilities in vendor systems so that no critical vulnerabilities will be not patched more than 7 days.

**Outcome**: Mitigates risks of data breach and non-compliance by confirming that the vendors must comply with the security and privacy requirements as warned in 2025 PDPO enforcement actions [7].

1. **Contractual Controls (ISO/IEC 27001:2022, 5.20)**  
   **Measure**: Modify vendor agreements to require the satisfaction of ISO/IEC 27001:2022, ISO/IEC 27701:2019, and Ugandan regulation with other penalties in case of non-conformance [1], [4].  
   **Implementation**:
   * Add provisions to clauses to have vendors keep audit trails (8.16) and provide quarterly security reports in line with ISO/IEC 27002:2022 recommendations [2].
   * Introduce a 72-hour breach notification requirement in line with the Uganda Data Protection and Privacy Act, 2019 (Section 22) and Uganda Health Data Access, Sharing and Use Guidelines (2025) [3].
   * Make vendors perform regular penetration tests and report results which must comply with control 8.30 (outsourced development) [1].
   * Apply legal reviews to enforce contractual obligations as advised by a 2025 PDPO decision concerning accountability of the vendors [11].

**Outcome**: Reduces the risk of non-compliance with the vendor to vulnerabilities by stating clear vendor security expectations and accountability processes.

1. **Technical Audits of Cloud and Telemedicine Platforms**  
   **Measure**: Technical audits on secure configurations, encryption and access controls in vendor systems that are in line with ISO/IEC 27001:2022 and ISO/IEC 27701:2019 [1], [4].  
   **Implementation**:
   * Payment of any cloud hosting providers running secure configuration (8.9), encryption at rest and in transit (5.31) and multi-factor authentication (8.5) - such as Qualys or Wireshark to ensure AES-256 encryption [2].
   * Exercise telemedicine web-based platforms against possible vulnerabilities (OWASP Top 10, like SQL injection or cross-site scripting) and check end-to-end encryption (PIMS 6.10.2.3) which is essential in telemedicine security [9].
   * Ensure that data segregation is in place in shared cloud environments to prevent unauthorized access in accordance with ISO/IEC 27001:2022 control 8.2 [1].
   * Write audit reports of findings and include evidence such as packet captures or configuration logs to make them traceable.

**Outcome**: Provides protection against risks of data breach and unauthorized access by having technical controls in place at the vendor systems to support the Uganda Health Data Protection, Privacy and Confidentiality Guidelines (2025) compliance [13].

1. **Incident Response Integration (ISO/IEC 27001:2022, 5.26)**  
   **Measure**: Audit the incident response plans of vendors in order to align them with the ISMS of SwiftHealth and ascertaining whether they comply with regulatory requirements [1].  
   **Implementation**:

* The vendor incident response plans have to be reviewed to make sure they include breach detection and containment and notification practices as required by the Uganda Data Protection and Privacy Act, 2019, (Section 22) [3].
* Engage vendors in mock-based tabletop trainings to test breach processes (ransomware attacks) and ensure impact on response effectiveness based on the healthcare security studies [8].
* Be able to have vendors integrate into the SwiftHealth SIEM tools to monitor in real-time (8.16) and detect and respond swiftly [2].
* Confirm that the vendors keep records of incidents, and report breaches within 72 hours as in accordance with 2025 PDPO enforcement trends [7].

**Outcome**: Minimizes the effect of data breaches through coordinated and timely response to incident to improve the resilience of the ISMS.

1. **Continuous Monitoring**  
   **Measure**: Create a system of continuous monitoring of the performance of the vendors based on security information and event management (SIEM) tools and audit on a regular basis [2].  
   **Implementation**:
   * Install SIEM (Splunk) solutions to detect abuse of vendor systems against unauthorized access or anomalies reflecting the ISO/IEC 27002:2022 control 8.16 [2].
   * Arrange quarterly second-party audits in order to ensure that ongoing compliance with these controls is maintained with a specific emphasis on the following items that are more prone to cause an impact; encryption (5.31), and access management (8.2) [1].
   * Track the security score somewhere in the line of measures such as patch compliance indicators and corrective actions response time provided by the vendors as advised by the researchers in the sphere of supply chain security [10].
   * Revise the ISMS risk register according to monitoring results in response to new threats to ensure compatibility with ISO/IEC 27001:2022 Clause 6.1.2 [1].

**Outcome**: Addresses all the risks identified by allowing proactive inspection and response that guarantees uninterrupted compliance and ISMS functionality.

**Conclusion**

Use of third-party vendors to provide cloud hosting and telemedicine solutions also poses a severe risk to SwiftHealth Uganda ISMS such as data breaches, vendor non-compliance, data loss or corruption and unauthorized access. These risks pose a threat to ISO/IEC 27001:2022, ISO/IEC 27701:2019 and Ugandan compliance, patient confidence and operational resilience. These proposed audit-based measures (vendor risk assessments, contractual controls, technical audits, integration and ongoing audits and incident response) present a decent measure against these risks when considered in place. These measures can guarantee that vendors meet security and privacy requirements highlighted through recent law enforcement of PDPO and guidelines in the health sector using ISO/IEC 27002:2022 checklists, SIEM tools, and penetration testing.

**Part C: Nonconformity Report and Presentation**

**a) Nonconformity Report Following a Security Incident**

A Nonconformity Report is drawn up in accordance with ISO/IEC 27001:2022 Clause 10.1 (nonconformity and corrective action) and ISO 19011:2018 guidelines, following a security incident in which an external attacker exploited a vulnerability in a telemedicine platform of a third-party vendor which led to the exposure of patient records [1], [5]. The report deals with how the incident affected the ISMS of SwiftHealth and its compliance with the Uganda Data Protection and Privacy Act, 2019 and the Uganda Health Data Protection, Privacy and Confidentiality Guidelines (2025) [3], [13].

1. **Nonconformity Description**

A third-party vendor telemedicine platform reported to be unpatched on the security of one of the vendors was targeted by an outside hacker who hacked the patient records using an unpatched software vulnerability, allowing him to access diagnoses and insurance information about the patients. This failure led to the violation of sensitive health information in terms of confidentiality and integrity and breached:

* + Weak security of vendors oversight as a result of the ISO/IEC 27001:2022 Annex A control 5.19 (information security in supplier relationships) [1].
  + ISO/IEC 27701:2019 PIMS 6.2.1.1 (according to access control to personal data) since the vendor did not restrict its access to authorized users [4].
  + Uganda Data Protection and Privacy Act, 2019, Section 8 (lawful processing), and Section 22 (requirements to report breaches) [3].
  + Uganda Health Data Protection, Privacy and Confidentiality Guidelines (2025) that requires health data to be securely handled [13].

1. **Objective Evidence**
   * **Incident Logs:** Security Information and Event Management (SIEM) logs of Splunk dated [August 10, 2025] exhibit attempted unauthorized access and data exfiltration to the telemedicine platform with IP addresses that are associated with the hacker.
   * **Vendor Audit Report:** An independent second party audit (June 2025) documented pre-incident vulnerabilities UNPATCHED in the vendor system without signs of remediation within 7 days in violation of ISO/IEC 27002:2022 control 8.8 (management of technical vulnerabilities) [2].
   * **Patient Complaints:** Complaints of over 50 patients, reported through SwiftHealth data protection officer on [August 11, 2025] about unauthorized access to their records have been confirmed, with breach notification emails received by the vendor.
   * **Penetration Test Results:** Penetration tests (post incident) on [August 12, 2025], with Nessus validated the exploited vulnerability showed an element of failure by the vendor of installing vital updates.
   * **Regulatory Notification:** SwiftHealth should have notified the Personal Data Protection Office (PDPO) within the timeframe of 30 days as stipulated by Section 22, the notification by SwiftHealth on [August 11, 2025] verifies the extent and effect of the breach [3].
2. **Classification**

**Major Nonconformity**: According to its high level of implying data confidentiality in patient data and the work of the ISMS, this incident is considered a major nonconformity. The lack of an effective vendor management system (5.19) and vulnerability management (8.8) is a signal of serious failure to manage supplier relationships and puts certification and regulatory compliance with ISO/IEC 27001:2022 at risk [1]. The nature of the breach covering more than one patient record and its accordance with the patterns of 2025 enforcement of PDPO regulations regarding the cases of the third party breach prompt the necessity of this classification [7].

1. **Implications for ISMS Performance**
   * **Compliance Failure**: The violation of the Uganda Data Protection and Privacy Act, 2019 (Section 22) poses a risk of fines up to 2% of annual turnover as per recent 2025 pdpo ratiums [7]. Malpractices such as the failure to comply with the ISO/IEC 27701:2019 PIMS controls erode privacy protections which are vital to health data [4].
   * **Reputation Damage**: Leaking of patient records destroys patient and stakeholder confidence that can shrink the user base and partnerships of SwiftHealth noted by research on healthcare security issues [8].
   * **Operational Disruption**: Incident response, remediation and regulatory reporting processes and resource diversion used to respond to incidents disrupt healthcare operations services provisions and having an effect on operational effectiveness as per ISO/IEC 27001:2022 Clause 8.1 [1].
   * **ISMS Weakness**: There is a systematic weakness in third-party risk management which is not being mitigated effectively because of lack of enforcement of vendor controls (5.19) and vulnerability monitoring (8.8) in an effective ISMS system and preparation readiness certification [2].
2. **Recommended Corrective Actions**
   * **Immediate (1 Week)**:
     + Isolate compromised systems of telemedicine platforms to prevent any other unauthorized access.
     + Step 2: Based on critical patches, to prevent and treat CVE-2025-XXXX, apply updated vulnerability scans with Nessus Software that follows ISO/IEC 27002:2022 control 8.8 [2].
     + Apply multi-factor authentication (MFA) to any access to vendor systems and require control 8.5 [1].
   * **Short-Term (2-4 Weeks)**:
     + Perform a second-party audit with the vendor to determine that vulnerabilities are addressed and that the vendor is in compliance with ISO/IEC 27001:2022 (5.19) and ISO/IEC 27701:2019 (PIMS 6.2.1.1) [1], [4].
     + Revise contracts with vendors to contain tighter security provisions including mandatory patching and breach reporting within 72 hours, in accordance with the Uganda Data Protection and Privacy Act, 2019 (Section 22) [3].
   * **Long-Term (1-3 Months)**:
     + Set up a vendor risk management program whereby there is routine auditing and security scorecard as advised by ISO/IEC 27002:2022 control 5.20 [2].
     + Enforce continuous monitoring with SIEM (Splunk) to identify the anomaly in the vendor systems to comply with control 8.16 [2].
     + Educate SwiftHealth employees and vendors on incident response and secure development practices of software (5.7 ) to assure that they are complying with the Uganda Health Data Protection, Privacy and Confidentiality Guidelines (2025) [13].
   * **Preventive Measures**: Conduct collaborative tabletop exercises with vendors to test breach situation that leads to excellent integration of incident responses (5.26) [1].
3. **Presentation Strategy for the Closing Meeting**

The Nonconformity Report should communicate the problem, need or issue of interest with the SwiftHealth senior management (CISO, CEO, legal team) in terms of what needs to be done (solution focused), how to do it, when to do it in a structured methodical and engaging manner and in accordance to the ISO 19011:2018 guidelines of communicating (effective audit communication) [5]. The plan has consistency with earlier consultations on the need to consider stakeholders to enhance ISMS and is in line with ISO/IEC 27001:2022 Clause 9.3 (management review) [1].

1. **Opening Statement**
   * Mention the seriousness of the incident and how it affects patient trust and regulatory compliance, as well as how it relates to the mission of SwiftHealth to secure sensitive health data within the Uganda Health Data Protection, Privacy and Confidentiality Guidelines (2025) [13].
   * Present the audit as an important step toward ISO/IEC 27001:2022 certification and risk mitigation that highlights the organization is ready to become resilient and compliant with the overall 2025 PDPO enforcement trends [7].
2. **Structured Delivery**
   * **Structure**: Frame Nonconformity Report in a convenient structure:
     + **Description**: Describe the breach, and associate it to the vendor unpatched vulnerability and the breach to ISO/IEC 27001:2022 (5.19) and ISO/IEC 27701:2019 (PIMS 6.2.1.1) [1], [4].
     + **Evidence**: Summarize any objective evidence (SIEM logs, audit reports, patient complaints) in order to be credible and transparent.
     + **Classification**: Describe nonconformity top level classification and cite systemic failure to oversee vendor access and regulatory risk [7].
     + **Implications**: Identify the implications of compliance, reputation and operational effects and cite the average cost of misuse of healthcare information ($ 10.93 million) [8].
     + **Corrective Actions**: Provide immediate, short and long term actions with focus on quick wins (patching) and strategic (vendor risk framework).
   * **Visual Aids**: If possible provide charts to demonstrate impact of breaches (redacted estimate of number of affected records, likely fines) and the corrective actions schedule to ensure clarity by non-technical stakeholders.
   * **Regulatory Context**: Appeal to the legal obligation by referencing the Uganda Data Protection and Privacy Act, 2019 (Section 22) as well as the guidelines in the health sector as given in 2025 [3], [13].
3. **Engaging Management**
   * **Stakeholder-Specific Messaging**:
     + **CISO**: Point out technical vulnerabilities (absence of MFA, unpatched vulnerabilities), and suggest SIEM to manage real-time monitoring [2].
     + **Legal Team**: Focus on compliance risks and the fines of PDPO, with the references to the law enforcement in 2025 [7].
     + **CEO**: Preconcentrate on reputational and financial consequences, correlate potential corrective measures with the practice of building greater patient confidence and ISO/IEC 27001:2022 certification advantages [1].
   * **Timeline and Resources**: A straightforward timeline (1 week for patching, 1 month for contract updates, 3 months vendor framework) and estimation of resource requirement (audit tools, training budget) should be proposed with feasibility.
   * **Benefits**: Highlight how remedial measures will mitigate risks of breach, foster compliance and make SwiftHealth a reputed digital health support service provider, similar to peer-reviewed reports on the importance of sound ISMS [8].
4. **Call to Action**
   * Obtain management approval of resources in the remedial context such as funding of SIEM tools and the hiring of external auditors.
   * Suggest task force consisting of the CISO and others to manage vendor risk and monitor vendor implementation.
   * Agree to perform follow-up audits 3 months later to ensure remediation with progress reported at the next ISMS management review meeting (Clause 9.3) [1].
5. **Tone and Approach**
   * Adopt a professional tone in a constructive manner with an emphasis on solutions instead of blame as suggested in ISO 19011:2018 [5].
   * Encourage questions and collaboration so that the management knows the urgency and supports corrective actions, creating a proactive security culture..

**Conclusion**

The Nonconformity Report covers a serious security incident by an unpatched vulnerability of a third-party vendor that led to patient data being exposed and breaching ISO/IEC 27001:2022 and ISO/IEC 27701:2019 controls, along with Ugandan laws and regulations. Based on objective evidence, the report categorizes the problem as a significant nonconformity because of its systemic nature, and the major impact on the performance of ISMS. Mitigation measures based on strategic actions have been recommended which are immediate patching, short-term audits and long-term vendor risk management which help minimize the risks and increase resilience. The presentation approach guarantees the involvement of the management by explaining adequately the implications of the incident, offering remedial solutions, and has synergies with the objectives of SwiftHealth relating to compliance and patient confidence.

**Part D: Risk Treatment Plan and Verification**

**a) Risk Treatment Plan Based on Nonconformities Identified in Part C**

The nonconformity described in Part C is that of an external attacker using a third-party vendor telemedicine platform vulnerability (CVE-2025-XXXX), which has not been patched, and a malicious actor makes unauthorized access to patient records. This significant nonconformity contravenes ISO/IEC 27001:2022 control 5.19 (information security in supplier relationships) and IS ISO/IEC 27701:2019 PIMS 6.2.1.1 (access control to personal data) and the Uganda Data Protection and Privacy Act, 2019 (Section 8, lawful processing) [1], [4], [3]. This risk is mitigated by the Risk Treatment Plan below, which complies with Clause 6.1.3 (risk treatment) of ISO/IEC 27001:2022 and the corresponding ISO/IEC 27002:2022 guidelines and deals with the problems of systemic control of vendors and vulnerability management [2].

1. **Risk Identification**
   * **Risk**: Confidentiality and integrity breach through unauthorized access of the patient data as a vulnerability in the telemedicine platform of a third-party vendor is not addressed, and this may affect the data or its privacy.
   * **Standards Violated**:
     + There are 5.19 (relationships with suppliers) and 8.8 (management of technical vulnerabilities) in Annex 1 of the ISO/IEC 27001: 2022 standard [1].
     + The provisions of ISO/IEC 27701:2019 address PIMS 6.2.1.1 (access control) and PIMS 6.10.2.3 (encryption of personal data) [4].
     + Uganda Data Protection and Privacy Act, 2019, s 8 (lawful processing), s 22 (breach notification), [3].
     + Uganda Health Data Protection, Privacy and Confidentiality Guidelines (2025), which requires the secure integrity of processing health data processing [13].
   * **Root Cause**: Insufficient vendor control, absence of virus solutions and patch upkeep (patch timely), absence of strong access control and encryption.
2. **Risk Treatment Options** (ISO/IEC 27001:2022, Clause 6.1.3)
   * **Mitigate**: Putting in place measures to prevent the risk eventualities of the risk.
   * **Avoid**: End contract with the vendor when remediation is not possible across a stipulated timeline.
   * **Transfer**: Put risk on vendors via penalties in a contract or insurance.
   * **Accept** Residual risk should be accepted just when it is minimal and endorsed by management as a result of installing controls.  
     **Selected Option**: The option of mitigation is selected to resolve the nonconformity without terminating the relationship with the vendor since this can affect the delivery of telemedicine service. Mitigation reflects the risk-based approach in ISO/IEC 27001:2022 and promotes adherence to the Ugandan laws [1], [3].
3. **Risk Treatment Plan**
   * **Control 1: Vulnerability Management (ISO/IEC 27001:2022, 8.8)**
     + **Action**: Impose the requirement on the vendors to establish the vulnerability management process, implementing the critical patches no later than within 7 days after publication, checked by the vulnerability scans with the help of such tool as Nessus.
     + **Rationale**: Solve the cause of the breach (unpatched vulnerability: CVE-2025-XXXX) as per the ISO/IEC 27002:2022 guidelines on how to remediate in a timely manner [2].
     + **Implementation**: Contract mandatory monthly patch compliance reports, and Quarterly vulnerability scans by vendors. The IT team at SwiftHealth will monitor the results of scans to make sure that there are no severe vulnerabilities that will go unpatched.
   * **Control 2: Enhanced Access Controls (ISO/IEC 27001:2022, 8.2; ISO/IEC 27701:2019, PIMS 6.2.1.1)**
     + **Action**: Implement multi-factor authentication (MFA) on all access to vendor systems containing patients data and the least privilege concept.
     + **Rationale**: Keeps out unauthorized users, which is needed to combat the effects of breach on confidentiality as dictated by the UDPP law 2019 (Section 8) [3].
     + **Implementation** Within 2 weeks implement MFA solutions (Okta) across the vendor platforms and the review of access logs on these platforms monthly using SIEM tools (Splunk).
   * **Control 3: Encryption (ISO/IEC 27001:2022, 5.31; ISO/IEC 27701:2019, PIMS 6.10.2.3)**
     + **Action**: Data in-transit and at-rest encrypted end-to-end (AES-256) on vendor systems with technical audits on encryption usage.
     + **Rationale**: This will guarantee data confidentiality and integrity of the patient and mitigate the risks of data breach as outlined in the Uganda Health Data Protection, Privacy and Confidentiality Guidelines ( 2025 ) [13].
     + **Implementation**: Carry out packet analysis (using Wireshark) to verify the encryption requirements, audit done after every 6 months to verify compliance.
   * **Control 4: Incident Response Integration (ISO/IEC 27001:2022, 5.26)**
     + **Action**: Test the vendors to ensure their incident response plans conformed to those of SwiftHealth ISMS, with breach notification in less than 72 hours.
     + **Rationale**: Provides early identification and intervention with incidents as required by the Uganda Data Protection and Privacy Act, 2019 (Section 22) [3].
     + **Implementation**: Hold collaborative tabletop exercise sessions every quarter and trial the effectiveness of responses and finally capture that in audit reports.
   * **Control 5: Vendor Risk Management Framework (ISO/IEC 27001:2022, 5.19)**
     + **Action**: Develop a vendor risk assessment framework and include regular security scorecards on vendors and audit the vendors regularly.
     + **Rationale**: Covers systematic vendor oversight failure as 2025 PDPO enforcement cases point out [7].
     + **Implementation**: Design a scorecard on which to monitor patch compliance, response times of the incidents and audit results checked after six months. Within 1 month update the contract of vendors to have security clauses.
4. **Implementation Plan**
   * **Timeline**:
     + Immediate (1 Week): Activate MFA, isolate and repair affected machines system.
     + Short-term (2-4 weeks: Conduct 2nd Party audits, Update contracts encryption.
     + Long Term (1-3 Month): Define vendor risk framework, SIMTable Top Exercise, SIEM Surveilance.
   * **Resources**: IT security team, vendors management team, external auditors, SIEM tools (Splunk) vulnerability scanners (Nessus) encryption solutions.
   * **Responsibilities**:
     + RID: Performs audit, Implements and Coordinates CISO: Implements and Coordinates.
     + IT Group: Managing technical controls(patching, MFA, Encryption)
     + Vendor Managers: Re-negotiating/combatting of contracts & handling of audits.
   * **Cost**: SIEM tools: budget of $50 000 annually; vulnerability scanners: budget of 10 000 annually; training: budget of 5000 and audit services: budget of 20000 since the savings achieved is cost of breaches (average of 10.93 million) [8].
5. **Residual Risk**
   * Once controls have been brought in place, the residual risk becomes low provided there is compliance on the part of vendors regarding audit and contract.
   * Actively monitor residual risk using SIEM tools and quarterly audits and respond to emerging threats, such as zero-day exploits, as identified in 2024 healthcare threat reports [14].

**b) Verification During a Follow-Up Audit**

To ensure the effectiveness of the Risk Treatment Plan and efficiency thereof, a follow-up auditing will be performed 3 months after implementation in accordance with ISO/IEC 27001:2022 Clause 9.2 (internal audit) and the ISO 19011:2018 guidelines [1], [5]. The audit confirms that the controls are used to correct the nonconformity maintain positive ISMS performance and assist SwiftHealth to meet its goals of protection of patient data and compliance with regulations continuing with the nonconformity report found in Part C.

1. **Audit Scope**
   * **Controls**: ISO/IEC 27001:2022 Annex A 5.19 (supplier relationships), 8.8 (vulnerability management), 8. 2 (access control), 5.31 ( security, in context of encryption), 5.26 (incident response) and ISO/IEC 27701:2019 PIMS 6.2.1.1 (access control) and PIMS 6.10.2.3 (encryption) [1], [4].
   * **Regulatory Compliance**: Uganda Data Protection and Privacy Act, 2019 (Sections 8, 22) and Uganda Health Data Protection, Privacy and Confidentiality Guidelines (2025) [3], [13].
   * **Focus Areas**: Vendor telemedicine platform, oversight processes and incident response integration SwiftHealth.
2. **Audit Methodology**
   * **Document Review**:
     + Confirm that existing contracts with vendors are updated to include coverage of security terms (patch management, breach notification) of control 5.20 [1].
     + Review patch management policies, incident response plan and records of training to make sure that ISO/IEC 27002:2022 is applied [2].
     + Retrieve tabletop exercise reports, and staff training completion records (5.7) [1].
   * **Technical Testing**:
     + Scan vulnerability (Nessus) to ensure that there are no critical vulnerabilities out of patch beyond 7 days.
     + Conduct penetration tests to confirm MFA and AES-256 encryption, both on data in transit and at rest, with such tools as Wireshark [4].
     + Test the staging of the telemedicine platform in terms of secure settings (no open resources, manage 8.9) [2].
   * **Interviews**:
     + Interview personnel in the vendors to ensure that MFA is in place and patches updates are on schedule.
     + 5.26 Interview SwiftHealth IT and vendor management teams to confirm training and incident response preparedness (5.26) [1].
     + Check with the CISO that SIEM monitoring is functioning and useful.
   * **Log Analysis**:
     + Review SIEM logs (Splunk) to look at attempts to gain unauthorized access or anomalies (8.16) [2].
     + Audit the trail to determine whether breach notifications and responses took place in time and according to the Uganda Data Protection and Privacy Act, 2019 [3].
3. **Effectiveness Criteria**
   * **Patch Management**: There were no high severity findings past 7 days unpatched in scan reports confirming no critical vulnerabilities were left unpatched.
   * **Access Controls**: MFA is implemented during all vendor access which has been confirmed through the access logs which have not had unauthorized access.
   * **Encryption**: AES-256 encryption has been applied to data at rest and on the network and is validated through packet analysis and audit reports.
   * **Incident Response**: Vendor to have 72-hour breach notification, verified due to Tabletop Exercise results, as well as, Section 22 compliance [3].
   * **Vendor Management**: No serious nonconformities are reported by quarterly audits, and security scorecards demonstrate on-going conformity [2].
4. **Efficiency Criteria**
   * **Minimal Disruption**: Control measures put in place with minimal disruptions to the telemedicine functioning e.g. verified through operational reports that indicate zero disruptions.
   * **Cost-Effectiveness**: Budget-friendly costs confirmed using financial records, costs that were below budget due to the use of automation tools (patch management software) decreasing manual work.
   * **Sustainability**: To maintain controls there is little maintenance required which can be proved with vendor compliance reports and the staff opinion regarding ease of use [5].
5. **Follow-Up Actions**
   * **Reporting**: Report on findings in follow-up audit report, the findings on whether the compliance was met, remaining risk residuals and new nonconformities [5].
   * **Management Review**: Report findings at the next ISMS management review (Clause 9.3) to gain approval to further actions, e.g. more advanced monitoring applications [1].
   * **Plan Updates**: Modify the Risk Treatment Plan in the event of the emergence of another risk (Wall Street Journal example: evolving forms of ransomware), and enact subsequent revisions with ongoing improvements under Clause 10.2 [1], [14].

**Conclusion**

The Risk Treatment Plan focuses on major areas of Nonconformity (unauthorized access caused by an unpatched vendor vulnerability) eliminating it using specific controls: vulnerability management, enhanced access controls, encryption, Incident Response integration and a vendor risk management framework. Such actions are in line with the practices of ISO/IEC 27001:2022, ISO/IEC 27701:2019 and regulations of Uganda, minimizing the chances of breaches and compliance. The implementation is also verified in the follow-up audit to make sure that the implemented controls are effective in preventing the recurrence, efficient in continuation of operations and collection of evidence is rigorous through documentary reviews, technical tests, interviews, logs analysis.

**Part E: Continuous ISMS Audit Program and Reflection**

**a) Continuous ISMS Audit Program for SwiftHealth Uganda**

An ongoing ISMS audit program will help to maintain compliance in SwiftHealth Uganda, reduce the observed vulnerabilities and improve resilience of its data-sharing platform. In conformity with ISO/IEC 27001:2022 Clause 9.2 (internal audit) and ISO 19011:2018 recommendations, the program targets the risks reported in Part C (third-party vendor breach) and adds the prescribed corrective actions in Part D Risk Treatment Plan [1], [5]. It will enable adherence to the Uganda Health Data Access, Sharing and Use Guidelines (2025) and make SwiftHealth ready by the October 31, 2025, transition deadline to be ISO/IEC 27001:2022 certified.

1. **Audit Objectives**
   * Provide a future guarantee of adherence to the ISO/IEC 27001:2022, ISO/IEC 27701:2019, the Uganda Data Protection and Privacy Act, 2019 (sections 8, 22) and the Uganda Health Data Protection, Privacy and Confidentiality Guidelines (2025) [1], [4], [3].
   * Actively find and mitigate ISMS control gaps to keep certification and further enhance security governance.
   * Observe the third-party vendors (cloud hosting, telemedicine platforms) to minimize risks, and respond to the Part C vendor vulnerability.
   * Drive continuous improvement by integrating audit findings into the ISMS, aligning with the Plan-Do-Check-Act (PDCA) cycle [1].
2. **Audit Types and Frequency**
   * **Internal (First-Party) Audits**: Periodically, every 3 months, assessing all 93 Annex A controls of ISO/IEC 27001:2022, most important areas being access control (8.2), encryption (5.31) and incident response (5.26) [1]. These audits are going to deal with internal weaknesses, working on the Part A where costs effective analysis of gaps was promoted.
   * **Second-Party (Supplier) Audits** Conducted by semi-annual basis to select suppliers to ensure they meet the requirements of ISO/IEC 27001:2022 control 5.19 (supplier relationships) and ISO/IEC 27701:2019 PIMS 6.2.1.1 (access control) [1], [4]. Since the risks of third parties are mentioned in Part B, this moderates third-party risks.
   * **Third-Party (External/Certification) Audits**: These audits are carried out on an annual basis, by an accredited certification body, to eventuate ISO/IEC 27001:2022 certification, and bi-annual (half yearly) surveillance audit to monitor sustained compliance [1]. These audits are a form of neutral confirmation, as was demonstrated in Part A.
   * **Ad-Hoc Audits**: Activated by the occurrence of critical events (violations, regulatory changes) e.g. the Part C incident to mitigate the risks that arise [5].
3. **Audit Scope**
   * **ISO/IEC 27001:2022 Controls**: Overall inspection of Annex A controls, with particular concern on vendor related controls (5.19, 5.20), access controls (8.2) and encryption (5.31, incident response (5.26) [1].
   * **ISO/IEC 27701:2019 Privacy Controls**: PIMS 6.2.1.1 (access control) and PIMS 6.10.2.3 (encryption) order to support privacy compliance [4].
   * **Regulatory Requirements**: Uganda Data Protection and Privacy Act, 2019 (Sections 8, 22) and Uganda Health Data Protection, Privacy and Confidentiality Guidelines (2025) [ 5] [ 14 ].
   * **Vendor Systems**: Cloud hosting and telemedicine platforms, with secure configurations and arrangements to be compliant with contracts, mitigating concerns of risk as seen with Part B [2].
4. **Audit Process**
   * **Planning**: Conduct a yearly audit planning with emphasis on the areas of high risks (vulnerabilities of the vendors, patient data protection). Appoint auditors who are qualified to ISO/IEC 27001:2022 and 27701:2019, and make sure that auditors are competent according to ISO 19011:2018 [5]. Apply ISO/IEC 27002 2022 and 27701 2019 as audit standards [2], [4].
   * **Execution**: Obtain evidence by:
     + **Document Reviews**: Risk evaluations, security strategies, vendor agreements and response plans.
     + **Technical Tests**: Vulnerability scans (Nessus), penetration tests (Metasploit) and encryption checks(Wireshark) to check the functionality of controls such as 8.8 and 5.31 [2].
     + **Interviews**: Speak with IT personnel, vendor managers and vendor representatives to clarify on control implementation and training (5.7) [1].
     + **Log Analysis**: Use SIEM logs (Splunk) to analyze unauthorized access or anomalies (8.16) [2].
   * **Reporting**: Produce structured audit reports with sections for findings, nonconformities, evidence and corrective actions.
   * **Follow-Up**: Follow up on the audit by directing remedial actions to assess their success and revise the Risk Treatment Plan (Part D) on residual risks [1].
5. **Roles and Responsibilities**
   * **CISO**: Manages the audit regime, accesses resources and amalgamates the results into ISMS reviews (Clause 9.3) [1].
   * **Internal Audit Team**: This would carry out internal and second-party auditing and would remain independent as discussed in part A.
   * **External Auditors**: Conduct certification and surveillance audits in an objective validation process.
   * **Vendor Managers**: These managers arrange second-party audits and ensure vendor compliance, and they respond to the vendor oversight concerns under Part B.
6. **Tools and Resources**
   * **SIEM Tools**: Proactive detection through Splunk in order to monitor threats on a real-time basis (8.16) [2].
   * **Vulnerability Scanners**: Nessus or OpenVAS for identifying weaknesses (8.8) [2].
   * **Penetration Testing Tools**: A major goal is to put Metasploit to use in simulating attacks and verifying resilience.
   * **Audit Repository**: SharePoint to store report, evidence, traceability and compliance [5].
7. **Continuous Improvement**
   * Include review of audit findings within ISMS management reviews (Clause 9.3) in order to prioritize weak area improvements [1].
   * Ensure that the ISMS is updated according to future threats (ransomware, phishing) and PDPO enforcement in 2025 [8].
   * Carry consistent training of the staffs and vendors (5.7) to ensure staff security awareness as per the Uganda Health Data Protection, Privacy and Confidentiality Guidelines (2025) (2025) [13].

**b) Reflection on Contribution to Long-Term Resilience**

Auditing, nonconformity reporting and risk treatment planning are a holistic strategy that propels the force and strength of SwiftHealth Uganda in dealing with the threat of data breaches and changing threats as critically discussed below within the scope of ISO/IEC standards and on healthcare security issues.

1. **Audit Process**

The continuous audit program takes an aggressive approach to detecting weaknesses, so that controls such as encryption (5.31) and access (8.2) are not rendered useless [1]. Internal audits carried out quarterly identify internal weak spots whereas second party audits are performed semi-annually to tackle vendor risks as in the breach scenario in Part C. The compliance with ISO/IEC 27001:2022 and 27701:2019 is confirmed through annual external audits, which increases the credibility in front of the stakeholders [4]. As an example, encryption of vendors used by the medical facility can be audited to guarantee the safety of the patient data in case of telemedicine encounters with their care providers, which is regulated by the Uganda Data Protection and Privacy Act, 2019 (Section 8) [3]. Audits create accountability where staff and vendors are exposed to a culture that is focused in security, which is essential in healthcare environments where breaches make patients lose trust [9].

1. **Nonconformity Reporting**

Nonconformity reporting, systematically identifies ISMS breakdowns and reports (document) on the root cause (unpatched vulnerabilities), issues, to categories and provides corrective recommendations (patch management, 8.8) [2], [5]. Vendor audits and contract revisions were expected, and there is an intention to avoid a repeat of the third-party breach as a result of the Part C report. Evidence-based reports, which are clear as presented at the management reviews, win resources to be used in the area of improvements as highlighted by the presentation strategy in Part C. The process will make resilience stronger through limited breach consequences, compliance with the Uganda Data Protection and Privacy Act, 2019 (Section 22) and increased stakeholder confidence, as was observed in the 2025 trends of PDPO enforcement [3], [8]. Clearly and transparent reporting is considered to be in line with the fair presentation principle in Part A, developing faithfulness with patients and regulators.

1. **Risk Treatment Planning**

Risk treatment planning, helps to deal with risks by implementing specific controls such as multi-factor authentication (8.5), encryption (5.31) and vendor risk management (5.19) [1], [2]. By eliminating the cause of the breach of Part C, the plan limits the chances of breaches, which is consistent with the risk-based approach of ISO/IEC 27001:2022 (Clause 6.1) [1]. Audit findings help to continually update the plan to be adaptive to new threats, such as zero-day exploits as observed in 2024 threat reports [14]. As an example, verification of compliance by vendors to ISO/IEC 27701:2019 controls over privacy (PIMS 6.2) is useful in ensuring the rights of data subjects, promoting trust in patients [4], [3]. Monitoring residual risk through SIEM mechanisms as explained in Part D helps to maintain effectiveness to enable operational continuity.

1. **Long-Term Resilience**

The organizational combination of audits, nonconformity reporting and risk treatment is part of a volatile response cycle in line with the ISO/IEC 27001:2022 PDCA cycle [1]. Risks are determined through audits, nonconformity reports fix systemic problems, and risk treatment plans enforce controls so that the ISMS develops with threats and regulations. The strategy will reduce the financial and reputational costs, and healthcare breaches cost on average of 10.93 million [9]. Regulatory position and patient confidence, essential attributes of SwiftHealth digital health services [3], [13], are enhanced by compliance with ISO/IEC 27701:2019 and Ugandan regulations. These processes ensure that SwiftHealth is in a position to foresee and counter threats thereby making it operationally and competitively resilient through the creation of proactive security culture based on what the literature on healthcare security shows [9].

**Conclusion**

SwiftHealth Uganda sustaining the ISMS audit program in an effective and efficient manner where compliance, risk reduction and resilience are mitigated in the structured cycle of internal audits, second-party, third-party and ad-hoc audits. The program pursues the strategy of focusing on high-risk zones such as vendor systems and protection of the patient data by adhering to ISO/IEC 27001:2022, 27701:2019 and regulations of Uganda. All three processes involved during audit procedure, nonconformity reporting and risk treatment planning plan leads to resilience through proactive management of vulnerabilities, elimination of systematic problems and responding to emerging threats.

|  |  |
| --- | --- |
| [1] | I. 27001, "ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security controls," *ISO/IEC Standard,* 2022. |
| [2] | I. 27002, "ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls," *ISO/IEC Standard,* vol. 3, 2022. |
| [3] | UGANDA, "THE DATA PROTECTION AND PRIVACY ACT, 2019," THE REPUBLIC OF UGANDA, 2019. |
| [4] | I. J. 1. 2. Technical Committee, "ISO - ISO/IEC 27701:2019 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines," *ISO/IEC,* 2019. |
| [5] | I. J. 1. 2. Technical Committee, "ISO 19011: 2018 Guidelines for Auditing Management Systems," *ISO/IEC,* 2019. |
| [6] | Verizon, "Verizon: 2019 Data Breach Investigations Report," Computer Fraud & Security, 2019. |
| [7] | P. D. P. O. (PDPO), "2025 Annual Report on Data Protection Enforcement," Government of Uganda, 2025. |
| [8] | I. Security, "Cost of a Data Breach Report 2024," IBM Corporation, 2024. |
| [9] | A. K. e. al, "Security and Privacy Issues in Telemedicine: A Systematic Review," 2024. |
| [10] | M. A. e. al, "Third-Party Risk Management in Healthcare IoT Systems," *Computers & Security,* vol. 118, 2023. |
| [11] | P. D. P. O. (PDPO), "Decision on Healthcare Vendor Non-Compliance," *Government of Uganda,* 2025. |
| [12] | S. S. e. al, "Usability and Security in Healthcare Point-of-Care Systems," *International Journal of Medical Informatics,* vol. 167, 2023. |
| [13] | M. o. H. Uganda, "Uganda Health Data Protection, Privacy and Confidentiality Guidelines," *REPUBLIC OF UGANDA,* 2025. |
| [14] | C. a. I. S. A. (CISA), "2024 Threat Report: Healthcare Sector," *U.S. Department of Homeland Security,* 2024. |