HEALTH CARE AGENCY

INFORMATION SYSTEM AUDIT REPORT

TABLE OF CONTENTS

This report focuses on the discussion of Information Systems Audit Observations and corresponding Recommendations in the area of IT Governance, Development and Acquisition, IT Operations, Outsourcing, Continuity Planning, Information Security, and Application Controls when applicable. Some sections of the originally issued report were removed to protect the identity of the audit subject.

GOVERNANCE AND MANAGEMENT OF I&T[1]

1. **The Agency's governance and management of Information and Technology (I&T) needs improvement as it was exposed to the risk of misalignment of I&T objectives with the organization goals, unmanaged I&T projects, unrealized benefits of I&T investments and wastage of resources, among others. Moreover, a thorough and documented study was not conducted to assess if the selected system is the most advantageous option.**

1.1. It is important in the public health sector to improve healthcare, deliver health, and other related services faster. As public healthcare providers are now starting to rely on I&T, proper implementation, and good I&T governance are key to ensure intended benefits are realized and risks associated with implementing new technologies are managed.

1.2. I&T Governance is the discipline to help leaders understand why I&T goals must align with those of the organization, how I&T delivers value, how its performance is measured, its resources properly allocated and its risk mitigated.

1.3. Control Objectives for Information Technologies (COBIT) 2019, ITIL, and ISO/IEC 38500:2015 are some of the known framework used for governance and management of I&T. Each of these domains has high-level policies that form part of the framework and can be used by managers to build procedures, services, and operations that meet the organization's objectives.[2]

1.4. The efforts of the Management and IT staff for implementing projects aimed to automate processes and improve efficiency for the benefit of its stakeholders are recognized. However, in the course of the audit, the following deficiencies that need to be addressed to ensure effective implementation of I&T policies and projects were observed:

a. The Agency has no I&T Steering Committee or equivalent.

1.5. COBIT 2019, under Align, Plan and Organize (APO) 01.04, recommends one of its activities to "establish an I&T steering committee or equivalent composed of executive, business and I&T management to track the status of projects, resolve resource conflicts, and monitor service levels and service improvement.[3]"

1.6. I&T Steering Committee ensures programs and projects meet business requirements and align with the I&T architecture. They determine the overall level and allocation of resources to extend to I&T value across the enterprise while ensuring they communicate strategic goals to project teams and recommend changes to strategic plans.

[1] Information and Technology (I&T) refers to all the information the organization generates, processes and uses to achieve its goals, as well as the technology to support that throughout the organization. On the other hand, Information Technology (IT) refers to the organizational department with main responsibility for technology.

[2] Paragraph 5.1.4, Version 3 of Information Technology Infrastructure Library (ITIL)

[3] COBIT 2019 Framework, Governance And Management Objectives, p. 58

1.7. The Agency has a management committee that deliberates and resolves entity-wide issues, including those I&T related. However, due to numerous issues, it would be beneficial that an I&T Steering Committee that focuses only on I&T related issues, be created to ensure timely resolution and proper monitoring of I&T projects.

1.8. Having an effective I&T Steering Committee could have prevented problems encountered by the Agency in project implementation such as lack of coordination and the issue of funding other systems necessary for the improvement of Agency's services, among others.

b. No feasibility study and business case was developed.

1.9. A feasibility study scopes the problem, outlines possible solutions, and makes the recommendation. A business case is normally derived from the feasibility study, and contains information for the decision-making process on whether it should be undertaken; if so, it becomes the basis for a project.

1.10. COBIT 2019, under the Build, Acquire and Implement (BAI) 01.02, recommends one of its activities to "develop a detailed business case for a program and to involve all key stakeholders to develop and document a complete understanding of the expected outcome, how they will be measured, and the full scope of initiatives required, the risk involved and the impact on all aspects of the organization. It is also recommended to identify and assess alternative courses of action to achieve the desired outcomes."

1.11. Moreover, it was also recommended under BAI 02.02 for management practice to "perform a feasibility study of potential alternative solutions, assess their viability, and select the preferred option." Further, it provides for an activity where alternative solutions are reviewed by all stakeholders and select the most appropriate one based on feasibility criteria, including risk and cost.

1.12. Prudent management of funds dictates that considering the numerous alternatives for the Hospital Information System, there should be a documented analysis if the upgrade to the selected system is more advantageous than system of other service provider.

c. There was no evaluation and performance measurement of I&T investments and projects.

1.13. One of the important aspects of I&T governance is I&T portfolio management. It is the application of systematic management of the investments, projects, and activities. By doing so, the organization may determine what to continue investing in or what to divest from.

1.14. COBIT 2019, under Evaluate, Direct and Monitor (EDM) 02.02, recommends one of its activities to "evaluate the portfolio of investments, services and assets for alignment with the organization's strategic objectives; organization worth, both financial and nonfinancial; risk, both delivery risk, and benefits risk; business process alignment;

effectiveness in terms of usability, availability and responsiveness; and efficiency in terms of cost, redundancy and technical health.[4]" Further, EDM 02.04 recommends for governance practice "to monitor key goals and metrics to determine whether the enterprise receives expected value and benefit from I&T-enabled investments and services."

1.15. The Agency had no defined metrics to measure I&T project effectiveness in terms of timeliness, budget vs. actual spending, cost-benefit analysis, and whether the solutions delivered contributed to the achievement of organizational objectives. Moreover, there was no committee that evaluates the I&T investments, such as those implemented systems outsourced to third party contractors.

1.16. In the survey conducted, it was found that the system's users are generally satisfied. However, most of the respondents also raised issues regarding its speed, stability, navigation, and some find it less user-friendly. Additionally, some of the report requirements of the Accounting Department are still not available. Thus, a regular evaluation must be conducted by Agency to ensure whether the benefits of implementing the system outweigh the issues raised by its users.

d. The Agency lacks a formal information security control framework and I&T related policies.

1.17. An information security framework is a comprehensive plan for the implementation and ongoing operation of the tools and practices necessary to protect the organization's data and systems.[5] Its objective is to reduce the risk as it provides daily and emergency procedures for ensuring security.

1.18. Moreover, policies are important as it allows the management to communicate standard procedures that should be followed within the organization's premises. Information security policies are the foundation of a good security program. With defined security policies, individuals will understand the "who, what, and why" regarding their organization's security program, and organizational risk can be mitigated.[6]

1.19. The Align, Plan and Organize (APO) domain of COBIT, APO01.09 recommends an activity to "create a set of policies to drive IT control expectations on relevant key topics such as quality, security, privacy, internal controls, and usage of I&T assets," among others.

1.20. However, it was gathered from interview that the Agency had no formal information security control framework. As of audit date, only the Agency's Internet Usage Policy was submitted. It was also noted that there were no physical and environmental security policies, acceptable use policy, information security policies, and other I&T related

[4] COBIT 2019 Framework, Governance And Management Objectives, P.37

[5] https://www.solarwindsmsp.com/blog/information-security-framework (last visited on 20 january 2020)

[6] https://linfordco.com/blog/information-security-policies/ (last visited on 20 january 2020)

policies.

e. There were no established guidelines for allocation of resources and capabilities.

1.21. I&T governance specifies the decisions, rights, and accountability framework to encourage desirable behavior in the use of I&T. Also, incorporating the governing structure into the IT budgeting process and allocation of resources and capabilities can ensure that future IT investments are based on performance of past projects, help manage risks, optimize resources, and foster the exploration of possible benefits of technology investments.

1.22. Result of the audit disclosed that currently the Agency has no detailed process and guidelines for allocation of resources and capabilities. This poses risk of being unable to respond to organization's requirements speedily and to manage resources efficiently which may lead to interruption of operation and affect the quality of service.

Recommendations:

1.23. We recommended that Management:

a. Create an I&T steering committee or equivalent that shall address I&T related issues and the management of all the existing and implemented I&T investments. Ensure that the roles and responsibilities of the members are defined and that regular meetings are conducted.

b. Assess if the use of the new system will be advantageous for the Agency in the long run considering its benefits, practicality, and drawback. Moving forward, ensure that a feasibility study and business case was developed and documented before procuring or implementing an I&T project.

c. Conduct an evaluation of the implemented I&T projects to ensure that intended benefits are realized and whether the project objectives are achieved. Develop a dashboard or performance metrics for the assessment.

d. Develop an information security control framework and create I&T related policies. Involve the management in formulating the same and communicate them to intended users. Regularly update the policies to reflect relevant and reliable information.

e. Establish guidelines for the allocation of resources and capabilities and evaluate the current IT operational requirements to assess the sufficiency of resources allocated.

LOGICAL ACCESS MANAGEMENT

2. The logical access controls implemented in the Information System were inadequate thus, exposing the personal data processed therein to unauthorized access and possible misuse.

2.1. Logical Access Controls[7] are policies, procedures, organizational structure and electronic access control designed to restrict unauthorized access to computer software and data files. Section 28, Rule VI, of the Implementing Rules and Regulations (IRR) of the Data Privacy Act (DPA) provides that the personal information controllers and personal information processors shall adopt and establish technical security measures such as safeguards to protect their computer network against unauthorized access through an electronic network, among others.

2.2. Control Objectives for Information and Related Technologies (COBIT) 2019, under Deliver, Service and Support (DSS) 05.04, recommends to, "ensure that all users have information access rights in accordance with business requirements."

2.3. Likewise, Section 9 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27002:2013 also provides implementation guidance on access control, "to limit access to information and information processing facilities."

2.4. Result of the audit disclosed the following control gaps that need to be addressed to ensure that personal data are adequately secured:

a. There was no documented access control policy, guidelines and procedures.

2.5. Item 9.1.1 of the ISO/IEC 27002:2013 provides that, "an access control policy should be established, documented and reviewed based on business and information security requirements" to provide the management the needed support and direction. Some of the important aspects of a logical access policy are user management, password management, and session management, among others.

2.6. Likewise, Section 26 of the IRR of the DPA also requires having data protection policies including policies for access management and system monitoring.

2.7. It is the Management's responsibility to formulate this policy to ensure that the data stored and kept by the Agency is being protected. Moreover, this policy would serve as a guideline that the employees will follow and will eventually help them to establish the necessary logical controls to prevent, detect and correct identified risks. However, it was disclosed that the Agency has no documented access control policy yet.

[7] **ISACA Glossary**

b. Absence of formal process for user access management, provisioning and regular monitoring of user accounts resulted in failure to disable accounts of users already disconnected from the Agency.

2.8. Item 9.2.2 of the ISO/IEC 27002:2013 provides that, "a formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services." This includes adapting access rights of users who have changed roles or jobs and immediately removing or blocking access rights of users who have left the organization.

2.9. For the initial registration, any request for access shall be made through a Service Request Form (SRF) approved by the IT department. The SRF includes the name, designation and section/department of the requestor. This will be the basis during the assignment of accessible modules.

2.10. However, no formal de-registration process was established yet. It was disclosed that IT department has never been informed of the current status of the employees and was not part of the process in obtaining clearance. The clearance process for the termination or transfer of employees must include approval with the management and notification to involved departments, including its IT department to terminate or modify the access right granted to such employees.

2.11. Thus, it poses a challenge for the IT department to determine the appropriateness of the authorization and rights that were originally granted to users who access the application.

2.12. This also adversely affects the account management of the system. Validation revealed that thirty-five (35) user accounts are still active despite being separated from the Agency.

2.13. Further, it was found out that the two (2) accounts below were still accessed even after the effectivity of their termination, which may indicate its inappropriate use. User accounts of terminated employees must be locked or disabled as it could be used in system attack.

2.14. Item 9.2.5 of the ISO/IEC 27002:2013 provides that, "asset owners should review users' access rights at regular intervals". Users' access rights should also be reviewed after any changes, such as promotion, demotion or termination of employment and re-allocated when moving from one role to another within the same organization.

2.15. It was disclosed that no one performs a periodic review of the access rights granted to the existing users. This exposed the Agency to the risk of unauthorized access and disclosure of information. It was also noted that five users have more than one user accounts. In the event that roles have to be changed, the old account should be disabled prior to registration of a new one.

c. **Some group users can access modules that are incompatible with their assigned duties. Moreover, the granting of privileged access rights was not adequately documented and managed.**

2.16. The two of the frequent principles directing the access control policy includes the need-to-know and need-to-use. This means that you are only granted access to the information you need to perform your role.

2.17. Item 9.2.3 of ISO 27002:2013 provides that the allocation of privileged access rights should be restricted and controlled through a formal authorization process in accordance with the relevant access control policy.

2.18. The "administrator" group account has the capability to view, modify or delete a transaction made in the application. It is usual to have more than one administrator account. However, the Management should consider the risk of granting such rights to numerous users. The audit disclosed that all the IT department employees were granted administrative rights.

2.19. Due to numerous users that were given administrator account, additional controls should be implemented. It is recommended under Item 9.2.3 of ISO/IEC 27002:2013 that privileged access rights should be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy. Also, requirements for the expiry of privileged access rights should be defined. An authorization process should also be maintained.

d. **The system has not been configured to enforce restrictions on password syntax and length. Also, proper password aging was not implemented by the Agency.**

2.20. Password is the most common method for users to authenticate themselves when entering computer systems or websites. It acts as the first line of defense against unauthorized access. The more sensitive the data, the more restrictions should be placed to protect these data from unauthorized access.

2.21. An organization's password policy should be flexible enough to accommodate the differing password capabilities provided by various operating systems and applications. It should also consider the nature of the organization to reflect its needs when establishing the requirements for password management.

2.22. Item 9.4.3 of ISO/IEC 27002:2013 recommends enforcing of a choice of quality passwords. However, it was revealed that the system was not configured to set restrictions as to password syntax and length. Only a reminder to use a complex password is prompting.

2.23. Consequently, it was observed that most users are using a less complex password, such as a one to three characters password in logging to their accounts. It was asserted that this is tolerated for the fast delivery of the services to the public.

2.24. Though the immediate medical response is of importance, the Management shall also consider the risk and impact on personal data security. One of the compensating control that Management may implement is to have a password aging policy wherein a user is prompted to change his/her password after a lapse of a certain period of time. Thus, weak passwords that are shared unintentionally to unauthorized users will be no longer usable and could prevent unauthorized access. This is also aligned with Item 9.4.3 (e) of ISO/IEC 27002:2013, which recommends enforcing regular password change as needed.

e. Default/temporary password given to users during account creation were not set as pre-expired to prompt the user to change the password upon initial logon. As a result, some of the users still use default passwords.

2.25. Item 9.2.4 (b) of the ISO/IEC 27002:2013 provides that, "when users are required to maintain their own secret authentication information they should be provided initially with secure temporary secret authentication information, which they are forced to change on first use."

2.26. System simulation disclosed that the user account creator could set an expiry date for the temporary/default password given to users. However, it was disclosed that they were unable to set an expiration resulting in unchanged passwords over time. It was observed that most of the users are still using the default/temporary password.This exposes risk to brute force attacks[8] and unauthorized use of the hospital employee's account by the other person who knows the default password.

f. Account lockout policy and session timeout were not implemented. Moreover, the system allows concurrent login.

2.27. Account lockout is a useful method for slowing down online password-guessing attacks as well as to compensate for weak password policies.[9] However, this was not implemented in the system. System simulation also revealed that an account is not disabled or locked despite numerous unsuccessful login attempts. Thus, making it easier for a malicious attacker to penetrate the system. The absence of account lockout policy is not in conformity with Item 9.4.2 (e) of ISO/IEC 27002:2013 that recommends having controls against brute force log-on attempts.

2.28. Session timeout defines action window time for a user. Thus, this window represents the delay in which an attacker can try to steal and use an existing user session. Good practices for this include the setting of session timeout to the minimal value possible depending on the risk and sensitivity of the data that may be exposed. Infinite session timeout should be avoided. Item 9.4.2 (k) of ISO 27002:2013 recommends, "terminating inactive sessions after a defined period of inactivity, especially in high-risk locations such as publicly accessible offices."

[8] A brute force attack is a trial-and-error method used to obtain information such as a user password. (technopedia)

[9] https://www.ultimatewindowssecurity.com/wiki/page.aspx?spid=accountlockout (last visited 26 january 2020)

2.29. It was disclosed that the system is not capable of implementing a session time-out. Thus, allowing users to be logged in even during prolonged inactivity for several hours. As most users tend to leave their computers with an active session of the system, it increases the risk of unauthorized access of the system. Considering the computers are publicly accessible, it would be a better control to implement session time-out.

2.30. Another instance noted is when a cashier unintentionally used other collecting officer's system user account as it remained logged in after his/her shift. This reflect irresponsibility on the part of the prior user and failure of the system to automatically logout said user. This may result in accountability issues, and erroneous system reports.

2.31. It was also observed that the system allows concurrent logins, thus an account may be used simultaneously with other computers or laptops. The absence of simultaneous login control increases the risk of users sharing their credentials. This creates accountability and non-repudiation issues as it would be difficult to identify the person who actually performed a certain action in the system.

g. Regular monitoring and analysis of the audit logs in the system was not conducted.

2.32. The National Institute of Standards and Technology (NIST) promotes conducting a periodic review of audit logs using a timeline that is appropriate for the security needs of the company[10]. Audit logs are important for timely detection of security incidents, policy violations and, should a response be needed, determination and implementation of necessary actions. Hence, Item 12.4 of ISO 27002:2013 provides that event logs should be produced, kept, and regularly reviewed. Additionally, because of these logs, employees can be held accountable for their inappropriate actions that adversely affected the system.

2.33. Audit disclosed that the IT department only conducts a review of the audit logs as the need arises. Thus, if a security issue is not reported, then the Agency will not be able to detect such because they solely depend on incident reports and only a corrective control rather than a detective control was present. Audit logs should be used to detect security issues then, afterward, implement corrective actions.

Recommendations:

2.34. We recommend that Management:

a. Formulate a comprehensive Access Management policies, guidelines, and procedures. Disseminate the policy to concerned personnel and periodically update to consider the changing needs and security requirements of the Agency.

b. Review granted users' access rights at regular intervals and after any changes such as

[10] https://www.smartsheet.com/audit-trails-and-logs (last visited on 12 February 2020)

promotion, resignation, retirement, movement in the organization, among others. Disable the accounts of terminated employees.

c. Ensure that granting of access rights is based on a need-to-know and/or need-to-use basis. Manage the provision of privileged access rights adequately.

d. Implement sufficient and appropriate Logical Access controls such as restrictions in password syntax and length, password aging policy, account lockout, session timeout policy, among others, based on the result of risk assessment and impact analysis. Consider having controls in the application that determines whether the password being used is weak or strong, based on the parameter set, as part of input validation.

e. Monitor the security logs regularly. Analyze the data gathered to come up with a meaningful report of events captured by the system.

I&T ASSET MANAGEMENT

3. The Agency had not fully complied with the good practices on I&T Asset Management resulting in risk exposure to unaccounted I&T equipment, equipment damage, disruption of operation and accidental data leakage and non-compliance to the DPA of 2012 and its IRR.

3.1. Asset Management is the process responsible for tracking and reporting the value and ownership of financial assets throughout their lifecycle.[11]

3.2. Control Objectives for Information and Related Technologies (COBIT) 2019, under Build Acquire and Implement (BAI09) domain recommends to, “manage I&T assets through their lifecycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose), and they are accounted for and physically protected, and those assets that are critical to support service capability are reliable and available.”

3.3. Likewise, Section 8 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27002:2013 also provides implementation guidance on asset management, “to identify organizational assets and define appropriate protection responsibilities,” ensure that information receives an appropriate level of protection in accordance with its importance to the organization and to prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

[11] ITIL, Service Transition, Glossary

3.4. Evaluation of the Agency’s I&T Asset Management disclosed the following:

a. There was no documented policies for I&T Asset Management and Acceptable Use of I&T Assets.

3.5. The Align, Plan and Organize (APO) domain of COBIT, APO01.09 recommends the creation of IT control policies particularly on internal controls and usage of IT assets to drive control expectations and ensure that staff is fully aware of the IT asset management process. The objective of the policy is to maintain adequate protection of organizational assets and make the best use of available resources.

3.6. Item 8.1.3 of ISO/IEC 27002:2013 recommends having identified, documented and implemented rules for the acceptable use of information and assets associated with information and information processing facilities. Employees and external party users using or having access to the organization’s assets should be made aware of the information security requirements of the organization’s assets associated with information and information processing facilities and resources. They should be responsible for their use of any information.[12]

3.7. While the Agency have guidelines and standard operating procedures relevant to the receipt, inspection, acceptance and recording of all assets, it does not have a documented policy to strictly implement this. Further, it lack provision specifically for IT asset planning, installation, maintenance of software and its licenses, responsibilities of asset owners, among others, relevant to the management of IT asset.

3.8. No policy on the acceptable use of I&T Assets was also developed. Section 17 of the National Privacy Commission (NPC) Circular No. 16-01 provides that each government Agency shall have an up-to-date Acceptable Use Policy (AUP) regarding the use by Agency personnel of information and communications technology. The policy shall be explained to all Agency personnel who shall use such technology in relation to their functions. Each user shall agree to such policy and, for this purpose, sign the appropriate agreement or document, before being allowed access to and used of the technology.

3.9. The absence of an approved written policy and procedure on I&T asset management and its acceptable use exposes the Agency to the risk of unaccounted I&T assets, loss, damage, improper allocation of assets and inadequacy of equipment that are critical to operations.

[12] ISO/IEC 27002:2013, p. 14

b. The I&T Asset Inventory provided by inventory management department was incomplete and not updated. Further, the I&T assets were not categorized in terms of value, criticality, or other categories. Moreover, the data about the lifecycle of the assets were not readily available.

3.10. Item 8.1.1 of ISO/IEC 27002:2013 provides that, "assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained. It further provides that an organization should identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information should include creation, processing, storage, transmission, deletion and destruction. Documentation should be maintained in dedicated or existing inventories as appropriate."

3.11. The IT department, being the responsible for the management, maintenance and protection of these I&T assets, should also have an updated I&T Asset Inventory. However, it was observed that they do not keep one and they simply rely on inventory management department who handles the recording of all assets in the Agency.

3.12. Moreover, the I&T assets were not categorized and the complete asset lifecycle data were not indicated in the inventory. Asset lifecycle data allows an organization to keep track of when a hardware is purchased, how long it has been used and when warranty/support is expiring on the equipment. This assists IT teams to decide if they should replace an old or faulty hardware, uninstall or patch a vulnerable application, or update the firmware on the system.

3.13. It is important for administrators to maintain and have an updated inventory of assets and servers, perform risk assessment and business impact analysis and prioritize equipment that is critical to day-to-day operations. The most critical network equipment must be prioritized first in planning and budgeting and the plan should address the current future requirements for performance, security and scalability.

c. There was no process of information classification and labelling.

3.14. Item 8.2.1 of ISO/IEC 27002:2013 recommends that, "information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification." This is to ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

3.15. Moreover, Item 8.2.2 also recommends that, "an appropriate set of procedures for information labelling be developed and implemented in accordance with the information classification scheme adopted." The procedures should give guidance on where and how labels are attached in consideration of how the information is accessed or the assets are handled depending on the types of media.

3.16. Interviews disclosed that the Agency did not have an information classification and labelling guidelines. Classification and labelling are beneficial as it provides people who deal with information assets with a concise indication of how to handle and protect it. This approach reduces the need for case-by-case risk assessment and custom design of controls.

d. There were no documented policies procedures for media handling. It was observed that files containing personal data were only stored in local hard drives of a leased computer and yet, secure disposal and wiping of data was not practiced.

3.17. To prevent unauthorized disclosure, modification, removal or destruction of information stored on media, Item 8.3.1 of ISO/IEC 27002:2013 recommends that, "procedures should be implemented for the management of removable media in accordance with the classification scheme." Further, Item 8.3.2 provides that formal procedures for the secure disposal of media should be established.

3.18. Moreover, Section 27 (d) of the IRR of DPA provides that those involved in the processing of personal data shall implement policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of personal data.

3.19. It was observed that Agency did not have documented guidelines and procedures in handling and securing electronic media. Further, the standard operating procedure for disposal of unserviceable equipment/property is not comprehensive and did not include data security procedures prior to disposal. Thus, increasing the risk of unauthorized or accidental disclosure of information and data loss due to varying process on media handling across the hospital departments.

3.20. It was also noted that Agency entered into a contract with IT equipment leasing company for the lease of various equipment. Review of the contract revealed that there was no provision on the responsibilities and accountabilities of the parties regarding secure asset disposal activities.

3.21. As observed, these computers were used in the processing of hospital transactions and the hospital personnel also store files in the local hard drives of the leased computers. Considering that, return of leased I&T equipment and/or its disposal should be in a secured manner. However, it was disclosed that after expiration of the lease contract, the computers were handled to the contractor together with the storage devices. There is also an option for the employee to buy them. Some asserted that they delete the files prior to handing over them to the contractor. However, data deletion is not sufficient as it could still be recovered.

3.22. The implementation guidance under Item 8.3.2 (a), (e) of ISO/IEC 27002:2013 provides that, "media containing confidential information should be stored and disposed of securely, such as by incineration or shredding, or erasure of data for use by another application within the organization and disposal of sensitive items should be logged in order to maintain an audit trail."

3.23. Proper disposal of Personal Information and Sensitive Personal data is important as violation could result inpenalty of imprisonment and fine as stated in Section 54 (a)(b), Rule XIII, IRR of RA 10173, also known as the Data Privacy Act of 2012.

Recommendations:

3.24. We recommended that Management:

a. Formulate and implement policies and procedures on I&T Asset Management that shall include acceptable use of I&T policies, guidelines on information classification and labelling, asset acquisition, installation, usage, media handling, disposals and recycling, inventory management and asset categorization, among others.

b. Ensure that I&T Asset Inventory is updated and that IT department have a copy of current inventory that contains all relevant information about the asset such as type of asset, owner, classification, location, license information, categorization, value and lifecycle data.

c. Develop guidelines on information classification and labeling based on the result of the Privacy Impact Assessment.

d. Comply with the rules stated in DPA of 2012 and its IRR on secure media handling and asset disposal especially during the return of leased computers to the lessor.

PHYSICAL AND ENVIRONMENTAL SECURITY

4. The Agency's asset are not adequately secured due to insufficient physical and environmental controls that resulted in risk exposure to unauthorized access, equipment theft, accidental or malicious damage, data loss and operational disruption.

4.1. Physical security describes measures that are designed to deny access to unauthorized personnel from physically assessing critical IT assets and stored information; and guidance on how to design structures to resist potentially hostile acts.[13] It is the protection of personnel, hardware, software, networks, and data from physical actions and events that could cause serious loss or damage to an Agency.

4.2. Control Objectives for Information and Related Technologies (COBIT) 2019 recommends that assets should be physically protected. Likewise, Section 11 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27002:2013 also provides implementation guidance and recognizes the need to have controls relevant to physical and environmental security to prevent unauthorized physical access, damage and interference to the organization's premises and information.

[13] WGITA- IDI Handbook On It Audit For Supreme Audit Institutions, p. 52

4.3. While there are physical and environmental controls implemented in Agency such as installation of Closed-Circuit Television (CCTV) in some areas, presence of security personnel, installation of fire suppression systems, monitoring of temperature in the data center/server room, among others, the audit also noted some deficiencies that need to be addressed and improved as follows:

a. There were no policies, guidelines, and procedures relevant to physical security measures.

4.4. The IRR of the DPA of 2012 under Rule VI, Physical Security Measures, provides that policies and procedures be implemented to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media.

4.5. Policies are important as it allows the management to communicate the standard procedures that should be followed within the organization's premises. Absence of it exposes the organization to the risks of inconsistent security practices across the organization that could result in unauthorized access to information assets and non-compliance with the relevant laws, rules and regulations.

b. The physical arrangement of some computers makes them susceptible to unauthorized access, accidental viewing of patient's personal data and theft.

4.6. Section 27 of the IRR of the Data Privacy Act of 2012 provides that the design of office space and work stations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public.

4.7. Further, Section 2.2, Rule 5 of the Health Privacy Code provides that anti-glare filters on computer monitors shall be installed as it provides additional security by preventing, or at least minimizing, unauthorized and/or accidental viewing of the computer screen.

4.8. During the walkthrough, it was observed that one of the computers with installed and opened system is located in an open area of the Emergency Room, making it easily accessible to the public and susceptible to shoulder surfing attack[14]. This also increases the risk of equipment theft, unauthorized access and disclosure of confidential information. Further, we have also noted that some computers were positioned where the screen is viewable to the public which increases the risk of accidental viewing of personal data.

[14] Shoulder surfing refers to a direct observation, such as looking over a person's shoulder, to obtain valuable information.

c. There were no sufficient controls to ensure fire safety and property protection in Agency.

4.9. Interviews disclosed that no inspection was done to check the water sprinklers and smoke detectors. Personnel from Engineering and Facilities Management asserted that even though they have not inspected the water suppression line, they maintain the availability of the water supply source. They also revealed that they have previously requested the rehabilitation of sprinklers and smoke detectors. However, it was not granted yet.

4.10. Without the conduct of routine inspection or maintenance, there is no assurance that these equipment will work accordingly during a fire incident which may result in more serious damage and put the life of the persons in danger.

4.11. Section 10.2.6.7 of the IRR of RA No. 9514 also provides that all buildings, structures, and facilities shall be installed with portable fire extinguishers that are designed, installed and maintained. Portable fire extinguishers other than wheeled types shall be securely installed on the hanger or in the bracket supplied or placed in cabinets or wall recesses.

4.12. It is worthy to mention that the Agency has complied with the installation of fire extinguishers. Engineering Office also maintains an inventory of functioning portable fire extinguishers and its location. However, it was also observed that most of them are placed on the floor, not in a secured hanger or bracket, which put it at risk of being knocked over, damaged and inoperable. There is also no evidence that they conduct regular inspections due to the absence of notes in the inspection record of the device tag.

4.13. Moreover, it was also observed that the portable fire extinguisher placed near the server room is a dry chemical type, which is considered inappropriate. Suppression agents such as those containing dry chemical agents or corrosive wet agents in fixed systems should not be used in any area containing I&T equipment.[15] Dry chemical-based fire extinguisher leaves a residue behind. This residue will corrode the components of servers and electronics and could essentially be more destructive.

d. The storage room for medical records can be further improved to ensure records are adequately protected.

4.14. Interview and physical inspection disclosed that improvements were already made in the medical records' storage room. It was also mentioned that the piling of files were more organized than before.

4.15. However, it can still be further improved. As observed, there were damaged and breakable windows which can be an entry point of intruders and could also cause rain penetration or water leaks through the window openings. Also, the comfort room therein

[15] Https://www.isaca.org/Journal/archives/2014/Volume-4/Pages/Fire-Protection-of-Computer-Rooms-Legal-Obligations-and-Best-Practices.aspx#11

is not strategically located.

e. **The video recordings in the CCTV are not archived and are kept only for seven days.**

4.16. Installation of CCTV and monitoring is useful to protect the Agency's property and data, prevent equipment theft, and quickly identify the perpetrator. It is commendable that there are 52 functional cameras installed and managed across the Agency.

4.17. However, it was observed that the recordings were deleted after seven days. Video recordings are essential in further investigation and verification of the identity of the malicious attacker and can be used as evidence for the incident.

4.18. Moreover, during the physical inspection, it was noted that some CCTVs (e.g. in Billing Section) were not showing surveillance feed. The security Agency who is responsible for the overall operations of the CCTVs explained that those cameras are intermittently working and were under observation.

Recommendations:

4.19. We recommended that Management:

a. Formulate formal policy, guidelines and procedures that define the controls that will ensure public safety and protect the IT infrastructure and facilities.

b. Conduct risk assessment and business impact analysis by evaluating the existing physical and environmental controls, the risk associated with the above-noted deficiencies, and the potential effects on the operation to address the gaps.

c. Implement sufficient and appropriate controls to address the deficiencies observed and protect the public, IT equipment, and devices from physical and environmental threats.

d. Monitor regularly and maintain the controls implemented to ensure their effectiveness and functionality.

BUSINESS CONTINUITY MANAGEMENT

5. Ineffective implementation of Business Continuity Management practices exposed the Agency to the risk of operational disruption, data loss, non-recovery of IT systems and services, and even risks to human life upon the occurrence of incidents or disasters.

5.1. Business Continuity Management (BCM) is essential to maintain the availability of the information system as it integrates the disciplines of Emergency Response, Incident/Crisis Management, Disaster Recovery, and Business Continuity. This helps an organization to be prepared in incidents, to strategize on the continuity of operations and get back on its optimum performance when a disaster arises by quickly restoring its business-critical functions affected by the unexpected interruption.

5.2. Having an effective BCM in a healthcare facility is paramount as the effects of a disaster in such an environment can be far-reaching. With patient lives on the line, the stakes are higher in healthcare than in other industries. As the hospital is becoming dependent on information systems, IT failures can have a huge impact as they put inconvenience to patients and health services providers.

5.3. COBIT 2019 framework and ISO 22301:2012 recommend to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.

5.4. In the compliance assessment conducted relevant to BCM, the following was noted:

a. The Agency Emergency Preparedness, Response, and Recovery Plan has not been updated since 2013. It was also not reviewed and tested regularly.

5.5. Result of audit disclosed that the Plan was not regularly reviewed and updated to adapt the changes brought about by new information, technology, infrastructure movement, and lessons learned during emergencies and disasters. Testing of the plan for its functionality and adaptability to the current situation was also not conducted. According to one of the members of the Emergency Management Bureau, it has not been tested as they are currently in the process of reviewing and updating.

5.6. It was also noted that IT operations were not taken into consideration during their risk assessment. Due to the advancement of technology, and organizational changes over the past few years, the contents of the Plan may be no longer applicable at present which could jeopardize the effectiveness of the Agency's Business Continuity Management.

b. There were no documented procedures for the management of data backup and recovery processes.

5.7. The IT department in their Quality Management System (QMS) documentation requires IT staff in-charge to perform backup weekly. However, it was noted that no data backup plan procedures were written for the proper implementation of these guidelines to ensure the effective execution of the backup and recovery process.

5.8. Interviews with the IT department personnel disclosed that a full database backup is being performed on a daily basis. The backup data are stored in Network Attached Storage (NAS) and have a data retention of 6 months but it was noted that the old backup files are not being archived.

5.9. Lack of defined procedures may lead to inconsistent and varying approaches in performing backup and security measures in handling and storage.

Recommendations:

5.10. We recommended that Management:

a. Develop a Disaster Risk Reduction Managemet plan following the provisions of the existing rules and regulations and properly implement it to ensure resilient health systems. Ensure that IT operations and information security were considered in business impact analysis and risk assessment. Review, test and disseminate the plan regularly.

b. Formulate backup and recovery plans and procedures according to the Agency's requirements.

INCIDENT AND PROBLEM MANAGEMENT

6. The overall incident and problem management process needs to be improved to ensure outstanding service delivery.

6.1. Incident Management is the systems and practices used to determine whether incidents or errors are recorded, analyzed and resolved on time. While, Problem Management aims to resolve issues through investigation and in-depth analysis of a major or recurring incident to identify the root cause.

6.2. The primary goal of the Incident Management process is to restore normal service operation[16] as quickly as possible and minimize the adverse impact on operations, thus ensuring that the best possible levels of service quality and availability are maintained.

6.3. It is noteworthy to mention that the IT department conducts regular preventive maintenance on IT equipment including servers, network devices, and computers, to minimize the occurrence of incidents. However, we have also noted the following deficiencies that need to be addressed to manage incidents effectively and to minimize risk to the availability of systems, application, and data:

a. There were no documented policies and procedures for Incident and Problem Management.

6.4. While IT department was able to formulate guidelines to support the delivery of IT services, there is no documented policies and detailed procedures to ensure the effectiveness and adequacy of their incident and problem management.

6.5. Lack of policies will not guarantee that standardized methods and procedures for efficient and prompt response, analysis, documentation, management and reporting of incidents or problems. Moreover, recurring incidents could not be prevented and the

[16] **Normal Service Operation is service operation within limits prescribed under the Service Level Agreement.**

impact of incidents could not be minimized due to lack of the Problem Management process.

b. The IT department did not maintain an electronic log of service requests, incidents, and problems.

6.6. COBIT 2019, under Delivery, Service and Support (DSS) 02.02, recommends logging all service requests and incidents, recording all relevant information, so they can be handled effectively, and a full historical record can be maintained.

6.7. Item 4.2.5.2 of ITIL V3, Service Operation also provides that, "all incidents must be fully logged and date/time stamped. All relevant information relating to the nature of the incident must be logged so that a full historical record is maintained and so that if the incident has to be referred to other support group(s), they will have all relevant information to hand to assist them."

6.8. It was observed that service requests and incident reports were received through telephone calls or emails. While the IT department file and keep the hard copies of requests, they did not maintain a log or a summary of incidents and its important details such as reference number, categorization, urgency, impact, prioritization, date/time recorded, name of the person recording the incidents, method of notification, description of systems, incident status, activities undertaken to resolve the incident, resolution and closure date and time, among others.

6.9. The absence of this log made it difficult to conduct incident trend analysis, track the progress and monitor the resolution of each incident.

c. The service requests and incident reports were not properly categorized. Moreover, the prioritization of service requests were not defined and documented.

6.10. COBIT 2019 Delivery, Service and Support (DSS) 02.01 and DSS02.02 emphasize the need to classify incidents and service requests. According to Item 4.2.5.3 of ITIL v3, "part of the initial logging must be to allocate suitable incident and request categorization so that the exact type of incident/request is recorded." This will be important later when looking at incident/request types/frequencies to establish trends for use in various IT Service Management (ITSM) activities.

6.11. All Service Requests received by the IT support must be categorized because not all of them are incidents. Based on good practices, Incident and Service request handling are two different processes and, therefore, should have different categorization and prioritization for a more effective and accurate analysis. According to ITIL, Service Requests are a way of meeting the user's needs and do not represent a disruption to agreed service while incidents are unplanned interruption or reduction in the quality of an IT service.

6.12. However, observation of the IT department's process disclosed that all incidents are categorized as service requests. Also, it was not broken down and identified as to their categories (e.g., hardware, software, application, server, etc.).

6.13. Item 4.2.5.4 of ITIL v3 also provides that, "another important aspect of logging every incident is to agree and allocate an appropriate prioritization code as this will determine how the incident is handled both by support tools and staff. Prioritization can normally be determined by taking into account both the urgency of the incident and the level of impact it is causing."

6.14. Though, it was disclosed that requests from higher officials are expected to be prioritized by IT department personnel regardless of the complexity. This practice may be inappropriate. Without a defined and documented prioritization basis and procedures, it is possible that the urgency and impact was not considered. Also, the criteria will tend to vary across the support staff. Thus, it may jeopardize the resolution of higher risk requests/incidents.

d. There was no separate response plan for "Major" incidents.

6.15. According to COBIT 2019 DSS02.01 and Item 4.2.5.6 of ITIL, the management should define separate incident escalation rules and procedures with shorter timescales and greater urgency for major incidents.

6.16. While a Response Call Tree Notification that contains the contact details of IT department personnel responsible for the notification, initial response, and the full response was created for emergency cases, no detailed procedures were formulated in response to major incidents or emergency cases.

6.17. The absence of such documented procedures increases the risk of untimely and inappropriate resolution of major incidents that may adversely affect the operations.

e. The target set by IT department was not communicated to its stakeholders, and no Operational Level Agreement (OLA) was defined. Moreover, the priority and impact of the incident/service request were not considered in the target formulation.

6.18. COBIT 2019, APO09.03 recommends to define and prepare service agreements based on options in the service catalogues including operational agreements.

6.19. OLA is internal agreement that a service provider (IT department) defines for internal users to meet Service Level Agreements (SLAs). OLAs can also contain one or more objectives or service targets. The OLAs would be used to track internal service commitments such as response time for incidents or problems assigned to IT groups and the availability of servers supporting various applications.[17]

[17] **https://www.bmc.com/blogs/ola-operational-level-agreement/ (last visited on 17 January 2020)**

6.20. Due to the absence of OLA, their current targets were not communicated and agreed upon by the stakeholders. There was also no assurance that the target set is appropriate for the operations and is aligned to the required level of services of Agency.

6.21. The objectives and measurable targets of IT department were set out in their Quality Objectives and Plan (QOP). As stated therein, their target is to provide technical assistance to computer users within 24 hours from the incident/request notification. However, no separate target was set for incident/request that is critical and should be prioritized. The target resolution time for critical incidents should be less than 24 hours as it could result in loss of service and client dissatisfaction.

f. Some technical concerns were not timely resolved as it arises beyond IT department working hours.

6.22. Result of the audit disclosed that based on their risk assessment, IT department implements three work shifts to support the daily hospital operations from 7 AM to 11 PM. It was said that hospital operations during wee hours were considered low risk due to few users and only a small number of issues were being reported during that time of the day which doesn't have significant impact in the overall operations of the hospital.

6.23. However, based on the feedback from the survey conducted, some departments wish to have IT support during these hours, particularly the Laboratory Department which have peak operations during early in the morning and the Emergency Department which suggested that IT support be available 24/7 in order to fully support their operations including other departments with the same work schedule. This is to resolve the issues encountered within the required timeframe to minimize any adverse effects on operations.

g. The Incident Management Process was not monitored and reported to the management.

6.24. Item 4.2.8 of ITIL v3, Service Operations, provides that the metrics that should be monitored and reported upon to judge the efficiency and effectiveness of Incident Management Process, and its operations, will include, among others:

- Total numbers of Incidents (as a control measure)
- Breakdown of incidents at each stage (e.g., logged, work in progress, closed, etc.)
- Number and percentage of major incidents
- Mean elapsed time to achieve incident resolution or circumvention, broken down by impact code
- Percentage of incidents handled within agreed response time (incident response-time targets may be specified in SLAs, for example, by impact and urgency codes)

- Number of incidents reopened and as a percentage of the total
- Number and percentage of incidents incorrectly assigned
- Number and percentage of incidents incorrectly categorized
- Breakdown of incidents by time of day, to help pinpoint peaks and ensure matching of resources

6.25. However, it was observed that these metrics were not monitored. It was disclosed that IT Service levels and performance were not discussed during Management Committee meetings and was not evaluated whether it was performing based on the requirements and objectives of the hospital. Thus, there is a possibility that incident management problems and concerns are not addressed.

Recommendations:

6.26. We recommended that Management

a. Formulate incident management policies and procedures that are aligned with the objectives of the hospital. Ensure that these are well-documented and reviewed regularly. Incorporate important process activities such as incident logging, prioritization, and categorization in the policies.

b. Ensure that service requests and incidents are logged with the pertinent details necessary for monitoring and trend analysis.

c. Review the current process and improve it for efficient tracking, categorization, and prioritization.

d. Develop separate procedures for handling major incidents that shall be aligned with the objectives of the Agency. Define and agree on what constitutes a major incident based on risk assessment.

e. Develop an OLA and document the IT services offered by IT department, service level targets, and the responsibilities of IT department and Agency’s stakeholders. Ensure that targets are aligned with the Agency’s service requirements. Monitor the incident management process and report the achievement of targets defined in the OLA.

f. Re-assess through risk and impact analysis the need for IT support outside the current IT department’s working hours. Coordinate to the concerned departments formulating a specific OLA for them.

g. Regularly monitor the efficiency and effectivity of incident and management process.

APPLICATION CONTROLS AND ITS UTILIZATION

7. Inadequate application controls, system limitation and numerous manual processes in Cash Operation Section resulted in unreconciled difference between manual and system generated reports.

7.1. Application controls are controls over input, processing and output functions. They include methods for ensuring that (a) only complete, accurate and valid data are entered and updated in a computer system; (b) processing accomplishes the correct task; (c) processing meets expectations and (d) data are maintained. These application controls are designed to ensure correct processing of transactions to prevent error, loss, unauthorized modification or misuse of the information in applications.[18]

7.2. COBIT 2019, under Deliver Service and Support (DSS) 06.02, recommends to verify that transactions are accurate, complete and valid; handle output in an authorized manner; and verify the accuracy and completeness of the output, among others.

7.3. As observed, the use of system helped to simplify other processes in the hospital such as posting of charges and discounts, rendering of requisitions and computation of billed amount. However, control gaps were also noted as discussed in the succeeding paragraphs.

Cash Operation Section (COS) showed that several processes required human intervention that resulted in inefficiency and increased risk of human error.

7.4. Manual processes carry a higher risk of human error, and the following were observed in Agency's COS:

- Cash Collecting Officers (CCOs) had to manually prepare their daily reports using MS Excel because the system generated reports do not comply with the regulatory requirements;
- CCOs had to manually identify and tick the transactions to be paid in preparing the ORs; and
- There are several editable field/s in the "Cash Receipt" component making it prone to input errors.

[18] CISA Review Manual, 2016 Edition

Reconciliation and analysis of both system generated and manually prepared[19] Report of Collections from April to September 2019 revealed discrepancies.

7.5. The following table shows the discepancy resulting from the reconciliation made between the Manual and System generated reports:

Table 1: Discrepancies between manual and system generated reports

MONTH	MANUAL	SYSTEM	DIFFERENCE
APRIL	43,014,466.88	24,249,382.20	18,765,084.68
MAY	39,368,279.02	28,347,237.30	11,021,041.72
JUNE	47,135,253.32	26,777,632.38	20,357,620.94
JULY	37,431,685.84	30,557,918.92	6,873,766.92
AUGUST	34,000,942.76	28,507,584.19	5,493,358.57
SEPTEMBER	30,440,868.62	29,119,701.15	1,321,167.47
TOTAL	**231,391,496.44**	**167,559,456.14**	**63,832,040.30**

7.6. This shows that system generated report of collections could not be relied upon since not all collections were recorded in the system. These discrepancies may result in confusion that eventually lead to misstatement of revenue reported in the financial statements.

7.7. The cause of discrepancies noted were as follows:

- ORs were recorded in the manually prepared Report of Collections but not reflected in the system and vice versa
- Different OR Amount/s recorded in the manually prepared Report of Collections from the system generated reports
- Inconsistent OR dates between the manual and system generated reports
- Erroneous OR numbers were found in the system's database. Also, disparities were noted between the OR numbers recorded between the manually prepared and system generated reports.
- The Cash Collecting Officer reflected in the OR is not the one who received the payment.
- Cancelled ORs in the manual report were not tagged as cancelled in the system.
- A cancelled OR in the system generated report could not be found in the "Cash Receipt" module.
- The discount amount reflected in the OR was inaccurate.
- Manual collection reports for some dates were not submitted.

[19] Manually prepared reports are those prepared using ms excel.

Recommendations:

7.8. We recommended that Management:

a. Customize the format of system generated collection reports to comply with regulatory requirements so that the CCOs can utilize the report manager.

b. Ensure that all collections are recorded in the system especially those inter-agencies collection for medical assistance. Reconcile the discrepancies between manual and system generated reports.

c. Improve the "Cash Receipt" component for the system to be able to generate "ready to print" ORs to reduce input errors and unnecessary modifications. The following improvements can be made:

   i. Make the Receipt Date a non-editable field and ensure the default value is set to today's date.
   ii. Ensure that accurate OR nos. were recorded in the system. Avoid manually entering the OR no.
   iii. Impose session timeout and ensure that the cash collecting officer whose name is appearing in the OR is the one who received the payment
   iv. Ensure cancelled ORs were timely tagged as cancelled in the system.
   v. Investigate instances on unsearchable cancelled ORs and fix the issue.
   vi. Ensure accuracy of the discount amount appearing in the ORs.

8. Some components of the system did not conform to user's needs and requirements. System limitations and deficiencies resulted in inefficiencies and increased risk of error.

8.1. Considering the huge influx of admitted patients on a day-to-day basis, a suitable HIS is needed to be efficient and more productive. However, system simulation and interviews disclosed the following issues on the use of the system:

- Some reports needed are either unavailable in the system or system's report format did not conform to user's requirements, rules and regulations.
- Issues on the system's navigation and features were observed.
- Additional Room Charges for patient tagged as May-Go-Home (MGH) can only be done on a per-day basis that resulted in inefficiencies in Admitting Unit
- Cut-off payment when a "pay patient" becomes a "charity patient" and vice versa is not available in the system.
- Existence of option to re-open the patient's account led to inappropriate/excessive room charges.
- Lack of input control in the system resulted in processing error
- The Pharmacy Unit still has to carry out a manual inventory and maintenance of stock cards due to nonutilization of inventory management department. In addition, there are variances between the number of issued medicines provided in the systems and issuances based on the manual report

Recommendations:

8.2. We recommended that Management:

a. Customize the reports based on user’s requirements and current rules and regulations. Evaluate the accuracy and completeness of reports.

b. Conduct a meeting with representatives of each Department/Unitto gather information about the system’s utilization and proposed enhancements to meet their needs and address the issues/deficiencies observed.

c. Analyze and prioritize the implementation of the enhancement based on its impact on operations, level of difficulty and cost, among others. Most significantly, conduct system testing to ensure the accuracy and consistency of the data after the upgrade has been completed.

d. Ensure the reduction of tedious manual processes and those that require unnecessary human intervention such as in room charging and changing from pay to charity patient.

e. Re-configure the system so as not to allow input of special character to minimize the errors in the transmission of e-Claims.