

SOCIAL EQUALITY and PROTECTION AGENCY

INFORMATION SYSTEM AUDIT REPORT

TABLE OF CONTENTS

DEVELOPMENT AND ACQUISITION.....	1
CONTINUITY PLANNING	6
INFORMATION SECURITY	10
Physical and Environmental Security	10
Workstation Security.....	12
Security Awareness	15
APPLICATION CONTROLS	15
Application Controls – LOS Input Controls	17
Application Controls – LOS Processing and Output Controls.....	24
Application Security – Password, Session, and Audit Management	30
Application Security – User Access Management.....	38

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.

DEVELOPMENT AND ACQUISITION

1. The Agency has partially complied with the best practices on Systems Development, Project Management and Change Management of the LOS system due to the absence of: (a) project sponsor or executive level representative in the steering committee; (b) quality assurance testing; and (c) program change management. These exposed them to the risks of project failure, complications in system maintenance and implementation which may lead to wastage of government fund.

1.1 Systems Development Life Cycle is a framework defining tasks performed at each phase in the software development process. It is a detailed process requiring careful planning, requirements definition, program development, testing/execution, implementation and feedback on post-implementation. When not managed properly, the downside is scope creep, blown budgets, undefined user requirements, inefficient program specifications incorrect program development leading to stressed out programmer/developers.¹

1.2 Maintenance of an IT system during its life cycle includes changes and updates to the system as a result of new policies, laws or regulations, fixing of system errors/bugs, and enhancements made as a result of new interfaces.²

1.3 LOS system aims to integrate the operation function related to workers. It is designed to generate reliable, accurate and accessible information needed in formulating policies and promote transparency. Assessment of the Control Evaluation Questionnaires, interviews, observation and verification of documents disclosed the following:

a. The absence of project sponsor and executive level representative from business units in the Steering Committee exposed the Agency to the risk of project implementation failure and this may have been the reason for the lack of support and commitment from the other intended users.

1.4 COBIT5 APO01.01³ *Define the organizational structure.* - Establish an internal and extended organizational structure that reflects business needs and IT priorities. Put in place the required management structures (e.g., committees) that enable management decision making to take place in the most effective and efficient manner by:

- Establishing an IT steering committee (or equivalent) composed of executive, business and IT management to determine prioritization of IT-enabled investment programs in line with the enterprise's business

¹ <https://www.techopedia.com/definition/24776/system-development-lifecycle-sdlc>

² INTOSAI Working Group on IT Audit (WGITA) and the INTOSAI Development Initiative (IDI) updated Handbook on IT Audit

³ Page 52, Chapter 5, COBIT5: Enabling Processes – Align, Plan and Organise

- strategy and priorities; track status of projects and resolve resource conflicts; and monitor service levels and service improvements;
 - Establishing and maintaining optimal coordination, communication and liaison structure between the business and IT functions within the enterprise and with entities outside the enterprise; and
 - Regularly verify the adequacy and effectiveness of the organizational structure.
- 1.5 A project Steering Committee is an advisory committee usually made up of high-level stakeholders and/or experts who provide guidance on key issues such as company policy and objectives, budgetary control, marketing strategy, resource allocation, and decisions involving large expenditures.⁴
- 1.6 The absence of a project sponsor or an executive from the concerned business units/agencies in the steering committee who will address issue which has major implications for the project, provide with guidance on business issues and reconcile differences in opinion exposes the Agency to the risk that project issues are not properly addressed and monitored at the top level which resulted in uncommitted and poor performance of personnel involved.

b. Absence of documentation on the user requirements or the lack thereof.

- 1.7 COBIT 5 BAI02.01 *Define and maintain business functional and technical requirements*. Based on the business case, identify, prioritize, specify and agree on business information, functional, technical and control requirements covering the scope/understanding of all initiatives required to achieve the expected outcomes of the proposed IT-enabled business solution.
- 1.8 COBIT 5 BAI02.04 - *Obtain approval of requirements and solutions*. Coordinate feedback from affected stakeholders and, at predetermined key stages, obtain business sponsor or product owner approval and sign-off on functional and technical requirements, feasibility studies, risk analyses, and recommended solutions.
- 1.9 Activities such as workshops and interviews with the concerned department were conducted by the contractor during the requirements analysis phase. However, documentation and approval that can be used as a basis for development and proof of what the users expect from the new system are nonexistent. The properly documented user requirement is very important in determining how the current system works and what the users want from the new system.

⁴ <http://www.businessdictionary.com/definition/steering-committee.html>

c. Non-conduct of Quality Assurance Testing.

- 1.10 Assessment of the CEQ and interviews revealed that there was no QA team who verifies if the application works as designed and if it is compliant with the technical specification, deliverables, and standards of programming. This exposes the agency to the risk of having poor quality software, late detection of errors which can be costly and more difficult to correct, generate unreliable reports and software not aligned and does not reflect current business processes.
- 1.11 Quality assurance is a critical part of well-managed system development projects. Comprehensive quality assurance, risk management, and testing standards provide the best means to manage project risks and ensure software includes expected functionality, security, and operability.
- 1.12 Aside from the User Acceptance testing (UAT) which focuses on the functionality of the application, part of the final acceptance testing is the Quality Assurance Testing (QAT) which focuses on the documented program specifications and the technology employed. It verifies that the application works as documented by testing the technology and its logical design. It also ensures that the application meets the documented specifications and deliverables and that the software is aligned with business processes and objectives.

d. Non-Acceptance of LOS system by some key stakeholder.

- 1.13 Verification of documents, specifically the *Certification from Data Users* revealed that key stakeholders were not part of the data users who signed the certification confirming that the required deliverables were completely delivered by the consultant and were fully functional.
- 1.14 Key stakeholders and intended users should be involved in the project from the data gathering to system testing, most especially on user acceptance of LOS. It is important that all stakeholders accept the system to ensure that the system follows the requirements as defined in the project documentation and ensure that these users/stakeholders will not refuse to utilize the system.
- 1.15 A properly documented user requirements, the performance of quality assurance and stakeholder's acceptance of the developed system will help ensure that IT services are aligned with business process, delivered solution utilize by stakeholders, the information needed for decision making are available and the system gives benefit to the organization.

e. Absence of approved change management policies and procedures.

- 1.16 A change management process is a formal set of procedures and steps that are set in place to manage all changes, updates, or modifications to hardware and software (systems) across an organization. It should be formalized through a management-approved policy.

1.17 *Sub-clause 14.2.2 of the ISO/IEC 27002:2013* provides that changes to systems within the development lifecycle should be controlled by the use of formal change control procedures which should be documented and enforced to ensure the integrity of the system, applications, and products, from the early design stages through all subsequent maintenance efforts.

1.18 The audit team requested a copy of all the policies and procedures issued by the department including the Change Management Policy but none was provided. The same was confirmed in an interview that there was no policy issued regarding the matter. This increases the risk that changes applied to LOS are unauthorized, undocumented, could lead to disruption of operations or potential security breaches.

f. Change requests are not properly documented and approved.

1.19 *Sub-clause 14.2.2 (b), (f), (g) and (j) of the ISO/IEC 27002:2013* provides that change control procedures should include:

- Ensuring changes are submitted by authorized users;
- Obtaining formal approval for detailed proposals before work commences;
- Ensuring authorized users accept changes prior to implementation;
- Maintaining an audit trail of all change requests.

1.20 It was revealed in an interview that requests for change are received through email, skype or during meetings with the concern departments. There are no change request form, documentation and formal approval from the system owner to proceed with the change request. To monitor changes and additional modules implemented in LOS, a list of updates and additional modules containing the description, date, and details were maintained by the development team. However, the date of request, requestor, justification or reason for the change request were not logged.

1.21 Moreover, additional modules were implemented without the proper change request documentation and approval. Inadequate documentation and approval on change request may result in the introduction of erroneous processes, unauthorized business processes, and inefficiencies.

g. Lack of segregation of duties.

1.22 Changes in the system are tested by the same programmer who performs the change. Good practice dictates that testing and quality assurance should be performed and accepted by actual user, requestor or tester before implementing it in the production. Due to this practice, implemented solution which might help the requestor may affect other users or may not be working as expected. It could also lead to inconsistent processing result and system failure resulting in a lack of system availability.

h. Absence of version control.

- 1.23 *Sub-clause 14.2.2 (i) of the ISO/IEC 27002:2013* provides that change control procedures should include maintaining version control for all software updates.
- 1.24 LOS has no version or revision control system that manages source code; track all the changes made to the source; provide information such as who made the changes, when and why it was implemented; and references to problems detected and fixed. Interview conducted disclosed that changes were applied to the latest source code and the updated version were loaded to the production afterward.
- 1.25 This lack of control in implementing change increased the risk that a new/modified application program could be deployed in the production environment without the knowledge of IT management and overwriting of code. Implementing change management is extremely important in ensuring quality delivery of IT services as this will reduce the risk associated with completing changes and reduce the impact of changes on the IT and business organizations.
- 1.26 The risks that may stem from a lack of documentation were heightened by the fact that the computer programmer/developer holds a job order position or considered as temporary personnel. In the event that these personnel leave the agency, maintenance or enhancement of the system may be difficult. Also, the above observations if not addressed may lead to project failure or wastage of government fund.

Recommendations:

- 1.27 We recommended that Management:
- a. For future projects, Management must ensure that project sponsor and management level representative from the business owner or unit are represented in the project steering committee;
 - b. Ensure proper systems documentation and approval of project documents such as user requirement definitions, functional procedures/processes, conduct of systems quality assurance and user acceptance testing before system implementation. Also, consider creating a Quality Assurance team who will ensure that user requirements are met, and adequate validation controls are embedded in the system. Moreover, we recommended that key stakeholders is represented during user requirements definition, system testing, and acceptance; and
 - c. Formulate Program Change Management policies and procedure that will be used to ensure changes in both hardware and software are controlled, approved and properly executed. Moreover, implement a

version control to systematically retain chronological copies of revised programs and program documentation.

CONTINUITY PLANNING

2. The Agency inadequate practices on the preparation for fortuitous/disruptive events exposed them to the risks of operational interruptions and other critical service discontinuance brought about by data unavailability and inability to provide IT service operational requirements for key business functions and processes.

2.1 According to SANS,⁵ Business Continuity refers to the activities required to keep your organization running during a period of displacement or interruption of normal operation. Whereas, Disaster Recovery is the process of rebuilding the operation or infrastructure after the disaster has passed.

2.2 To determine the agency's preparedness in the event of disaster/disruptions, the audit team evaluated its business continuity strategy and noted the following:

A. Absence of Business Continuity policy, plan or procedures exposes the agency to risk of inability to respond to disruptive events and continue its operations after the occurrence of a disaster or disruptive incident.

2.3 Business continuity plan is a set of procedures and instructions to guide an organization during and after a disruption event, to speed up immediate response, recovery, and resumption of minimum operational conditions, and restoration of normal operations.⁶

2.4 This plan is a key element to ensure business continuity, and a number of elements should be covered, like roles, responsibilities, and authorities to be performed during and after an incident, a process to activate the incident and response structure, activities to manage immediate impacts, the communication flow with interested parties, and the continuity and recovery activities.

2.5 *Sub-clause 5.3 of ISO 22301:2012* on "Business Continuity Management" provides that top management shall establish a business continuity policy that: (a) is appropriate to the purpose of the organization; (b) provides framework for setting business continuity objectives; and (c) includes a commitment to continual improvement of the Business Continuity Management System. The policy shall be available as documented information, be communicated within the organization, be available to interested parties, as appropriate, be reviewed for continuity suitability at defined intervals and when significant changes occur.

⁵ Fried, Stephen. "Information Security: The Big Picture – Part IV" Information Security KickStart Highlights, SANS GIAC, 2001.

⁶ Page 5, Clause-by-clause explanation of ISO 22301 by Advisera Expert Solutions Ltd. 2016.

- 2.6 The standard requires that the agency should establish and maintain a plan to enable the agency and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain the availability of information at an acceptable level.
- 2.7 Interview with the LOS administrator revealed that there is no Business Continuity Plan covering the LOS system. Absence of this plan and policies could mean that the agency is not prepared when a disaster happens. Its employees will not know what to do in times of panic and this could implicate severe loss of properties, data, reputational damage, and especially, loss of lives.

B. Failure to conduct Business Impact Analysis (BIA) exposed the agency to unidentified and untreated critical systems and data which could lead to data loss and prolong a disruption of operations in case of disaster.

- 2.8 Conducting BIA in an organization aids in accurately identifying critical business processes, potential incident impacts, and implementing suitable preventive, detective and corrective controls.
- 2.9 *Sub-clause 8.2.1 of ISO 22301:2012* provides that organization shall establish, implement and maintain a formal and documented process for BIA that:
- a. Establishes the context of the assessment, defines criteria and evaluates the potential impact of a disruptive incident,
 - b. Takes into account legal and other requirements to which the organization subscribes,
 - c. Includes systematic analysis, prioritization of risk treatments, and their related costs,
 - d. Defines the required output from the business impact analysis and risk assessment, and
 - e. Specifies the requirements for this information to be kept up-to-date and confidential.
- 2.10 The standard requires that adverse impacts to the organization's services and operations must be systematically analyzed and treated, considering criteria to define potential disruption events, business, legal and other requirements the organization must fulfill, the main risks to be treated, and strategies to be followed.
- 2.11 The agency's resources are not infinite, and they play a very critical role during disruptive events, therefore, there is a need to systematically identify continuity and recovery priorities. Which critical resources or data should be given priority to be replicated or backed up can only be determined through the conduct of business impact analysis and risk assessment.

- 2.12 Without BIA, Recovery Point Objective and Recovery Time Objective or the target objectives in case of disruptions will not be established. With undefined targets, the appropriate actions needed to minimize the impact of risks cannot be determined.
- 2.13 Through the conduct of BIA, an organization can correctly identify critical business processes, identify potential incident impacts, and implement suitable preventive, detective and corrective controls. Therefore, the absence of this process will expose the agency to risks of unidentified critical business processes and data, non-prioritization of core functions and its eventual failure to adopt suitable controls.

C. Inadequate and unsecured backup strategy and media handling procedures exposed the Agency to high risk of unauthorized access to confidential/private information and the inability to continue operations and recover data in the event of a disaster.

c.1 Publicly accessible backup media.

- 2.14 Inspection of the cloud storage account configuration showed that the LOS backup can be accessed by all network, including the internet. Further testing showed that the contents of this storage container “LOSdisks” on the “LOSdb” are indeed accessible by the public. Using the Azure Application Programming Interface on the storage disk through the URL the audit team was able to get the list of backup files in the cloud storage and can be downloaded.
- 2.15 LOS Backup which contains confidential data should be adequately secured. This sensitive personally identifiable information, if obtained by an unauthorized person with malicious intent may result in aggravating consequences such as identity theft and others.

c.2 Non-conduct of backup recovery testing.

- 2.16 *Sub-clause 12.3.1 (e) of ISO/IEC 270002:2013* provides that backup media should be regularly tested to ensure that they can be relied upon for emergency use when necessary; this should be combined with a test of the restoration procedures and checked against the restoration time required. Testing the ability to restore backed-up data should be performed onto dedicated test media, not by overwriting the original media in case the backup or restoration process fails and causes irreparable data damage or loss.
- 2.17 Interview with personnel disclosed that regular testing of restorability of the LOS backup files is not performed. The last two restorations of backup were only conducted during the LOS data migration to the cloud and backup on the test server used for this IS audit.
- 2.18 The backup and recovery of IT service should be monitored and tested to ensure that when they are needed during a major incident, they will

operate as needed.⁷ Therefore, non-conduct of this procedure may expose the Agency to risk that these backup files cannot be restored to serve its purpose and may cause an interruption in operation.

c.3 Absence of locally available backup copy.

- 2.19 Interview revealed that there is no copy of backup that is available locally. Though contract with the Azure cloud assures some degree of reliability, Bureau being the system maintenance and support provider and the Agency as the owner of the data must have a copy of the LOS data.
- 2.20 The non-maintenance of local backup copy renders the Agency reliant to the service provider. In the event of disruption/disaster at the service provider, the agency has no recourse but to depend on the providers control measures and actions.
- 2.21 In view of the foregoing, the preparedness and ability of Agency to resume its IT processing operations the soonest possible time in the event of disaster or fortuitous event are doubtful. Thus, exposing the agency to a higher risk of operational disruption and the inability to continue its key business functions and processes when disasters happen.

Recommendations:

- 2.22 We recommended that Management:
 - a. Formulate business continuity policies, plans, and procedures by considering the following good practices:
 - 1. Perform Business Impact Analysis and Risk Assessment in identifying the critical systems and data, and in determining the appropriate controls to mitigate the identified risks;
 - 2. Define detailed procedures to be followed in the event of disruptions which include the following, among others: (i) response actions and communications to be taken, (ii) conditions and recovery procedures that would enable resumption of operations, and (iii) roles and responsibilities of the BCP teams; and
 - 3. Regularly evaluate the effectiveness of these policies and plans through exercise, test, and review.
 - b. Adopt best practices in its backup strategy to ensure Confidentiality, Integrity, and Availability of its critical systems and data. Particularly, implement strict access control on the cloud storage account on which the back-up server is located.

⁷ ITIL v3 2011 Service Design – 4.6.5.4 Stage 4 – Ongoing operation, Testing

INFORMATION SECURITY

Physical and Environmental Security

3. The physical and environmental security controls of the Agency were inadequate and non-compliant with the provisions of ISO 270001 good practices on protecting the information assets as evidenced by the: (a) absence of security personnel manning the perimeter and premises; (b) physical exposure of confidential records; and (c) lack of fire alarm system, suitable fire extinguishers (IT data media/equipment) and fire exits. These exposed the Agency to the risks of destruction of IT data, equipment, and infrastructure; disruption of business operation; and the inevitable loss of human lives.

3.1 Physical Security refers to the protection of building sites and equipment (and all information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage.⁸ Physical and environmental security controls are used to prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

a. Absence of security guards manning the perimeter and premises of exposed the Agency to possible security threats such as theft of documents and/or confidential information.

3.2 Security personnel duties include protecting people, places, and property from potential threats. Locking doors, watching surveillance footage/CCTVs for hours, patrolling quiet area and monitoring alarms.

3.3 Without the designated security personnel to enforce security and safety in the premises. With its mandate that serves hundreds of people daily and thus, prone to security and safety threats such as theft, vandalism, sabotage, assault, vandalism, and other crimes. Having security guards on site can significantly deter these crimes from taking place as they will ensure smooth operation and address security issues.

b. Personally identifiable information or confidential records of citizens were kept in an open area that is accessible by the public. This exposes to the risks of data leakage or theft of confidential information.

3.4 *Section 25 of the IRR of the DPA* provides that personal information controllers and personal information processors shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data. **The security measures shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing.** These

⁸ Protecting Your System – Physical Security, <https://nces.ed.gov/pubs98/safetech/chapter5.asp>

measures shall be implemented to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination.

- 3.5 Conducted walkthrough, observation, and interviews disclosed the following control weaknesses:
- Copies of the contracts, Job Orders, and supporting documents such as the Employer's Civil ID, visa and passport, among others, are kept at the workstation of the encoder/processor. These documents are yet to be processed in LOS while those that are already processed are kept in an unused staircase and in the basement garage. Both locations – stairs and garage, are observed to be accessible by the public.
 - verified documents and reports are kept in open shelves and on top of the table in an area that is accessible by the visitors/public
- 3.6 As a result of the foregoing, the confidential information was exposed to unnecessary disclosure and fraudulent misuse which may put the Agency at risk of data privacy infringement.
- c. Absence of fire suppressant alarm system, fire exits and the lack of suitable fire extinguishers in the Building of Bureau exposed them to the risk of inability to suppress or prevent fire which could cause prolonged disruption of operations and loss of human lives.***
- 3.7 *Sub-clause A.11.1.4 of the ISO/IEC 27001:2013 (E)* provides that physical protection against natural disasters, malicious attack or accidents shall be designed and applied.
- 3.8 Also, *Section 25 of the IRR of DPA* requires that personal information controllers and processors implement security measures to maintain the availability and integrity of personal data.
- 3.9 Interview and inspection disclosed that the building has no fire suppressant alarm system, designated fire exits signage and only three fire extinguishers are noted and located in the pantry. No fire extinguisher is located in the other floors and places of the building.
- 3.10 The audit team assessed that in the event of a fire, the Bureau may not be capable of early detection; suppression and protection of personal data, equipment, and human lives. These may result in prolonged disruption of operation and reputational damage.
- 3.11 On the positive note, the audit team has observed good physical entry controls such as – perimeter is made of heavy metal, perimeter gates are protected with two locks (steel gate door with built-in lock and backed-up by chain lock), the entry doors are secured by biometric device, manned by guards, and CCTVs are in place.

- 3.12 The above noted control weaknesses if not addressed may expose the Agency to risks of destruction of IT data, equipment, and infrastructure; disruption of business operation; and the loss of human lives.

Recommendations:

- 3.13 We recommended that Management address the above observations by considering the following measures:
- a. Install adequate physical controls to ensure the protection of the information assets against physical security threats as well as the safety of the personnel and the transacting public;
 - b. Locate the confidential records in a secured place that is not accessible by the public. For instance, store these documents/records in a locked cabinet/drawer inside a locked room to ensure protection against unauthorized disclosures; and
 - c. Conduct a study to consider the installation of fire suppressant alarm systems, fire exits signage and suitable fire extinguishers in every floor of the building to ensure the preparedness in the event of a fire.

Workstation Security

- 4. Workstation security controls were found to be inadequate due to the: (a) absence of Acceptable Use Policy (AUP); (b) absence of anti-virus software; (c) inadequate access controls on the workstations; and (d) use of unsupported Operating System and varying patch levels on workstations exposes the Bureau to risks of unauthorized access to its data and disruption of operations.**

4.1 *Absence of Acceptable Use Policy (AUP) resulted in the installation of unnecessary software* The audit team requested for the AUP on both the LabDep head office and its Bureaus, however, this was not provided; the management confirmed its absence. This absence of AUP may have led to the installation of unnecessary software:

4.2 *Installation of unnecessary software.* Review of the installed applications on the workstations revealed that there was software present which the team determined to be unnecessary in the performance of duties. One notable installed application is the “DisableMSDefender.” Suggestive of its name, this application disables the MS Defender antivirus software. As a result, the said workstation with this application has a number of viruses. These installations were made possible due to the presence of administrator access to individual workstations.

4.3 Unrestrained installation of applications gives hackers greater attack surface as application, particularly the freeware sometimes comes with vulnerabilities. It gives the attackers more opportunities to compromise the computer and network which may have caused the slow processing of the workstation and the system.

- 4.4 ***Absence of antivirus application on some workstation.*** Inspection of the installed antivirus application revealed that varying antivirus applications are used by the Bureaus. Some of these applications are trial only, free versions, and sometimes expired. Varied antivirus applications were used such as Windows Defender, Kaspersky, Avast, Avira, and McAfee. Scanned on the sampled workstations revealed a total of 80 viruses.
- 4.5 Virus/malware is the common medium in which hackers exploit local machines. Deployment of viruses would allow attackers to log keys entered by the user allowing capture of login credentials and at worst, to encrypt all files of the system, thereby causing interruption of operations and may have been one of the reasons of slow processing/retrieval of data in the LOS.
- 4.6 ***Workstations with local administrators' rights.*** Inspection of the workstations revealed that most of the workstations have local administrator access which gives the user unlimited power to their machine. This allows the user to perform virtually any actions such as, but not limited to, installation of applications and modification of configuration. Though individual users control these devices, still, this posed a security threat as privilege account is highly targeted and compromise of such by malicious users have catastrophic effects.
- 4.7 ***Inadequate password and session controls.*** Passwords are fundamental for information security. They are used as a first-line defense in securing almost all electronic information, networks, servers, devices, accounts, databases, files, and more. Therefore, it is important that a password must be strong and secured.⁹
- 4.8 The audit team conducted an inspection of the workstations in which LOS was installed and noted the following login configurations:

Particulars	Bureau			
	A	B	C	D
Minimum Password Age	0	0	0	0
Maximum Password Age	42	42	42/-1	42
Minimum Password Length	0	0	0	0
Password Complexity	0	0	0	0
Password History Size	0	0	0	0
Lockout Bad Count	0	0	0	0
Require Log on To Change Password	0	0	0	0
Force Logoff When Hour Expire	0	0	0	0

- 4.9 The above table shows that there were no password and session security controls implemented at each workstation. This lack of controls exposed the agency to attacks such as brute force, password cracking, and others.

⁹ Page 1, Password Management Applications and Practices by SANS Institute. Dated February 15, 2016

Weak implementation of these controls heightens the possibility of unauthorized access.

- 4.10 ***Use of unsupported Operating System (OS) and varying patch levels on workstations.*** Review of the workstations revealed that one machine is using an unsupported OS – Windows XP. Microsoft has announced in its website that support for Windows XP has ended on 8 April 2014.
- 4.11 Usage of unsupported OS exposes the Bureau to a wide array of vulnerabilities. These unsupported OS are outdated and any vulnerabilities existing on these OS are not patched by the software provider.
- 4.12 Further, review of patches disclosed that the different workstations have varying patch levels. These varying patch levels on workstations lead to an incoherent level of security to be followed. While some workstations are patched and thus, have some degree of security, other workstations are not. This allows an attacker to target the weakest link – the outdated workstation becomes a vector to attacks and as a whole leaves the office vulnerable to security breaches or attacks.
- 4.13 Due to absence of an approved AUP, absence of antivirus application on some workstation, inadequate access controls on the workstations and use of unsupported OS and varying patch levels on workstations may lead to inappropriate use of IT resources by users thus exposing the agency to various risks, virus attacks, disclosure of confidential information, data leakage, disruption of business of operations.

Recommendations:

- 4.14 We recommended that Management:
 - a. Formulate and implement policy on Acceptable Use of its IT resources. This policy should stipulate constraints, practices, and responsibilities that a user must agree to for access to the workstation, network or the internet;
 - b. Conduct periodic inspection of workstations to ensure that: workstations are adequately protected by Antivirus software; workstation users are not privileged users or have no local admin rights; there is no illegal/unlicensed and unnecessary software installed; and there is no unsupported Operating System;
 - c. Consider delegating the responsibility for periodic inspection to a Bureau personnel; and

- d. Ensure the immediate cleanup or sanitation of those virus-infected workstations and the installation of antivirus software in each workstation.

Security Awareness

5. The non-conduct of security awareness training led personnel to bypass LOS access controls. This puts the Bureau at risks of non-compliance to the provisions of ISO 270001 good practices and computer/network viruses and the eventual disruption of operation.

- 5.1 One of the greatest threats to information security could come from within the organization. It is not always the disgruntled workers and hackers who are a threat but often the non-malicious or uninformed employee. It is the uninformed users who can harm the organization's network and system by visiting websites infected with malware, responding to phishing emails, storing their login information in an unsecured location, or even giving out sensitive information over the phone when exposed to social engineering. Thus, the conduct of information security awareness training cannot be overemphasized.
- 5.2 Interview with the concerned personnel revealed that information security awareness was is not conducted/provided. Several employees, however, disclosed that they have undergone cybersecurity training but this training was provided years ago or before their deployment to Bureau that they can barely remember the content of the said training.
- 5.3 Moreover, observation and interview disclosed that an employee shares her LOS account to a local hire who is not bonded under the Fidelity Bond to perform cashiering function. Due to absence of security awareness training and many workloads, the said personnel is unaware that she might be putting the Bureau at risk of malicious activities resulting in misappropriation of collection.
- 5.4 The non-conduct of security awareness training may result in a violation of the applicable data privacy law, computer, and network infected with viruses which could interrupt the operation of the Bureau.

Recommendation:

- 5.5 We recommended that Management regularly conduct security awareness training through different delivery media such as classroom-based, web-based, email, newsletters, social media, among others and ensure that employees are aware of the consequences of their actions in the system, network or on the internet.

APPLICATION CONTROLS

6. LOS design was insufficient and not user-friendly. These may lead to risk exposures of compromised accreditation of Placement Agencies

(PAs)/Principals, inefficiencies or duplication of works at Bureau, misappropriation of collections, and compromised the integrity of data.

- 6.1 ***LOS has a module which caters the offline encoding of issued (manually issued) Official Receipts (ORs). This module may preclude the LabDep and Bureaus to capture transactions in real time.*** The Verification/Job Order Payment module is divided into two sub-modules, namely, Payments and Posting. The Payments module or Cashiering System module allows a cashier to record verification payments and issue corresponding ORs. On the other hand, the Posting module allows posting of payments (issued with manual ORs) by batch which could be done after office hours or at a later date.
- 6.2 This sub-module was intended to aid the Bureaus with heavy transactions which issue manual ORs and later on encode the same by batch.
- 6.3 However, to ensure that transactions are entered in real-time, the Management should discourage the issuance of manual ORs as this would only weaken the agency's internal control and defeats the objective of LOS to capture transactions in real-time. Thus, this sub-module should be disabled.
- 6.4 ***Encoded and issued OR can be deleted and edited even without supervisory authorization and a cashier can view the ORs issued by the other cashiers.*** It was noted that issued ORs can be deleted and edited. Moreover, cashiers can view the report of collections or list of ORs issued by other cashiers which are not under his/her accountabilities. As a result, the integrity of LOS data may be compromised and misappropriation of collections may arise.
- 6.5 ***The system design of LOS is insufficient and not user-friendly as it is not easy to navigate, not optimized for seamless interaction among modules, and data or information are repetitively encoded.*** Application systems, as a tool for productivity, should be designed to streamline the operations of an organization. They are built to facilitate business functions; and improve the accuracy, efficiency, and effectiveness of operations.
- 6.6 However, there were several noted observations that may hinder the fulfillment of the said objective of the system. Among the noted inadequacies of the system that has affected its user-friendliness and efficiency were the following:
 - a. Absence of marks/indications for mandatory fields;
 - b. Cashiering module require the encoding of the name of the Payor (this is interpreted as Payee in the system) when this information can be fetched from either the tables (database) of Principal;
 - c. Verification of Documents module requires the encoding of OR No when this could be fetched from the OR table (database); and

- d.* Encoding of the Local Agency Profile in LOS when this could be fetched from the systems of the other available system.
- 6.7 These system weaknesses do not only reduce the effectiveness and efficiency of operations but may have been the reason for its non-full implementation/utilization to all Bureaus.
- 6.8 The above-noted inadequacies may not only preclude the LabDep and Bureaus to meet the objective of the LOS to streamline its operations but may put them to inefficiencies and ineffectiveness thus, affecting their productivity, compromised integrity of data, compromised accreditation of PA/Employers and misappropriation of collections.

Recommendations:

- 6.9 We recommended that Management:
 - a.* Ascertain that encoded/issued ORs cannot be deleted/edited. In cases that there is a need to cancel an OR, this should be done at supervisory level;
 - b.* Conduct a study to determine the much-needed information of the top management or the LabDep management from the Bureau and ensure that these will be tagged as required fields. Also, ensure that redundancies are avoided/eliminated in the LOS and LOS management to work on making the system more user-friendly; and
 - c.* For smooth integration with the systems, consider to re-design the system to enhance its response speed while taking into account the security measures which will ensure Confidentiality, Integrity, and Availability of the data as well as the cost of installation for any update or changes in the system.

Application Controls – LOS Input Controls

- 7. **Input controls of LOS were inadequate that the system accepted the input of inaccurate, invalid, incomplete and duplicate data which exposed the LabDep/Bureaus to risks of erroneous reports, wrong decisions, mishandled collections or loss of revenue, and the inability to perform its mandate to protect and promote the rights, welfare and interests of the workers against abusive and fraudulent employers.**
 - 7.1 Simulation in the test environment and analysis of data extracted in the database disclosed several deficiencies in the input controls of LOS as follows:
 - 7.2 *Lack of data entry validation and range check on the accreditation “Valid Until” field resulted in the inability to determine the validity of the Employer’s accreditation.* It was noted during system walkthrough that the “Date Approved” and “Valid Until” fields were automatically

filled with encoding/processing date. This was also observed when the audit team conducted simulation test wherein an Employers Profile was processed on 10 October 2018, these two fields displayed the date of 10 October 2018 and allowed the record to be saved and processed.

- 7.3 This was further confirmed when the audit team analyzed the provided LOS test data. Of the 26,280 records of employer with “Valid Until” date, 14,701 records were dated the same as the Approval Date. These inaccurate or unreliable dates on the validity of Employer’s accreditation may put the LabDep/Bureaus to the risks of having hired by Employers with invalid/expired accreditation which may result in the inability to protect and promote the rights, welfare, and interests of the workers.
- 7.4 ***Lack of automated validity, required field, and completeness checks for the fields of Address, Tel. No., Fax No., and Email –information that may be needed to effectively respond to workers welfare cases.*** During the simulation test, the audit team intentionally entered invalid inputs on the “Tel. No.,” “Fax No.” (e.g. 123), and “Email Address” (e.g., NA) fields and the system accepted them, and these entries were successfully recorded in the database. Moreover, the system also accepted a blank/null/empty entry on these fields. This observation was confirmed in the processed data where Telephone No., Fax No., and Email fields contained blank, incomplete and invalid data.
- 7.5 In addition, address fields (Address and City) which are essential information of the Employer were not properly completed. Data showed that 124,559 employers out of 138,969 records or almost 90% of the employer records were either with incomplete or without address. These contact details of agencies are vital information in aiding distressed workers.
- 7.6 Based on the foregoing, the LabDep/Bureau was exposed to risks of inability to respond immediately on worker’s welfare cases due to lack of available Employer’s contact information in the system.
- 7.7 ***Absence of embedded program routine to check for duplicate record/s on the Employer Name prevented the LabDep/Bureau to ensure that all employer has a unique profile.*** During the simulation, it was observed that duplicate check/validation control was not embedded in the system as it accepts duplicate profile for Employer.
- 7.8 Keeping the Employer’s profile unique is critical to the operation and nature of transactions especially for confirming the agency’s accreditation status. If an Employer has duplicate or multiple records and one has a negative accreditation status or no status at all, the Bureau will not be able to efficiently and effectively perform verification procedures.
- 7.9 This situation allows the possibility that an employer with revoked accreditation or negative status due to its previous violation history can

still hire Filipino workers thru another profile (duplicate) with positive accreditation status.

- 7.10 ***The Country field in the Employer Profile module has no dependency check and is not a required field which resulted in employer's profile with erroneous, incomplete and misleading information.*** Simulation tests disclosed that the Country field is not automatically populated or defaulted to the country where the processing Bureau is located. The need to select/encode data in the "Country" field under the Principal Profile has led to 737 records with wrong country information. Moreover, this field is not mandatory which is why there are 1,067 entries or records without country information. This field should be automatically filled up with the country where the processing Bureau is located.
- 7.11 Based on the foregoing, data on Principal/Employer profile were exposed to risks of erroneous, incomplete and misleading information which may further lead to wrong decisions by the top management.
- 7.12 ***Non-existent table lookup on the fields under the Accreditation Data grid resulted in the re-entry of data which is prone to errors.*** During testing, the audit team observed that there was no table lookup that could populate fields such as "Status," "Type," "Arrangement," "Category," "Class" and "OR No." from the previously encoded/processed data. This resulted in inconsistent data and tedious encoding of data which is also prone to error. Analysis of the test data showed that there were 2,436 ORs attached as payment for Document Verifications that were not in the "OR" table (LOS database) where all issued ORs are saved. Moreover, there were 22 ORs encoded/used in the Verification of Documents module which pertained to payments of another Employer. Moreover, there were 22 ORs encoded/used in the Verification of Documents module which pertained to payments of another Employer.
- 7.13 ***Absence of Error handling in the Accreditation Data grid.*** During the testing of controls, an error was encountered by the team while encoding the needed information under the Accreditation Data. The grid where the input is supposed to be entered should be done in the correct sequence, otherwise, an error message will pop up and the user will have no option but to close the window, leaving the encoded data unsaved. This will not only confuse the user but also affect his/her productivity.
- 7.14 ***Payment Date field can be edited by the Cashier.*** The system allows payment to be posted at a date other than the date it was transacted in LOS. According to concerned personnel, the payment date is editable to allow the late posting of payments which were not encoded in real time as transactions are sometimes voluminous.
- 7.15 However, analysis of extracted data showed that there were 242 postdated ORs. These ORs are not late posting as the OR dates are future dates or dated later than the current/posting date. The absence of control over the OR date exposed the Bureau to inaccurate collection reports, unaccounted cash collections and mishandled collections.

7.16 ***OR No. can be encoded, edited, skipped, and re-used. This exposed the LabDep/Bureaus to risk of unaccounted/unrecorded collection which may lead to loss of revenue.*** Simulations were conducted in the system to test its embedded input controls on this module. The result of the tests was captured in *Figure 3* or the *Report of Collection for the period 1 to 17 August 2018* and noted observations were explained below:

Observation	Explanation
1. <i>OR No. can be skipped or changed.</i>	As can be observed from <i>Figure 3</i> , OR Nos. are not in series. The audit team intentionally changed the auto-generated OR No. into a new OR No. and the system accepted it.
2. <i>Previously issued/posted OR No. can be re-issued.</i>	The audit team intentionally entered a previously issued OR (OR No. 1000001) and the system replaced the details of the OR with the recently posted OR. It appeared that the first instance of the OR can no longer be recovered from the system. The OR No. 1000001 which was posted on 22 June 2018 was reposted or re-issued for another payor on 10 July 2018. The said OR is now posted under a new payor.
3. <i>The system accepts and processes OR with blank details on Payor and Amount.</i>	The system accepted OR entries without Payor Name and Amount. This can be seen in <i>Figure 3</i> where OR No. 10000182 and 10000183 were posted without Payor and Amount.
4. <i>Auto-generated OR No. cannot be relied upon as the sequence restarted at some point.</i>	During a simulation, the auto-generated OR No. restarted and went back to previously issued OR. The OR No. 2000001 which was posted/issued on 10 July 2018 was re-prompted again on 1 August 2018.
5. <i>A cashier can issue OR series outside assigned OR series</i>	As a control, the Administrative Staff who is assigned to perform the Cashiering is being assigned a series of OR number thru the Accountable Forms module. However, the test of control revealed that a cashier can post or issue series of OR number not assigned to him/her. Also, the test revealed that OR need not be a registered OR in the Accountable Forms in order to be issued in the cashiering or payment issuance module.

OR Date	Payor	No. of Documents Verified	Official Receipt No.	Amount(Local Currency)
08/02/2018	TEST	1	1000016	10.00
08/07/2018	TEST NOT ISSUED FORMS	1	10000181	0.00
08/07/2018		0	10000182	0.00
08/07/2018		0	10000183	0.00
08/02/2018	TEST FUTUREDATE	0	2000008	0.00
08/02/2018	TEST FUTUREDATE	0	2000009	36.00
08/02/2018	TEST FUTUREDATE	2	2000010	40.00
7		TOTAL:		86.00
8/17/2018 10:20:01AM				

Figure 3. Report of Collection presenting nonsequential OR No., and blank/empty OR details (Payor and Amount)

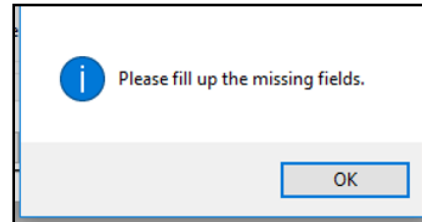
- 7.17 The absence of document control or the issuance of non-sequential OR will prevent the proper accounting and monitoring of issued ORs which could result in manipulation and mishandling of collections.
- 7.18 ***The lack of table lookup on Payor field unnecessarily allows the erroneous entry on this field and may lead to difficulty in associating the OR to the verified documents.*** It was observed from the system that the Payor (called Payee in LOS) field is just an input field where the cashier needs to encode the name of the payor instead of just fetching this data in the Employer profile.
- 7.19 Absence of input control such as table lookup to ensure that only valid Payor (called Payee in LOS) or employer is inputted in the Payee field when posting payments resulted in numerous payments accepted from unidentified employer. This practice exposed the Bureaus to the risk that payments will not be tagged to the employer who actually paid the verification fee.

Other Notable Observations on Various Modules

- 7.20 In addition to what was noted in the aforementioned modules, below are observations on other modules of the system:

Observation	Details
<i>Viewable forms of the query/search function of the system are in edit mode</i>	All modules of the system are equipped with a query/search function. This function is a good utility to view the previously encoded transactions or transaction history in the system. Simulation test disclosed that these data which are intended for read/view only can be edited without restriction and warning. For example, any user can search and view the profile of a certain employer and may either intentionally or unintentionally modify the said employer profile. As a result, the data integrity of the LOS may be compromised.

Observation	Details
<i>Lack of required field markings</i>	Mandatory field has no mark or identification (i.e. “*Required Field”) that will aid the user in determining which fields are required. To compensate for this absence of required field, LOS has an information message notifying the user that there are missing fields.



However, the message lacks information on which specific fields are missing. As a result, the encoder will have to guess which fields were left out in order to save the record.

This observation was particularly noted in the following modules:

- a. Validation of Documents
- b. Passport module - Date of Birth
- c. Verification/Job Order Payment Issuance

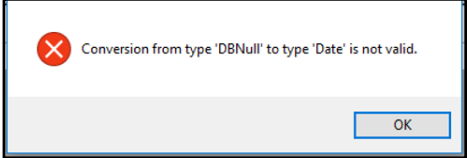
<i>Lack of table lookups in the Cash Advance module</i>	It was noted during simulation that Cash Advance module requires the encoding of the names of the payees, signatories and their positions. This information as already available in the system’s database should be fetched and not encoded. This exposed this information to inaccuracies and affects the efficiency of the encoder.
--	---

<i>Absence of user confirmation to validate inputted data when creating or editing records</i>	In LOS, users are not prompted with a confirmation dialog when editing/modifying/deleting record. This confirmation dialog will allow the user to review or check the actions taken and make a correction if necessary. A confirmation option also helps prevent or reduce errors, especially those committed accidentally.
---	---

<i>No status indicator or visibility of system status to show that there is a process running or that the system is responding to a user’s command</i>	The visibility of system status refers to how well the state of the system is conveyed to its users. Ideally, systems should always keep users informed about what is going on, through appropriate feedback within a reasonable time. ¹⁰
---	--

During testing, the team noticed that there is no status indicator that will inform the user if the

¹⁰ <https://www.nngroup.com/articles/visibility-system-status/>

Observation	Details
	<p>system is responding to actions such as searching for records or saving a transaction. Not knowing if the button was clicked the first time, the encoder will have the tendency to continue clicking the command button instead of waiting for the process to be finished. Without the information on the current state, the users will feel a lack of control on the system and may affect his/her productivity.</p>
<p><i>Error messages are not user-friendly or descriptive for the user to identify the cause of the error.</i></p> <p><i>Some of the functionalities or buttons are not working such as Delete and Print buttons in the Passports and Payment Issuance module</i></p>	<p>LOS error messages are not informative, user-friendly and descriptive as shown below:</p> <div data-bbox="858 645 1326 801" style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;">  </div> <p>As a result, the user would not know what happened and what should be done next. Thus, affecting his/her productivity.</p> <p>The audit team also tested if the command buttons are functioning as expected. The Delete and Print buttons in Passports and Payment Issuance module are found to be not responding or not working.</p>

- 7.21 Input controls are good in mitigating errors/mistakes, omissions, duplicates, and fraudulent entries. These controls will not only help in ensuring that inputted data are valid, accurate and reliable but also aid the agency to enforce compliance to laws, rules, and regulations.
- 7.22 Absence of embedded routines in the LOS Data Entry program to check and validate fields for validity, accuracy, and completeness may render LOS data invalid and unreliable and may expose the agency to risks of violation of applicable laws, rules and regulations.

Recommendations:

- 7.23 We recommended that Management address the above-noted observations and ensure that LOS data are valid, accurate and reliable. More specifically, the Management should ensure that the following are observed:
 - a. All modules should have the following input checks, among others:

1. Required Field Checks and markings for all mandatory field/data such as accreditation information, Name, contact details, and others.
2. Validity Check on *Tel No.*, *Fax No.*, *Email Address*, and all Date fields. “Valid Until” field under Employer/Principal Profile module should either be automatically computed or ensure that it does not accept date similar to or earlier than the encoding and approval date.
3. In the Verification of Documents module, table lookups should be in place for data that are already in the system such as OR No., Employer, and RA data. For information that should be shared from OEA like data for RA Profile, Worker profile and accreditation data, table lookup should also be in place to avoid erroneous entries and redundancies/re-encoding.

This should be observed also in the Cash Advance module for the fields of *payee (should be payor)*, *signatories*, and *position*.

- b. *OR Number* and *Date* are automatically generated, cannot be edited/modified, and re-used. Also, OR should be issued sequentially and the system should restrict modification or deletion of OR. Moreover, the system should ensure that ORs are properly assigned and cashier should be restricted to issue only within the assigned OR series. Management should discourage the issuance of manual ORs as this would only weaken the agency’s internal control and defeats the objective of LOS to capture transactions in real-time. Thus, the Posting sub-module under the Verification/Job Order Payments module should be disabled.
- c. Employers should not have duplicate profile entries. In case, an Employer has multiple branches, adding the branch name in the Employer’s Name is advised.

Application Controls – LOS Processing and Output Controls

8. **Processing and Output Controls of the LOS were inadequate that the LabDep/Bureaus were exposed to the unreliable accreditation process, erroneous and unreliable collection reports, untraceable malicious activities, compromised availability and integrity of data, disclosure of sensitive data, and the risks of misinterpretation and wrong judgment/decision brought by inaccurate output.**

A. Processing Controls

- 8.1 Simulation in the test environment and analysis of data extracted in the database disclosed several deficiencies in the processing control of LOS as follows:

- 8.2 **Missing Profile of Employee with transactions in LOS which may lead to or an effect of compromised data integrity.** File updating and maintenance authorization is one method of the data file controls to ensure that only authorized processing occurs to stored data. Proper authorization for file updating and maintenance is necessary to ensure that data are safeguarded adequately, correct and up to date.¹¹
- 8.3 Verification in the LOS database revealed that there were employee profiles with recorded transactions that were missing or deleted in the database. The Employee IDs that were found to have transactions can no longer be identified or were deleted in the system, thus, might cast doubt on the validity and authenticity of these transactions. These deleted employee profiles are presented in *Table 9* below:

Employee No.	Module	Field	No. of Records
57	Employer Profile	Approver	2
300			361
321	Verification of Documents	Encoder	2
125	Worker Profile	Encoder	2
153			61
321			3
455			3

Table 9. Deleted Employee Profiles with transactions in LOS

- 8.4 **Existence of 111 records with missing Employer or RA profile or without the agency name in the Employer Accreditation table resulted in the unreliable accreditation process and the difficulty to identify the employer or RA.** The Verification of Documents module of the LOS captures the creation of New Accreditation, Renewal of Accreditation, Cancellation of Accreditation, New Job Order, Dual Job Order, Additional Job Order, Workers Deployment and other Principal and Local Agency transactions including scanning/uploading of documents.¹²
- 8.5 This module was designed to register/accredit an employer to its RA partner. Data revealed that there were 26 records without the name of employer while 85 records were without RA name in its accreditation record. Validation of data showed that there were employers and PRAs profile that was deleted or no longer exists in the Employer and Agency table, respectively.
- 8.6 It was learned through simulation in the test environment that creation of Employer and RA profiles should be done first before the Verification of Documents. In the Verification of Documents module, the fields on Employer Name and RA/Agency Name were automatically populated.

¹¹ Page 227, Chapter 3 – Information Systems Acquisition, Development and Implementation of CISA Review Manual 26th Edition

¹² Section 4.7.5 of the LOS Manual

However, the above-noted observation showed that the system was either not able to fetch the data or the profiles of the employer and the RA were deleted. This was validated through audit logs review where the audit team noted that some of the above records were deleted. As a result, the processing controls in this module could not be relied upon.

- 8.7 ***Creating and updating Payments for Verification not captured in AuditLog may expose the LabDep/Bureau to the risk of untraceable malicious activities.*** Transaction Logs is one method of data file controls to ensure that only authorized processing occurs to stored data. It contains detailed listing, including date of input, time of input, user ID and terminal location. It also permits operations personnel to determine which transactions have been posted. This will help decrease the research time needed to investigate exceptions and decrease recovery time if a system failure occurs.¹³
- 8.8 LOS has two audit reports which include statistics for encoded data per module and Dashboard which shows the encoder's activity or action per module. However, verification and testing revealed that creating and updating of payments for verification were not captured in the Audit Log which is crucial in ensuring the traceability of transactions related to the collection of verification fees. Due to this, there is a possibility that posted payment or OR can be edited without being discovered. Thus, the LabDep/Bureaus may be exposed to the risk of manipulation/mishandling of collections or loss of revenue. Moreover, the LabDep/Bureaus will not be able to trace and prevent these malicious activities or fraudulent acts from happening.
- 8.9 ***Updating and deleting payment records caused gaps in the ORMasterID series which could lead to unaccounted collections.*** ORMasterID is the unique identification and control number that is used to track and validate OR sequence in LOS. It is a data validation control that can be used to identify data errors, missing or inconsistent data items.
- 8.10 In LOS, every OR Number (ORNo) has a corresponding field header called ORMasterID. This ORMasterID can be used as compensating control if certain issues arise in the ORNo series. Review and evaluation of the OR data disclosed the existence of gaps/missing series in the ORMasterID field of the ORMaster table.
- 8.11 Moreover, functional testing was conducted to determine the possible causes of the gaps in the series by editing OR No. 2000007 recorded under ORMasterID 218183 as depicted in *Figure 4*. After editing the OR amount, the said OR is now recorded under ORMasterID 219185 and the ORMasterID218183 is now missing in the series as shown in *Figure 5*. Another instance that caused the occurrence of gaps is by outright deletion of OR record as performed during the actual test conducted.

¹³ Page 227, Chapter 3 – Information Systems Acquisition, Development and Implementation of CISA Review Manual 26th Edition

	omasterid	omo	ordate	remitDate	poloid	payee	LocalAmount	UsdAmount
30	218180	10000183	2018-08-07 11:35:33.007	2018-08-07	12		0.0000	0.0000
31	218181	10000185	2018-08-17 10:22:20.000	2018-08-17	12	FRA-COA	20.0000	20.0000
32	218182	2000006	2018-08-22 14:10:34.000	2018-08-22	12	FRA	36.0000	36.0000
33	218183	2000007	2018-08-23 15:56:29.000	2018-08-23	12	FRA	10.0000	10.0000
34	218184	1111101	2016-06-22 16:21:13.000	2016-06-22	10	SAMPLE TEST	40.0000	0.0267
35	218185	2000008	2018-09-07 10:13:41.000	2018-09-07	12	COA	1.0000	1.0000
36	218187	2000012	2018-09-07 10:29:30.690	2018-09-07	12		0.0000	0.0000
37	218188	2000013	2018-09-07 10:29:30.690	2018-09-07	12		0.0000	0.0000

Figure 4. OR No. 2000007 amounting to USD10.00 recorded under ORMasterID 218183

	omasterid	omo	ordate	remitDate	poloid	payee	LocalAmount	UsdAmount
35	218187	2000012	2018-09-07 10:29:30.690	2018-09-07	12		0.0000	0.0000
36	218188	2000013	2018-09-07 10:29:30.690	2018-09-07	12		0.0000	0.0000
37	219185	2000007	2018-08-23 15:56:29.000	2018-08-23	12	FRA-TEST EDIT	30.0000	30.0000

Query executed successfully.

Figure 5. After updating the amount (from USD10 to USD30) of OR No. 2000007, it is now recorded under ORMasterID 219185

- 8.12 Since creating and updating of OR were not captured in the AuditLog, it will be impossible to determine the details of the missing series in the ORMaster table or the details of the OR before it was updated.
- 8.13 Thus, having skipped or missing ORMasterID will entail difficulties in the monitoring of processed ORs and could lead to the risks of lost or mishandled collections and that may affect the validity, integrity, and accuracy of the financial records.
- 8.14 ***Existence of erroneous timestamp in the posting of payment which may result in untraceable transactions and loss of revenue.*** Verification of test data revealed that there were 95 transactions in ORMaster table with a posting date of “12/06/2018” while the “ORDate” and “RemitDate” fields for the same transactions were both dated “3/6/18.” Inquiry with the LOS team revealed that the “timePosted” captured by the system is based on the client computer and not on the server date since date and time across Bureaus varies. This means that should the date of the client computer is not accurate, the posting date will be inaccurate, too.
- 8.15 The accuracy and consistency of date and time are important as these might affect the reliability and authenticity of payments being processed by the system. As a result, the LabDep/Bureau was exposed to the risk of loss of revenue due to possible fraudulent handling of collections and the inability to trace such transactions as the audit log was inadequate.
- 8.16 ***Employer and Agency Profile recorded “NULL” values on EncodedByID and DateEncoded fields*** An audit trail (audit log) is an important feature of a fully developed information system which acts as a secure data transaction recorder that reflects the sequence of events on a database or set of records. It can also provide documentary evidence on

the chronological occurrence of activities, specific operation, procedure, or event (i.e. add, edit/update, delete).

- 8.17 Verification of LOS data revealed that there were numerous profiles of Employer and Agency without details on encoder and timestamp. Aside from capturing the information in the transaction log, ensuring the completeness of the information is also important to easily identify who is responsible for the performance of action and trace when the action took place. This system deficiency may lead to an inability to immediately determine who created a transaction and when it was created, particularly those malicious ones.
- 8.18 The above-mentioned deficiencies in the processing controls of the LOS may pose risk exposures of compromised data integrity, invalid accreditation process, untraceable and cannot be validated changes in the database, and unreliable collection reports which could lead to loss of revenue.

Recommendations:

- 8.19 We recommended that Management address the above-noted observations and ensure that the following are observed:
- a. Prevent the deletion of records with dependencies or related transactions. Also, the system should restrict the functions of delete and update/edit to authorized personnel with Supervisory privileges only;
 - b. Ensure that all transactions are properly accounted for such that encoder and timestamp are captured and recorded accurately; and
 - c. Ascertain that audit trail/log should be able to capture and monitor all activities in the system which include Log-In, Add, Edit/Update, Delete and Print. Also, the audit trail should be able to provide a list of activities performed by a user for a given period upon request.

B. Output Controls

- 8.20 Reports generated from the system represent data that management relies upon for business decisions and review of business results. Therefore, ensuring the integrity of data in reports is a must to account for the reliability of the information in the systems and effectiveness of decision-making process.
- 8.21 ***Incomplete payment details in the Official Receipt (OR) may preclude the LabDep/Bureau to determine the accuracy of the OR.*** Printed payment receipt does not contain details such as the quantity and list of the verified documents as well as the name or initial of the cashier who processed the payment. This information can be used to check the number of documents verified as well as easily identify actual documents submitted by the employer for verification. In other words, this information will help in determining the accuracy of the amount charged. Thus, the absence of these details may preclude the agency to determine the accuracy of the amount charged to its clientele.
- 8.22 ***Report to Congress does not capture actual transactions in LOS, thus its reliability may be compromised.*** Generated Reports to Congress are not from actual transactions or data stored in LOS. Statistical information such as the job classification, labor/welfare cases, and other welfare services that can be captured in the system are manually inputted by the users in the module Report to Congress instead of just fetching it from the system's processed data. *Section 10 of the Bureau Manual* provides that all transactions at the OLO shall be recorded in LOS and therefore shall be the basis in generating the report. However, this was not observed. As a result, these reports are prone to errors and manipulation. Thus, their reliability is compromised.

B.1. Other notable observations on various reports

- 8.23 In addition to the above-noted findings, below are other minor deficiencies noted in the system:

Observation	Details
<p><i>Understandability of both the Report of Collections and the Monthly Report of Collections and Deposits is compromised</i></p>	<p>A report to be effective should be accurate, complete, and understandable. It is important that the information presented is easy to find and understand by the user/reader.</p> <p>It was noted in the Report of Collection, and Monthly Collections and Deposits Report that the OR No. or the Official Receipts No. column is not presented beside the OR Date column. Logically, these two columns should be presented side by side for easy flow of thought of the reader.</p>

Observation	Details
<i>Names and address information in the reports are incomplete</i>	Reports such as Employer and Agency Summary and Collection Reports are showing incomplete name or address information due to limited field space.

- 8.24 Inability to ascertain LOS output’s reliability and security can expose the LabDep/Bureau to the risks of misinterpretation and wrong judgment or decision brought by inaccurate output and disclosure of confidential information.

Recommendations:

- 8.25 We recommended that Management address the above-noted observations and ensure that the following are observed:
- a. OR details are complete and include details on *quantity, list of verified documents, and the name of the cashier*; and
 - b. Reports are understandable, properly formatted and with complete information such as the name and address.

Application Security – Password, Session, and Audit Management

9. The unsecured implementation of LOS’ password, session, audit management, and other data security measures exposed the LabDep/Bureaus to the risks of unauthorized access, disclosure and manipulation of confidential information which may render the LabDep liable for damages caused by a violation of international data privacy law.

- 9.1 *Usage of the encoding scheme in the transport and storage of passwords.*
 In providing data security, there are various methods which an organization can employ. These include encoding and encryption, among others. Encoding is the process of converting data into a format required for a number of information processing needs.¹⁴ While encryption is the process of converting messages, information or data into a form unreadable by anyone except the intended recipient.¹⁵ Encoding may seem like encryption for data gets changed from one form to another and the encoded text does not look like the original. However, it does not use substitution and transposition based on a secret key. Encryption requires a key while Encoding requires only knowledge of the type of encoding. Example of an encoding scheme is Base64.¹⁶
- 9.2 In the conducted simulation in the test environment under the User Administration module, the audit team selected each user account and it

¹⁴ <https://www.techopedia.com/definition/948/encoding>

¹⁵ History of Encryption by SANS Institute

¹⁶ Base64 Can Get You Pwned by SANS Institute: *Base64 is an encoding scheme originally designed to allow binary data to be represented in ASCII text.*

was observed that passwords were masked but its length is determinable. This means that the application system can reverse or has the knowledge of the actual password.

- 9.3 Review of source code disclosed that decrypt and encrypt function was used in its authentication process. However, further scrutiny of the source code revealed that the application was using a base64 encoding scheme. To confirm this, the audit team, through an online base64 decoder attempted to decode the test account's password contained in the "Users" table (database) and has successfully obtained the actual password ("password") as shown on the image below:

	A	B	C	D	E	F	G	H
1	User	UserName	Password	EmployeeID	ViewOnly	Encoded_from_base64	password	p_length
440	456	insulare	cGFzc3dvcnRlZS10b2t1bg==	676	0	passwordbe-token	password	8

- 9.4 This implies that the audit team (or anyone who has access to the LOS database) could also decode **the passwords of all LOS users** contained in the test database or the actual database.
- 9.5 Implementation of the encoding scheme in the transport and storage of passwords is a weak means of securing confidential information such as a password. Perpetrators who have knowledge of the type of encoding scheme may be able to decode the encoded password text and gain unauthorized access to the system. The perpetrators can simply copy-paste the obscured password text into an online base64 decoder to recover the original password text. Consequently, the agency is exposed to the risks of unauthorized access, data leakage or disclosure.
- 9.6 ***Access to the user administration module allows access to encoded password texts of users.*** Simulation at the user administration module disclosed that any user who has access in the user administration module can intercept the encoded passwords and determine the encoding scheme used. This was confirmed through packet sniffing at the said module which showed that the encoded password text of all the users is being fetched by the client's machine regardless of access permissions – whether write or read access.
- 9.7 As a result, anyone who has access to the user administration module whether read or write access, provided he/she has enough technical knowledge, may decode the encoded password text to obtain the password. This person may then use other user's account to perform unauthorized or destructive actions such as manipulation of data/records.
- 9.8 ***Password length and complexity was not implemented.*** Secured password management requires that unique passwords be used for each account. Passwords must be both long and complex; comprised of numerals, mixed-case letters, and special characters. They also should not

be words or be names of anything which could be associated with their owner.¹⁷

- 9.9 System simulation test revealed that minimum password length and complexity was not implemented. The application allowed users to change the password to only one character or a word similar to the User ID/User Name.
- 9.10 This absence of enforced control will lead to the use of a simplistic password which can be either the same as the User ID, a word found in the dictionary, and contain personal information, such as names of spouse or family members or any information that an attacker could easily derive from a user. This will expose the agency to high risks of brute force attacks or password-guessing attack which could be used to gain unauthorized access to the system.
- 9.11 ***Lack of compulsory change of password on the first login.*** It was disclosed through an interview with the LOS system administrator that during user account creation, a pre-defined/default password (*e.g. 1234*) is assigned to the user's account. Upon initial login, users were prompted to change their password. Any subsequent password change is through the user administration module in which the administrator resets the user's password to the same default password (*e.g. 1234*).
- 9.12 Interview with the system administrator revealed that if the user's password is similar to the default password, users will be prompted to change their password. This was later confirmed on system simulation. However, it was observed that though users were prompted to change their passwords, this does not prevent them from using the system.
- 9.13 Further validation of "Users" table in the LOS database showed that of the 438 total users, 186 or 42.47 % of LOS users have retained their default password as shown on the table below:

Particulars	No. of Users	%
Non-Default Password	252	57.53
Default Password	186	42.47
Total	438	100

- 9.14 Also, review of audit logs showed that there were users with default password who continued to access and process transactions in LOS. Some of these users were provided below:

UserID	UserName	LastLoginDate
454	kuyami	6/19/2018 10:58
349	usaragamr	6/13/2018 21:17
152	rubioc	6/13/2018 14:23

¹⁷ Page 2, Password Management Applications and Practices by SANS Institute. Dated February 15, 2016

UserID	UserName	LastLoginDate
286	huangm	6/7/2018 11:08
352	avilama	6/2/2018 11:30

- 9.15 This absence of enforced password change resulted in the retention of the default password. Anyone who has knowledge of the default password can maliciously access concerned accounts and perform unauthorized actions as allowed by the account’s access rights.
- 9.16 ***Absence of predefined password expiry.*** Inquiry with LOS Administrator and review of the “Users” table (LOS database) disclosed that the system had no functionality to set password expiry as there were no fields for date of the last password changed and password validity in the database.
- 9.17 This absence of predefined expiry of a password will result in the unchanged password for an indefinite period. A perpetrator who has the knowledge of the user’s password will have unlimited time to access this compromised account. Depending on the user’s access rights, the perpetrator may be able to destroy or modify critical data.
- 9.18 ***Reuse of passwords.*** Simulation test in the system revealed that the system allowed the reuse of previously used passwords. The audit team was able to change the password to the same password currently being used.
- 9.19 Further inspection of the “Users” table (LOS database) disclosed that the system does not keep a history of previously used password other than that of the currently used password. This resulted in the inability to check whether the new password matches previously used passwords and consequently, the system is unable to prohibit the reuse of past or previously used passwords.
- 9.20 Reusing of password affords the attacker a great chance to determine the password through brute force attacks. Thus, exposing the agency to the risk of unauthorized access and leakage of confidential data.
- 9.21 ***Absence of self-service password change functionality.*** It was observed during simulation tests that the system has no self-service password change functionality. Subsequent password change is effected only through the user administration module in which the administrator resets the user’s password to the same default password.
- 9.22 This absence of self-service functionality may cause a delay in changing passwords. Users who suspect that their accounts were compromised will have no recourse but to request the system administrator to effect password modification. Consequently, perpetrator’s window time for malicious activities is unnecessarily increased.
- 9.23 ***Storing of password on the configuration file.*** Inspection of the configuration/manifest file of the LOS Client application version dated 07 May 2018 showed that password and username for database connection

were divulged. However, for versions after 26 June 2018, this issue was no longer observed.

- 9.24 Although further testing showed that this password is not accepted in the system, this situation gives the attacker a hint on the password requirements and structure of the application, thereby aiding the attacker in its brute-force attacks.
- 9.25 **Single default password is generated/used for each created user account**
It was observed during the simulation that the pre-defined or default password is similar for each created user account. In addition, all password resets were reverted to the said default password and not to a randomly generated password. This means that an authorized user who already knows the system's default password can easily perform an unauthorized transaction using the accounts of others.
- 9.26 **Lack of session timeout.** A session is a series of interactions between two communication end points that occur during the span of a single connection. Typically, one endpoint requests a connection with another specified endpoint and if that endpoint replies agreeing to the connection, the endpoints take turns exchanging commands and data ("talking to each other"). The session begins when the connection is established at both ends and terminates when the connection is ended.¹⁸ While session timeout defines an action window which represents the time span in which an attacker can try to steal and use an existing user session.
- 9.27 Upon inspection of the system, it was observed that the server does not revoke connections even after long idle or inactivity of the application. This was confirmed through validation of audit logs which showed that a user's session remained active despite its long duration of inactivity in the system. Sample of these are presented in the table below:

User ID	Audit LogID	Entity/Module	Trans Name	Trans Date	Time Diff bet. Login & Transaction	Remarks
100	1415599	Main Menu	LogIN	18/03/2018 20:35:16	00 19:04:01	User 100 logged in at Main Menu
	1418043	Worker	LogIN	19/03/2018 15:39:18		User 100 accessed the W Module
119	1497332	Main Menu	LogIN	28/04/2018 9:07:22	01 1:37:36	User 119 logged in at Main Menu
	1497566	Worker	LogIN	29/04/2018 10:44:58		User 119 accessed the W Module

- 9.28 The above table showed that a user (UserID 119) has stayed logged in and remained idle for as long as one day, one hour, and thirty-seven minutes before it accessed or transacted in the Worker module. The audit team, however, was not able to determine when did the user logged out as the system's audit log does not capture the user logout event.

¹⁸ <https://searchmicroservices.techtarget.com/definition/session>

- 9.29 Absence of session timeout or the functionality of the system to forcibly log out a user after a period of inactivity exposes the system to session hijacking and Man-In-The-Middle¹⁹ attacks. The attacker has an unlimited time to steal and use an existing user session which will result in unauthorized access to confidential information as permitted by the compromised account's access privilege.
- 9.30 ***Lack of automatic account lockout after several unsuccessful log-in retries.*** Testing revealed that the application does not automatically lock out the account after consecutive unsuccessful log-in retries. This absence of account lock-out mechanism exposed the agency to risk of brute-force attack in which the attacker has an unlimited number of retries in its attempt to gain unauthorized access in the application.
- 9.31 ***System allows simultaneous log-in and the lack of warning/detection thereof.*** Simulation test conducted in the LOS revealed that the system allowed simultaneous log-in. The audit team was able to login to multiple computers at the same time. It was further noted that the user is not notified of the other sessions.
- 9.32 Also, data analysis of the audit logs showed that there were instances of consecutive login events on the same User ID. Below are a sample of these instances:

Audit LogID	Trans Name	User ID	Trans Date	Time Diff (in seconds)	Remarks
1600468	LogIN	1	26/06/2018 17:48	0	First login instance
1600469	LogIN	1	26/06/2018 17:48		Subsequent login instance
1610468	LogIN	455	27/06/2018 11:23	1	First login instance
1610469	LogIN	455	27/06/2018 11:23		Subsequent login instance
1620724	LogIN	455	03/07/2018 14:56	1	First login instance
1620725	LogIN	455	03/07/2018 14:56		Subsequent login instance

- 9.33 The audit team, however, was not able to determine the origin of each connection as the IP addresses of the user's connection are not logged. Allowing simultaneous log-in and the absence of notification to the account owner will result in the possibility of compromised account and the eventual data manipulation and disclosure.
- 9.34 ***Absence of transport encryption of confidential information exposed the agency to the risks of data disclosure/leakage.*** Interview with the LOS administrator disclosed that the connection string used by the application is encrypted. During the period when the application was hosted on the

¹⁹ The man-in-the middle attack intercepts a communication between two systems. For example, in an http transaction the target is the TCP connection between client and server. - https://www.owasp.org/index.php/Man-in-the-middle_attack

premise of the Bureau office, a Virtual Private Network was used to encrypt the connection between the client application and the server.

- 9.35 Sniffing of packets transmitted and received while using the system revealed that information is transmitted in unencrypted form as the audit team was able to capture the transmitted data in clear text form. This means that all transported information through the system such as Employer's name, passport number and other information is forwarded in a readable format.
- 9.36 Based on the foregoing, perpetrators who may have tapped the connection between the server and the application may obtain sensitive information. The LabDep/Bureaus is exposed to the risk that sensitive personal information obtained from this activity may then be used for malicious intent such as identity theft.
- 9.37 ***Application installer was downloadable by anyone without prior authentication which may put the agency to risks of unauthorized access to the system.*** Interview with the LOS team revealed that initial installation is facilitated onsite or at Bureau site while subsequent updates are deployed through the auto-update functionality of the system.
- 9.38 Review of the "LOS.UI.application" configuration located at the installation folder of the application client disclosed that the application installer is available for download at the URL. This URL is also the same site in which the application fetch updates. The same URL is also indicated in Section III, Item 3.1 "Launching LOS" of the LOS Manual.
- 9.39 Subsequent validation revealed that this download link is accessible outside of the LabDep network. Through this site, the audit team was able to download and install the application. Further testing using a generic account and a default password combination, the audit team was able to gain access in the application.
- 9.40 The lack of control over the download of the application installer allows anyone with knowledge of the URL and internet connection to obtain a copy and install the application. This would then allow perpetrators to reverse engineer the application and may subsequently pose possible unauthorized access to the system.
- 9.41 ***Log out and invalid log in events are not logged.*** Inspection of all the event types on the audit logs table disclosed that only successful system Login, used transaction modules, and other transaction related events were logged. Log out and invalid log in events were not logged in the system.
- 9.42 Successive invalid login may be indicators of brute force attacks and are a precursor to unauthorized access. Lack of logging of these events will result in an inability to identify accounts compromised by brute-force attacks. As a result, the LabDep/OLOs are exposed to the risk of inability

to determine session hijacking and brute-force attacks and to proactively act on them.

- 9.43 ***Device identity and location or origin of the users are not captured.*** The LOS system is expected to be accessed anywhere in the world. Attacks coming from other sources even from the geographically distant parts of the world are possible.
- 9.44 Review of the fields of the audit log tables showed that there is no identification of the actual origin of the connection i.e. IP address. Though OLOID field is present, this information is linked to the account and doesn't necessarily mean the actual location of the user. Therefore, in the case of a security breach, the LabDep/Bureaus will not be able to identify the location of the perpetrator.
- 9.45 This inadequacy of logging and subsequent monitoring thereof will result in an inability to (a) track and identify security threats; (b) proactively act on these threats as they progress to prevent serious harms to the agency; and (c) provide sufficient evidence in support for legal remedies on security breaches.
- 9.46 The lack of application security controls as evidenced by the (a) absence of password policy and the unsecured password security measures; (b) unsecured session and log-on procedures; (c) absence of transport encryption of sensitive personal information; (d) publicly downloadable application installer; and (e) inadequate logging of user activities posed high risks of unauthorized access, leakage and manipulation of confidential information which may lead to data privacy law infringement.

Recommendations:

- 9.47 We recommended that Management:
- a. Formulate, adopt and enforce password policy to address the above-noted weaknesses in LOS' password security measures. In doing so, management should consider the following:
 1. Secure the password using irreversible hashing algorithm or encryption;
 2. Disable fetching of encoded password when using the User Administration Module;
 3. Implement password complexity requirements;
 4. Implement password change mechanism which covers the following:
 - i. Compulsory change of password at first or initial login;
 - ii. Password expiry;
 - iii. Prevent re-use of passwords; and
 - iv. Self-service password change functionality
 5. Prevent the storing of login credentials on unsecured locations such as configuration files; and

6. Consider the use of a randomly generated password on user account creation and password resetting.
- b. Implement sound session management which includes the following control measures, among others:
 1. Session time-out;
 2. Account lock-out after invalid logins; and
 3. Prevent simultaneous login and provide the facility to detect and warn the user in the event of simultaneous login.
 - c. Ensure that traffic between the client and the server is always encrypted;
 - d. Restrict access to application installer to only authorized personnel; and
 - e. Ensure that all relevant log events and information are captured in the system's audit log which includes the following, among others:²⁰
 1. User IDs;
 2. System activities;
 3. Dates, times and details of key events, e.g. log-on and log-off;
 4. Device identity or location if possible and system identifier;
 5. Records of successful and rejected system access attempts;
 6. Records of successful and rejected data and other resource access attempts;
 7. Changes to the system configuration;
 8. Use of privileges;
 9. Use of system utilities and applications;
 10. Files accessed and the kind of access;
 11. Network addresses and protocols; and
 12. Records of transaction executed by users in the application.

In addition, ensure that these logs are reviewed and monitored regularly.

Application Security – User Access Management

10. Absence of formal and documented procedures on user accounts management has led to unsecured practices in LOS; exposing the LabDep/Bureau to possible unauthorized access, leakage of confidential information, destruction of data, and other security breach posed by incompatible duties. Further, the agency may also face the sanctions and penalties as a result of non-compliance with the applicable international data privacy laws.

10.1 *Absence of Role Based Access Control (RBAC) resulted in excessive access rights assigned to various users which may have violated the segregation of duties.* According to the LOS administrator, accounts are

²⁰ Sub-clause 12.4.1 of the ISO/IEC 27002:2013(E)

created, and access rights are assigned in accordance with the request of the concerned officer. If access right is not explicitly specified, users are assigned with default access rights which include access to all LOS reports except statistics, and transaction modules.

- 10.2 During system simulation, it was noted that the application's access rights were maintained in the "user administration module." Access to modules is assigned to a user by selecting or checking the box beside each module which is categorized into main modules of Maintenance, Transaction, and Reports. The LOS also has options for "Check if for Viewing Only," "Select All," and "Select Default" for easier assignment of modules access. It was evident that assigning access right was not based on the user's job role but rather individually assigned for each user by selecting the modules.
- 10.3 Though job assignment/designation is provided in the employee profiles table (LOS database), these data are used for human resource purposes and cannot be associated to job roles as these pertain more to job position such as Computer Technician, and Admin Officer, among others. Thus, actual access rights are not based according to these designations.
- 10.4 Analysis of the Users Access table (LOS database) showed that there were users having almost full access to the system (LOS has 119 modules). As a result of this excessive privilege, there were noted activities performed by the System's Administrator that were not commensurate to his job roles such as transactions made on ORMaster, Passports, Request Assistance, and Bank Transactions. These are a clear violation of the segregation of duties.
- 10.5 In today's modern workplace, most if not all-important information and sensitive data are kept on a computer system, readily accessed at any point in time. With RBAC, access to network resources and computer networks such as the LOS will purely be based on the roles assigned to individual agency's personnel. This means that data is not open for all to see/edit/create, and any breaches are more easily narrowed down to the person at fault. For this reason, implementing an effective RBAC system is crucial to data security.
- 10.6 Lack of RBAC resulted in overlapping functions and excessive functions granted to individual accounts which could lead to exposure of sensitive information, data manipulation, and destruction.
- 10.7 ***Non-System Administrators were granted access to the User Administration Module, exposing the agency to the risk of issues in the segregation of duties.*** Through an interview with the administrator and simulation at the test environment, the audit team noted that the User Administration/Account module facilitates the creation of an account, assignment, and revocation of access rights, and resetting/changing of user's password.

10.8 According to concerned personnel, only the designated administrators (i.e. 3 personnel) of the LOS are allowed to use the system’s user accounts administration module. However, data analysis revealed that 29 users have access to the aforementioned module.

No.	MenuName	ModuleID	ModuleName	UserID
1	Maintenance	14	User Accounts	1
2	Maintenance	14	User Accounts	3
3	Maintenance	14	User Accounts	7
4	Maintenance	14	User Accounts	10
5	Maintenance	14	User Accounts	11
6	Maintenance	14	User Accounts	17
7	Maintenance	14	User Accounts	20
8	Maintenance	14	User Accounts	23
9	Maintenance	14	User Accounts	26
10	Maintenance	14	User Accounts	33
11	Maintenance	14	User Accounts	34
12	Maintenance	14	User Accounts	35
13	Maintenance	14	User Accounts	39
14	Maintenance	14	User Accounts	61
15	Maintenance	14	User Accounts	62
16	Maintenance	14	User Accounts	63
17	Maintenance	14	User Accounts	75
18	Maintenance	14	User Accounts	76
19	Maintenance	14	User Accounts	77
20	Maintenance	14	User Accounts	88
21	Maintenance	14	User Accounts	96
22	Maintenance	14	User Accounts	163
23	Maintenance	14	User Accounts	167
24	Maintenance	14	User Accounts	179
25	Maintenance	14	User Accounts	180
26	Maintenance	14	User Accounts	181
27	Maintenance	14	User Accounts	182
28	Maintenance	14	User Accounts	243
29	Maintenance	14	User Accounts	305

Table 1. Users with access to the User Accounts/Administration Module.

10.9 Further review of the audit logs showed that the above non-administrators had performed user administration activities such as account creation, update, revocation or deletion. Samples of these activities performed are provided in *Table 2*:

Audit LogID	Entity	Trans Name	User ID	Remarks
179303	User	Update	11	UserID 11 updated a user account. This user is not among the declared administrators of the LOS.

Audit LogID	Entity	Trans Name	User ID	Remarks
284679	User	Create	20	<i>UserID 20</i> created a user account. This user is not among the declared administrators of the LOS.
186577	User	Update	180	<i>UserID 180</i> updated a user account. This user is not among the declared administrators of the LOS.
1047492	User	Delete	305	<i>UserID 305</i> deleted a user account. This user is not among the declared administrators of the LOS.

Table 2. *Non-administrators who performed user administration activities.*

- 10.10 Having excessive access rights will allow users to perform activities outside their responsibility. These may include creating a dummy account to bypass approval protocol, delete critical information, and perform other actions which are detrimental to the system or to the LabDep/Bureau itself.
- 10.11 ***Unrevoked access rights of separated employees may lead to unauthorized access.*** The existing procedure for revocation of access rights of transferred or separated employee was found to be inadequate. Examination and comparison of LOS user accounts with the provided list of employees revealed that there were 97 active users which access rights need to be revoked.
- 10.12 These users could either be transferred or separated from the LabDep/Bureau as they were no longer found in the list of existing employees.
- 10.13 Unrevoked access rights of resigned/separated employees can be exploited, hence, exposed the agency to unauthorized access that may lead to loss, misuse or leakage of confidential information.
- 10.14 ***Existence of employees/users with multiple user accounts exposed the agency to the risks of possible segregation of duties violation and inability to monitor user activities.*** Data analysis of "Users" and corresponding "Employee" tables (LOS database) revealed that there were instances of multiple User IDs assigned to an employee/user.
- 10.15 Granting of multiple accounts to a single person may result in bypassed functions which by design are segregated in the system. This may also pose difficulty in monitoring user activities that may lead to risks of an undetected security breach.
- 10.16 ***Presence of generic user accounts which may lead to difficulty in accountability enforcement and user's identity determination.*** Generic accounts are typically set up and shared among users with rotating or temporary positions. Setting up these accounts may save the IT personnel's time, but this poses security risks. As generic accounts are mostly untraceable, its use may preclude the agency to trace fraudulent transactions and associate these to a user.

10.17 Analysis of extracted data revealed that there were two (2) unidentifiable generic accounts in the system. Details are shown below:

User ID	User Name	Employee ID	First Name	Last Name	End of Tour
1	Admin	1	ADMINISTRATOR	ADMINISTRATOR	12/31/2020
64	trainee	234	TRAINEE	TRAINEE	12/31/2018

10.18 Existence of these accounts may invite attacks because of its identifiable access rights such as the username of "administrator" or "admin." Thus, the agency was not just exposed to risks of inability to trace and associate fraudulent/unauthorized transactions but also to risks of possible security attacks.

10.19 ***Lack of standard naming convention on user name may preclude the agency to immediately identify perpetrators of malicious transactions.*** During an interview with the LOS administrator, the audit team was informed that the naming convention used in the LOS application is the combination of the user's last name and the initial/s of first name (*e.g. lastnameef*).

10.20 However, analysis of the user names obtained from the "employee profiles" showed that the said naming convention was not observed. There were 132 user names not in *lastnameef* convention.

10.21 As observed, LOS user names do not have a standard naming convention. In addition to implementing unique user IDs, having standard naming convention will help the agency in easily associating transactions to an employee or trace accountability and account identification. Therefore, the lack of it may hinder the agency in identifying the accountable user for unauthorized or malicious transactions.

10.22 ***Accounts with deleted employee profiles and User ID exposed the agency to inability to trace or investigate fraudulent transactions.*** The audit team was informed through an interview that user account becomes inactive once the user's tour of duty expired.

10.23 Review of the entries in the audit log showed that there were 14 deleted user IDs, as shown below:

AuditLogID	Entity	ParentID	Trans Name	User ID	Olo ID
858	User	6	Delete	1	0
1114	User	19	Delete	1	0
105613	User	24	Delete	1	10
1416979	User	431	Delete	1	10
1431138	User	440	Delete	243	10
42858	User	188	Delete	1	0
1410802	User	411	Delete	305	10
6623	User	53	Delete	1	0
22823	User	5	Delete	1	0

AuditLogID	Entity	ParentID	Trans Name	User ID	Olo ID
1047492	User	392	Delete	305	10
1405193	User	425	Delete	305	10
20162	User	153	Delete	1	0
1293664	User	321	Delete	305	10
1293794	User	125	Delete	305	10

10.24 Upon further review of the audit log, it was discovered that there were 170 transactions that were processed by these deleted UserIDs. This deletion of accounts will lead to orphaned transactions or transactions without direct traceable account user/owner. As a result, the agency was exposed to the risk of inability to trace or identify unauthorized transaction such as concealed malicious or fraudulent transactions.

10.25 The absence of enforceable policy and the unsecured practices on user account management exposed the LabDep/Bureau to the risks of unauthorized access, data leakage, system misuse, fraud, other security breach, and data privacy lawsuits which could result to reputational damage.

Recommendations:

10.26 We recommended that Management:

- a. Formulate and enforce user access management policy to address the above-noted security weaknesses;
- b. Evaluate the application security of the LOS, particularly on user account management and consider the following:
 1. Implement RBAC which will regulate access to LOS by only allowing certain authorized personnel to view, edit and create data (sensitive reports, data, user accounts module). In conjunction with RBAC, define LOS access rights and permissions based on personnel's assigned authority and their responsibilities;
 2. Restrict access to user administration module to authorized personnel only and periodically monitor actions performed by these personnel. Also, immediately revoke the access rights of those non-administrators as noted above;
 3. Ensure the immediate revocation of access rights of those employees who are transferred to another division/office or separated from the LabDep/Bureau;
 4. Conduct periodic review and monitoring of Users Access lists to determine those with inappropriate access rights that must be changed and deactivated, and those users with multiple accounts;

5. Enforce accountability by creating a unique user profile for each user and discontinue the use of generic user names, and by setting naming convention for User Names; and
- c. Ensure that there is no duplication of employee's user account by either using the Employee ID as the relative distinguished field or conduct regular checking of multiple accounts.