FINANCIAL AGENCY
INFORMATION SYSTEM AUDIT REPORT

TABLE OF CONTENTS

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

IT GOVERNANCE

1. The attainment of the Financial Institution's (FI) vision to become a one trillion FI by 2022 may be obstructed due to the presence of overdue IT projects that caused by the inadequate strategic planning, deficient Information Systems Strategic Plan (ISSP), and absence of roadmap.

1.1 ***The IT project initiatives were not clearly defined in the ISSP.*** Initiatives must be defined clearly to give the stakeholders an overall idea of what the project is all about. It includes the description/objectives of the project, the funding source and strategy. Review of documents showed that the FI's ISSP did not also show the current IT environment and the developments in place to achieve their vision of becoming a one trillion FA by 2022. By enumerating these initiatives, the FI would have been able to know which area they need to focus on in order to achieve their targets. Instead, the FA only document the general plans for the year 2018 to 2022 and the current projects. The ISSP did not show how these projects relate to their overall vision. Moreover, there is also no diagram of the FI and its business environment that showed its interdependencies with other agencies and its stakeholders. There was also no diagram of the FI's conceptual framework or enterprise architecture which could have shown where the FI was going in terms of its IT Direction.

1.2 Moreover, risk, costs and implications of organizational changes, technology evolution, regulatory requirements, business process re-engineering, staffing and insourcing and outsourcing opportunities in the planning process were not adequately addressed on the ISSP.

1.3 ***Objectives and target outcomes were not specified in the ISSP.*** Metrics were monitoring mechanism that helps management monitor the achievements of the enterprise's business-related goals and IT-related goals. Appropriate metrics help the governing body provide direction that is based on defined goals and an evaluation of metrics[1]. They are also useful for evaluating compliance and process effectiveness and measuring success against established objectives. While outcome is the result of carrying out an activity, following a process, or delivering an IT service etc. The term is used to refer to intended results, as well as to actual results[2]. As a result, details on the hierarchy of outcomes of ICT projects, measurable indicator, baseline data, targets, data collection method and the department responsible for the project were not mentioned on the ISSP.

1.4 ***Initiatives were not prioritized accordingly***. Initiatives should be prioritized according to importance. Initiatives with higher impact on the FA should be considered as top priority. However, both the ISSP and the business case does not show how these initiatives were prioritized. As shown on the FI's ICT Project Portfolio, some projects were beyond schedule and provided by a single contractor. The reasons for the delay as identified by Management were:

[1] *https://www.isaca.org/Journal/archives/2016/volume-6/Pages/performance-measurement-metrics-for-it-governance.aspx*
[2] *ITIL Service Strategy 2011 ed*

a. Key project team members/subject matter experts from e-channel operations were also loaded with tasks on daily operations;
b. Vendor has few resources deployed in for FI Project;
c. COMPETING PRIORITY projects; and
d. Resources also perform system maintenance on modules already implemented.

1.5 ***More than fifty percent (50%) of projects were not on schedule.*** Review of the project health status showed that more than 50% of the projects were considered delayed or beyond schedules. One of the main reasons why these projects were delayed is due to the transition from one Project Manager to another. Likewise, the old practice the FA did is to implement first the project, and then define the process after. Accomplishing the ISSP should also have minimized the effect of the delayed projects since it will give an overall picture of the ICT Projects the FA has in terms of priority, resource allocation, interdependencies of these initiatives and the schedule.

IT projects, when managed improperly, often resulted in late deliveries, cost overruns, or poor-quality applications. Inferior applications can result in underused, unsecure, or unreliable systems. Retrofitting functional, security, or automated-control features into applications is expensive, time consuming, and often results in fewer effective features.

1.6 ***There was no roadmap to indicate relative scheduling and interdependencies of initiatives.*** A roadmap is the development of the time-bound action plan that will provide the instruction on sequence of the initiatives and projects required to close the gaps[3]. Although a roadmap is required only on a case-to-case basis, the FI should consider its benefits. A roadmap can define a clear direction for all of the FI's projects. This is especially useful considering that projects do sometimes rely on the completion and success of other projects. The delay of one is the delay of all. This is also to give the FI an over-all picture of what were their plans and how these plans connect to each other. A roadmap could have given management clear visibility of its stumbling blocks and the obstacles hampering its smooth travel on the "road". Right there and then, decisions could have been made to address them.

Recommendations

1.7 We recommended that the Management evaluate the need to adopt the following:

a. Evaluate how effectively the IT strategies have been integrated and aligned within the FI's goals for delivering value;

b. Collect relevant, timely, complete, credible and accurate data to report on progress in delivering value against targets. Obtain a concise, high-

[3] *ITIL Service Strategy 2011 edition*

level, all-around view of portfolio, programmed and IT (technical and operational capabilities) performance that supports decision making, and ensure that expected results were being achieved;

c. Obtain regular and relevant portfolio, programmed and IT (technological and functional) performance reports. Review the FI's progress towards identified goals and the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risk mitigated;

d. Define a balanced set of performance objectives, metrics, targets and benchmarks. Metrics should cover activity and outcome measures, including lead and lag indicators for outcomes, as well as an appropriate balance of financial and non-financial measures. Review and agree on them with the IT and other business functions, and other relevant stakeholders;

e. Create a road map indicating the FI's future plans alongside its targets, schedule and the interdependencies of the projects.

INFORMATION SECURITY

Logical Access Controls

2. The information security policies of the FI have not been updated since June 2014. Also, logical access controls deficiencies were observed that exposed the FI to the risks of loss and leakage of data and information, unauthorized access and data modification, denial of service and potential legal risks if unaddressed.

2.1 ***The information security policy was not reviewed and updated since 2014.*** The purpose of the information security policy was to define principles to which all FI employees and third parties must adhere to when handling information owned by or entrusted to FI in any form. The principles cover the following areas:

- Defining the confidentiality, integrity and availability requirements for information used to support FI's objective;
- Ensuring that those requirements were effectively communicated to individuals who come in contract with such information;
- Using, managing and distributing such information – in any form, electric or physical – in a manner consistent with those requirements.

2.2 The policy itself clearly stated that "This Information Security Policy shall be reviewed by FI management at planned intervals, and/or significant changes to the policies, standards, guidelines and procedures for any changes affecting the basis of the risk assessment".

2.3 The outdated information security policies, and its non-compliance with

the current legal requirements, expose the FI to the risks that significant organizational or technical changes, new vulnerabilities and security incidents may not be addressed. These will adversely affect the effectiveness of the policy and the control requirements thereof.

2.4 ***Ten (10) users of GL system were given more than one access role.*** There were two types of access roles in the GL: "clerk" and "visor". These roles were created to segregate the access rights of users to be commensurate to their actual duties and responsibilities. Analysis of GL users disclosed that some employees had more than one active access role, it was either a combination of "clerk" and "visor" or two of each. Hence, the objective of role-based access was not achieved if both roles will be given to one and the same user.

2.5 There were eight accounts in the GL system that still active even after the users were separated from the FI. Likewise, 55 dormant or obsolete user accounts were still active in other system. While the application under audit is the GL system, it has come to our attention that there were numerous user accounts that have no login records or not used for more than 90 days but were still active in various system of the FI.

2.6 ***The user access request forms (UARFs) were not properly accomplished.*** Before a user be given access to the services and applications, a UARF is filled out by a requesting employee and should be submitted to the immediate supervisor for review and endorsement/recommending approval. Thus, approval is indispensable. However, examination of six UARFs disclosed the following exceptions:

a. One UARFs for GL revocation was not approved. Likewise, four UARFs application for services other than GL were also not approved prior to submission to Service Desk.

b. The IT Service Desk did not sign the receipt portion of said UARFs. Although, it is not explicitly stated in the UAMP said part of UARFs is

c. Also, the Information Asset Custodian (IAC) information portion of the User Access Request Form was not appropriately filled-up by concerned personnel.

Recommendations:

2.7 We recommended that the Management evaluate the need to adopt the following:

a. Ensure periodic review and update of the information security policies and related procedures to include those requirements and/or changes issued by the legislative and regulatory bodies that might affect the FI's Information Security Management System

b. Ensure the regular review of users' access rights and revoke the access

rights of all dormant and inactive user accounts in all FI application systems, in accordance with FI policies and procedures; and

c. Evaluate the current format of the UARF. Consider the acknowledgement of Acceptable-Use Policy and other relevant logical access policies by the users for their awareness.

Network Security

3. The lack of established guidelines and procedures in network monitoring, inconsistent and inadequate network security practices, absence of warning banner in core switches, and non-conduct of regular vulnerability assessment and penetration testing exposed the FI to the risks of disruption of operations, disclosure of sensitive information, violation of regulatory requirements and loss of customer confidence that may affect the delivery of services to the public.

3.1 ***There were no established guidelines and procedures in network monitoring.*** Network monitoring is a computer network's systematic effort to detect slow or failing network components, such as overloaded or crashed/frozen servers, failing routers, failed switches or other problematic devices. In the event of a network failure or similar outage, the network monitoring system alerts the network administrator (NA)[4]. Interviews with the Network Management Department revealed that they use SolarWinds as their monitoring tool for network availability. The NA in charge revealed that no manual or documented procedures for such activities were established. They also revealed that they create a monthly utilization report manually which will be submitted to the ICTMG Head upon completion thru electronic mail. This process is difficult, time consuming and may generate inaccurate reports.

3.2 Under Item 3.7 of the ITILv3 framework, "Documentation activities include establishing their own technical procedures manuals. These must be kept up to date and new material must be added as it becomes relevant, under change control." The point of establishing and documenting standard procedures is not just for the sake of fulfilling documentation requirements. Without established procedures, the process of diagnosing technical issues, resolving faults, and generating reports will not be consistent and as effective and may even take longer to perform. In effect, this may produce downtime and service interruptions to the FI's system.

3.3 ***Use of TELNET protocol in administration of core switches.*** TELNET is an application layer protocol providing "a bidirectional interactive text-oriented communication facility using a virtual terminal connection" to connect to someone else's computer. In short, you use a program to console (not an MS RDP-type console, but running a "command prompt" type connection) into a remote computer[5]. On the other hand, Secure Shell, or Secure Socket Shell (SSH) is a cryptographic protocol and interface for

[4]*Definition from https://www.techopedia.com/definition/24149/network-monitoring*
[5]*Definition from https://searchnetworking.techtarget.com/definition/Telnet*

executing network services, shell services and secure network communication with a remote computer. Secure shell enables two remotely connected users to perform network communication and other services on top of an unsecured network. There were reported exploits that may allow any infiltrator to gain access, issue DOS and possibly execute a code where it can flood the port[6].

3.4 Review of the core switch configuration of the FI showed that TELNET and SSH were used as transport protocol for core switches administration/maintenance. TELNET transmits login information (username and password) to the client in clear text. This allows intruders to obtain sensitive login information by sniffing on the network. This exposes the FI to the risk of theft of login credentials. CS No. 2.12 of FI's Switch Minimum Baseline Security Standards (MBSS) and Implementation Procedures Version 2.0 provides implementation procedures in utilizing session encryption. It states that the FI *"Use secure protocols whenever possible. A secure protocol choice includes the use of SSH instead of Telnet so that both authentication data and management information were encrypted. In addition, you must secure file transfer protocols when you copy configuration data. An example is the use of the Secure Copy Protocol (SCP) in place of FTP or TFTP."*

3.5 It is worthy to note that, as per Request for Change (RFC) Ticket No. 083118181, a request to disable the TELNET protocol was already requested on September 4, 2018. Disabling was approved on September 18, 2018 which remediates the issue.

3.6 ***No established warning banners in core switches.*** A widely used method for computer access is the use of warning banners. Warnings were an effective tool for providing adequate notice regarding the obligations and responsibilities entailed with using the server and networking environments.[7] It was observed that warning banners were not present in both of its core switches. The banner that is present in one core switch is only a reminder to users who successfully log on to the switch. This apparently disregards CS No. 2.1 of FI's Switch Minimum Baseline Security Standards and Implementation Procedures Version 2.0 that states that *"Display warning banners before and after users log onto the switch. The banner should not contain any specific information about the device name, model, software, or ownership. This information can be abused by malicious users. For example, a banner can provide some or all of this information:*

- *Notice that the system is to be logged into or used only by specifically authorized personnel and perhaps information about who can authorize use.*
- *Notice that any unauthorized use of the system is unlawful and can be subject to civil and criminal penalties.*
- *Notice that any use of the system can be logged or monitored without*

[6]*Definition from https://www.techopedia.com/definition/4127/secure-shell-ssh*
[7]*Definition from https://www.cybrary.it/study-guides/purpose-use-and-examples-of-warning-banners/*

further notice and that the resulting logs can be used as evidence in court."

3.7 Without these security banners, users or other entities trying to access the network will not be adequately informed as to the rules surrounding the use of critical network devices. This may result in an improper configuration on the devices or worse, exploitation of the network regardless of whether it was done intentionally or not.

3.8 ***Non-conduct of regular vulnerability assessment and penetration testing (VAPT).*** Reviewed of the report on the results of the last vulnerability assessment conducted on February 2016 revealed that some IP addresses passed and some failed the compliance test made by the certified assessor. However, these failed results were not verified if mitigated since the last scan report expired on May 2016 and since the vulnerability assessment and penetration testing have not been redone since then.

3.9 As threats continue to evolve rapidly and increase in sophistication, Management should ensure that threat monitoring and vulnerability scanning tools and processes remain effective in identifying both known and unknown (zero-day) security exposures. Without regular conduct of VAPT, thus, leaving security vulnerabilities unresolved, there is a risk that the IT infrastructure is not sufficiently secured. As a result, this can lead to severe monetary losses, and the loss of customer confidence when data is breached.

Recommendations:

3.10 We recommended that the Management evaluate the need to adopt the following:

a. Establish, maintain and disseminate a standard set of approved network monitoring guidelines and procedures that is reviewed and updated on a regular basis;

b. Ensure that secured protocol will be used as the remote login protocol instead of TELNET, as this builds the risk of leaking out administrative credentials due to the protocol being unsafe;

c. Establish Security/Warning banners without information about network devices, as well as to advise the authorized users of their accountability and to warn those trying to exploit the FI's network; and

d. Implement and regularly conduct vulnerability assessment and penetration testing, at least annually, in compliance with relevant regulatory bodies.

Data Center – Physical and Environmental Security

4. The implemented physical, environmental and administrative security controls to protect FI's critical information processing facilities from unauthorized access, loss, theft, damage and environmental threats were inadequate and fragmented, with adequate controls in some areas, and deficient controls in other areas thereby exposing the agency to the risk of loss of data and equipment, unnecessary financial losses, interruption of IT services and operational difficulties that in turn may have a disadvantageous effect on the achievement of the FI's business objectives.

4.1 ***The policy and procedures for providing access to the data center were not regularly updated.*** Currently, the FI implemented the I.T. Computer Center Access Control Policy and Procedures under Department Order No. 12-001 dated September 12, 2012. It was noted during our review of the policy that it had not been updated since that date. New security procedures being practiced today were not reflected on the department order such as requiring employees to seek the approval of the Data Center head through a User Access Request Form (UARF) prior to being given access to the data center. From a security standpoint, implementing these new security procedures without waiting for policy updates is preferable over policy provisions that were existing but not being complied with. However, without policy support, any new procedures being performed that is not in line with the existing policy may be construed as violations or excessive practice of authority. The periodic review and update of policies and guidelines is important in order for the Data Center security to be in line with latest security trends and to standardize the requirements in providing proper data center access.

4.2 ***Insufficient physical access controls inside the data center.*** The FI installed a multi-factor authentication system – a biometric access system with a proximity card facility at the main data center entrance for its enhanced protection. A multifactor authentication system[8] (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target. However, upon inspection, only a proximity card (which is a single factor authentication) is used when entering the data center. Further, the FI uses a manual sliding door with magnetic locks to access separate secured areas inside the Data Center. These sliding doors did not automatically close and were thus a security risk.

4.3 Review of the sample CCTV recordings showed that the supposedly secured doors of the data center were open for an extended period of time.

[8] *https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA*

This usually happens during night shift as employees leave the door open for air circulation. Interviews with Data Center Management (DCM) personnel disclosed that they advised the employees to leave the door open because the central air conditioning system is turned off at 4:30 PM during weekdays and all-day during weekends. The inadequate physical access controls increase the risk of unauthorized access to the data center and consequently, the sensitive resources and data it contains.

4.4 ***Defective magnetic door locks in sensitive areas.*** Inspection revealed that two magnetic locks leading to the TelCo room and Media library were not working. This would lead to unauthorized personnel to access a secured area especially if the area is not monitored by a CCTV. The affected doors have been reported and have been repaired.

4.5 ***Time in the biometric systems were not synchronized.*** Item No. 2.2.7 of the FI Biometric System Minimum Baseline Security Standards (MBSS) states that**: "**Biometric System should be kept in sync with a time synchronization mechanism of the FI." It was observed that the time display in the biometric displays were not in sync. This may lead to the incorrect capture of biometric data during incidents and inconsistencies when reviewing Data Center access logs. The Data Center personnel has been immediately notified and incident has been immediately remediated and re-synced.

4.6 ***Employee's Quarter inside the Data Center.*** Beside the media library, a room intended for Data Center Operators is located inside the Data Center. The quarters include lockers where employees can store their personal belongings inside the Data Center. Inspection of the quarters revealed the presence of combustible materials such as a tire, foams and a rechargeable lamp. Combustible materials inside a data center increases the risk of fire and should be stored in a location far away from the data center.

4.7 ***Inadequate number of CCTV cameras to view critical areas in the data center.*** Item 11.1.2 (e) of ISO 27002:2013 states that: "external party support service personnel should be granted restricted access to secure areas or confidential information processing facilities only when required; this access should be authorized and monitored". The FI uses multiple CCTV cameras to monitor the activity inside the Data Center. However, the TelCo room of the Data Center did not have a camera inside. Therefore, activities of personnel working on the network equipment and those who were entering and exiting the TelCo room cannot be monitored remotely nor recorded.

4.8 ***Insufficient review of the CCTV recordings.*** An adequate number of CCTV cameras viewing all critical areas is important for data center security. But what's more important is the review of the CCTV recordings, not only for monitoring and audit, but also to detect deficiencies in security and compliance. Based on interviews with the Security Service Unit (SSU), it was revealed that review of CCTV recordings was not regularly conducted but only done when requested by personnel or a

department. This request should be approved by the head of Physical Security Office (PSO). Reports of the request were kept confidential between the SSU and the requestor. Due to the infrequency of this review activity, there now exists a palpable risk that some violations of security protocols by personnel may have escaped detection.

4.9 ***Preventive maintenance for the fire suppression system was lax.*** The FI installed FM-200[9] and handled fire extinguishers inside the data center as their fire suppression system. However, the monthly maintenance fire suppression reports were not written legibly and not detailed enough to include the scope of work that was done. It was also noted that the FI did not have a formal checklist of procedures to be performed during preventive maintenance. Knowing that the cost involved in procuring and refilling an FM-200 system is high, it is paramount that proper care and conservation should be observed. More so, this is to prevent the happening again of the accidental activation and discharge of the FM-200 agent even without fire. The absence of a formal checklist may deter the FI from ensuring its good working condition and may lead to its failure to activate in case of fire. In contrast, it might also incur additional expense for the FI in case of its undue activation. Minimum contents of the checklist for preventive maintenance may include inspection of the cylinders, pressure gauge, hoses, actuating components and electricals.

Recommendations:

4.10 We recommended that the Management evaluate the need to adopt the following:

a. Assess whether existing policies and procedures on physical security need to be strengthened, reviewed, updated and strictly implemented based on the latest risk assessment made by the FI and the practicality of its implementation;

b. Improve the physical access controls, such as implementing a genuine multi-factor authentication control and an alarm for doors opened for an extended period of time;

c. Include in the shift report the monitoring of magnetic locks and time synchronization;

d. Install additional CCTV cameras to eliminate blind spots inside the data center and conduct regular CCTV reviews to monitor the security compliance and deficiencies inside the data center;

e. Evaluate the necessity of an employee's quarter inside the data center as against the security risks it introduces to the FI. The FI can provide for employees' needs for a good working environment especially those

[9] *An FM-200 is a waterless, non-toxic fire protection system that is discharged within 10 seconds and suppresses the fire immediately.*

working for night and weekend shifts without unnecessarily violating the FI's security policies.

f. Assess the need of having a formal checklist showing the detailed work done for the conduct of preventive maintenance to the fire suppression system and conduct periodic preventive maintenance of the fire suppression system to make sure that it is in good working condition to avoid unnecessary incidents that may cost the FI.

Database Security

5. The FI's GL database was vulnerable to various security threats due to the outdated Oracle minimum baseline security standards (MBSS), use of unsupported database and inadequately set security configurations as shown by multiple instances of excess privileges being granted to users, lenient policy enforcement and weak password configuration.

5.1 ***The FI Oracle Minimum Baseline Security Standards (MBSS) and Implementation Procedures v2.0 document was not updated and reviewed since 2014***. Review of the document revision history revealed that the Oracle MBSS had not been updated since June 6, 2014. The MBSS also clearly states that it *"shall be reviewed annually and an update by the FI may occur earlier if internal or external influences affect its validity."*

5.2 The outdated MBSS, and its nonconformity with the current legal requirements, exposes the FI to the risks that significant organizational or technical changes, new vulnerabilities and security incidents may not be addressed. This will adversely affect the effectiveness of the policy and the controls requirements thereof.

5.3 ***The GL system was using an unsupported version of Oracle database.*** Assessment of the database revealed that the FI is using Oracle database version 10.2.0.4.0 for the GL system. Likewise, quarterly application of critical patch updates was not applied. According to the Oracle Lifetime support policy[10], extended support for Oracle 10g ended in July 2013. The reason for using Oracle 10g is due to the dependency with the application. The GL has not been updated or changed since its installation and is already due to be replaced with the Integrated Core Financial Solution (ICFS) which is still currently under development. Having an updated database helps in safeguarding stability and security of information. Application of critical patches also helps in securing against vulnerabilities. Failure to remain aware of the security weaknesses and to address them could result in loss of data integrity or data theft.

5.4 ***Oracle sample data and users were not removed.*** Oracle sample schemas come pre-installed with an Oracle database. They were commonly used for training purposes and have their own preset authorizations and default

[10]*Oracle Lifetime Support Policy, http://www.oracle.com/us/support/library/lifetime-support-technology-069183.pdf*

credentials. From a security perspective, these were seen as threats because their default configurations were known publicly and can thus be used by anyone who knows the configurations, even those outside the FI. These sample schemas include Human Resources, Business Intelligence, Order Entry and others. Review of the GL database revealed that the database still has the sample Oracle users SH, HR, OE, PM, IX and BI in its user list. But though this was the case, further verification revealed that these accounts were already expired and locked, consistent with Item No. 2.11 of the FI Oracle MBSS which stated that *"Default user accounts installed with the database were disabled or removed if not required."*. While database personnel have applied the appropriate action for these accounts by disabling them, both the CIS security benchmarks and FI's own Oracle MBSS recommend that these users be removed if not required in the production database. The sample data is typically not required for production operations of the database and provides users with well-known default passwords, particular views, and procedures/functions. If not removed, such users, views, and/or procedures/functions could be used to launch exploits against production environments.

5.5 ***Database users can infer confidential data that they don't normally have access to by taking advantage of their privileges.*** Normally, an Oracle database user who did not have SELECT privilege on a database table, cannot view the contents of that table. However, there is still a way to guess the contents if the user has UPDATE or DELETE privileges. For example, if a malicious user wants to determine if a certain username exists in a user table but did not have access to view the user table, he/she may do so by guessing or inferring the username in the WHERE clause of a DELETE statement or a SET clause of an UPDATE statement. If the user guesses the value incorrectly, then the statement will produce an error. But if the user guesses the value correctly, then the statement will produce a message indicating the successful execution of the statement, thereby confirming the user's guess. Equipped with this information, the user can now update the other data fields pertaining to the username he/she is referencing. If the user table happens to be an application's reference for authentication and contains a password field, then the malicious user can now modify the password of the username he/she is referencing and subsequently take over the account. This is a crude tactic but is recognized by Oracle security experts as a real risk to confidentiality so they have developed the SQL92_SECURITY parameter to thwart such attempts. The SQL92_SECURITY parameter requires a user to have SELECT privilege on a column in order to reference it in the WHERE clause of a DELETE or UPDATE statement or on the right hand side of a SET clause in an UPDATE statement. However, in a review of the security settings of the GL database, the SQL92_SECURITY setting is turned off.

5.6 ***Two (2) Profiles have consistently failed the CIS benchmark test and/or violated internal policies, hence all users belonging to these profiles put the security of the GL database at risk.*** FI's MBSS for Password and Login Control stated that *"Except for application and process accounts, passwords must be changed at least every forty two (42) days. Password of*

system and security administrative accounts and other user accounts deemed as powerful must be changed at least every thirty (30) days." Below is a summary of the four profiles that failed the test:

Table No. 1 – DBA_PROFILES that failed the CIS benchmark test

CIS Benchmark Requirement where the Profile failed	Profile Name	
	'DEFAULT'	USERS
PASSWORD_LOCK_TIME is greater than or equal to '1'	X	X
PASSWORD_LIFE_TIME is less than or equal to '90'	X	
PASSWORD_REUSE_MAX is greater than or equal to '20'	X	X
PASSWORD_REUSE_TIME Is Greater than or Equal to '365'	X	
PASSWORD_GRACE_TIME' should be less than or equal to '5'	X	X
PASSWORD_VERIFY_FUNCTION' should be set for all profiles	X	
SESSIONS_PER_USER should be less than or equal to '10'	X	X

5.7 ***Weak database user password settings increased the likelihood of success for brute force password attacks.*** Layered security controls were one of the best information security practices. In the event that a control fails, a compensating control will be activated to prevent a security incident. Should the compensating control fail, another control will take its place, and so forth. As observed in this assessment, the database user accounts belonging to the above noted profiles were susceptible to brute force attacks and other forms of attacks that try to compromise a password. If the database fails to lock out these users after multiple failed login attempts, then the password's security settings should at least make it difficult for the attacker to succeed.

5.8 The lack of an appropriate cap for the number of concurrent user sessions increases the likelihood of Denial-of-Service (DOS) attacks. The CIS benchmark recommends a cap of at most 10 allowable concurrent sessions per user and for a good reason. Each session consumes memory resources and if left uncontrolled, can lead to memory resource exhaustion. This can then lead to the bigger problem of a DOS attack that targets the availability of data and services. In a DOS, the available resources can no longer support the load leading to a service interruption or even a crash. As observed in the analysis of database profiles, all of the database users have either unlimited or default caps for user sessions thereby heightening the risks to availability.

5.9 ***Multiple powerful packages that may potentially be misused have been granted to the 'PUBLIC' role by default but had not been revoked, thereby heightening the risks of data leakages and unavailability.*** According to the Oracle Database Security Guide[11], some of these packages were so powerful and have the potential to be misused that Oracle intends to revoke such privileges from the 'PUBLIC' role in subsequent releases. The CIS agrees to this and had also recommended the

[11] Oracle Database Security Guide, Security Policies, https://docs.oracle.com/cd/B19306_01/network.102/b14266/policies.htm#DBSEG7000 (last accessed November 21, 2018)

revocation of such privileges from the PUBLIC role unless absolutely necessary. Oracle recommends that these privileges be granted only to those applications that need to use them:

Table No. 2: Powerful packages that may potentially be misused

Package	Risk
DBMS_ADVISOR	Allows direct file system access, it can be used by an attacker to interact with the file system, outside of the database.
DBMS_JAVA	Allows an attacker to run operating system commands from the database.
DBMS_JAVA_TEST	Same with DBMS_JAVA_TEST
DBMS_JOB	Allows an unauthorized user to disable or overload the job queue
DBMS_LDAP	Used to create specially crafted error messages or send information via DNS to the outside
DBMS_LOB	Allows an unauthorized user to manipulate BLOBs, CLOBs, NCLOBs, BFILEs, and temporary LOBs on the instance, either destroying data or causing a Denial-of-Service condition due to corruption of disk space
DBMS_OBFUSCATION_TOOLKIT	One of the tools that determine the strength of the encryption algorithm used to encrypt application data and is part of the SYS schema.
DBMS_RANDOM	Used to encrypt stored data. Generally, most users should not have the privilege to encrypt data since encrypted data may be non-recoverable if the keys were not securely generated, stored, and managed
DBMS_SCHEDULER	Allows an unauthorized user to run database or operating system jobs.
DBMS_SQL	May be used by user to escalate their privileges through cursor snarfing and cursor injection.
DBMS_XMLGEN	An attacker can exploit this package with SQL injection. All data, including user credentials can be extracted from the database.
DBMS_XMLQUERY	May be used to search the entire database for critical information like credit card numbers and other sensitive information.
UTL_FILE	Allows user to read files at the operating system. These files could contain sensitive information (e.g. passwords in .bash_history).
UTL_INADDR	Can be used to create specially crafted error messages through SQL injection or send information outside via the Domain Name Service
UTL_TCP	Permits outgoing network connections to any waiting network service which then allows unauthorized transmittal of data to outside networks.
UTL_SMTP	Used for email exchanges. This can be used to leak confidential information or perform a DOS attack using junk mail and network saturation.
UTL_DBWS	Allows unauthorized user to corrupt the HTTP stream used for carry the protocols that communicate with the instance's web-based external communications
UTL_HTTP	Allows the database server to request and retrieve data using HTTP, i.e. it could be used to send sensitive and confidential information to external websites without proper authority

Source: *Oracle Database Security Guide, CIS*

5.10 Review of the database security configurations disclosed that all of the above packages can be executed by the 'PUBLIC' role. Other powerful

packages such as the UTL_FILE that could allow a user to read operating system files that contain sensitive information (e.g. passwords in .bash history) can also be executed by the 'PUBLIC' role. And considering that this role is available to ALL database users, then there is a likelihood and risk that all database users can exploit these privileges.

5.11 ***There was no logging of attempts to alter the database audit trail which could compromise its integrity.*** The SYS.AUD$ table provides the database audit trail and is open for read/update/delete/view. This table is a common target for malicious users who wish to delete any trace of their activities in the database. It is essential that the audit trail be protected from unauthorized users as it could provide the best forensic evidence of any wrong doing. Any attempt to alter the SYS.AUD$ table should be logged and reviewed from time to time. In the review of the security configurations of GL database, it was revealed that the logging of these attempts is not enabled. Hence, the FI would not be able to establish any pattern of unauthorized activities directed at manipulating the database audit trails. In the event that a security incident occurs, FI will be unable to pin down the perpetrators if they were able to successfully erase all trace of their presence in the FI's systems.

Recommendations

5.12 We recommended that the Management:

a. Ensure periodic review and update the MBSS to include those requirements and/or changes issued by the legislative and regulatory bodies that might affect the FI's database management systems

b. Regularly conduct database security assessments using IT security and best practice tools such as the CIS benchmark and initiate corrections based on the results of such assessments and the resulting recommendations;

c. Drop any test schemas such as those that came with the Oracle installation package for training purposes if these schemas were not being used;

d. Update existing policies and procedures to specify rules that will be appropriate for privileged, administrative and "super user" accounts;

e. Strengthen the database password configurations for each user role and profile, prioritizing security over convenience especially for powerful accounts. Human users in general should not have 'unlimited' password privileges;

f. Set an appropriate cap or resource limit that each DBA_PROFILE is allowed to have taken into consideration what is needed to perform the respective functions of those belonging to such profiles;

g. Revoke any excessive privileges provided to a role or profile; and

h. Considering the needs and resources of the FI, enable database audit options, which will allow adequate and proper recording of critical database user activities especially those of the privileged user accounts.

IT OPERATIONS

Problem and Incident Management

6. The timely resolution of incidents could be delayed due to insufficient prioritization criteria which may result in service requests backlog and problems in meeting business needs. Similarly, the inadequate design and improper implementation of guidelines and procedures on escalation, status monitoring and tracking may affect delivery of services to critical business operations which may result in unmet quality of service to the stakeholders.

6.1 ***Insufficient criteria for prioritization of service requests from high-ranking officials.*** DSS02.02 of COBIT requires to 'Identify, record and classify service requests and incidents, and assign a priority according to business criticality and service agreements. Observation of daily transactions of IT Service Desk revealed that service requests from high-ranking officials were prioritized without taking into consideration the severity or impact of the request. Analysis of the generated report of closed tickets from ITCLS revealed that there were 105 service requests from high-ranking officials have a prioritization of 'High' regardless of the severity. This prioritization may be beneficial to the FI but review of incident management policies showed no details about the specific prioritization given to high-ranking officials.

ITIL v3 has stated a guideline on how to address 'VIP' requests: '*Some organizations may also recognize VIPs (high-ranking executives, officers, diplomats, politicians etc.) whose incidents would be handled on a higher priority than normal – but in such cases this is best catered for and documented within the guidance provided to the service desk staff on how to apply the priority levels, so they were all aware of the agreed rules for VIPs, and who falls into this category. A better practice would be to formally recognize VIP priorities as an additional service option (the 'gold' level of service, for example) that is documented as part of the service catalogue tied to differentiated service levels.'* Without a more ostensible and appropriate prioritization criteria for high-ranking officials, there may be delays in addressing of other high priority incidents and may make IT unable to meet business needs.

6.2 ***Resolution of service requests were either delayed or still pending.*** DSS02.07 of COBIT states that an organization should "Regularly track, analyze and report incident and request fulfilment trends to provide information for continual improvement." This statement was supported by ITIL: "Incidents should be tracked throughout their lifecycle to support proper handling and reporting on the status of incidents."

6.3 Analysis of "ITCLS' Transaction Listing of All Pending Tickets" report revealed that there were tickets which were pending for more than 1,000 days. Detailed information on the reason of the delayed tickets was not indicated in the report. Interview with the Head of Service Desk revealed that a system issue is most likely the reason why the delayed tickets from 2015 were already closed but were still appearing in the pending tickets report being generated by ITCLS. Updating the ITCLS to correct this issue was not done since the developers of ITCLS were already resigned and the FI is already in the process of procuring a ticketing system which is more functional than ITCLS. Management also revealed in the interview that some pending tickets have been closed a few months ago but the person-in-charge overlooked it in the ITCLS.

6.4 The correct ticket status cannot be confirmed in ITCLS due to system issues and human errors. The above observations could have been avoided if the ICT Group's effort in monitoring all tickets were sufficient. Lack of monitoring of service requests and incidents is evident during our analysis of ITCLS reports and most likely the root cause of the delayed resolution and backlogs.

6.5 Moreover, analysis performed on the "ITCLS Closed Tickets" report found that 76 "High" and 290 "Medium" priority tickets did not meet the required resolution time and service level stated in the FI's MOP-I.390.2 which is within five (5) days. As common with the other tickets, no remarks portion was filled nor is a resolution in the generated report sufficient for future trend analysis and other incident management activities for continual improvement.

6.6 High priority tickets can be considered as 'Major' incidents that needs immediate attention before it could cause more harm to the operation or the business as a whole. As described by ITIL, *'major incident is the highest category of impact for an incident. A major incident results in significant disruption to the business.'* It is therefore a must that high priority tickets should be focused on and handled with urgency at all times.

Recommendations:

6.7 We recommended that the Management:

a. Determine the root cause of ticket delays and ensure continuous improvement of the Incident Management process by conducting activities like post-incident reviews, Incident Trend Analysis and regular review of Incident Categorization among others on a regular basis. Communicate the results of the Incident Management activities/efforts to the Management Committee.

b. Define more appropriate prioritization criteria for all VIP service requests that considers impact, urgency, cost, benefits and risk

exposures without compromising the existing incident prioritization process of IT Service Desk; and

c. Integrate sufficient guidelines and procedures on Incident Tracking, Monitoring and Escalation into the existing Incident Management process taking into consideration the SLA parameters.

Change Management

7. **The existing Change Management Policies and Procedures was inadequate due to the absence of remediation procedures for unsuccessful changes, thereby exposing the FI to various business risks such as unauthorized changes, increase in the number of application-related incidents, disruptions, delays due to rework and misalignment of IT with business needs.**

7.1 ***There were no approved remediation procedures for unsuccessful changes.*** Item 4.2.5 of ITIL states that, "No change should be approved without having explicitly addressed the question of what to do if it is not successful. Ideally, there will be a back-out plan, which will restore the organization to its initial situation." This is consistent with the requirement of the standard, ISO 20000-1 which states that, "The change management process shall include the manner in which the change shall be reversed or remedied if unsuccessful." In our perusal of the FI's change management policies and procedures, we determined that the FI did not have a formally established remediation plan in case where a recent change request is unsuccessful. This is not to say however that they will do nothing in such cases, as AMD personnel stated in our interview that they do have an unwritten plan or procedure if in case this occurs.

7.2 The fact however that these procedures were neither formalized nor sanctioned by top management means that the procedures can be arbitrarily changed depending on the intentions and competence of the person performing the procedure. Past mistakes in the conduct of rollback procedures may be repeated and confusion as to authorization may arise as there is no single guidance on the conduct of the procedures. The likeliness of this occurring is higher when the employee performing the procedure is new to the idea or had not previously undergone simulations or trainings on the back-out plan.

Recommendation:

7.3 We recommended that the Management evaluate existing procedures and formalize rollback procedures for unsuccessful changes. These procedures shall be tested from time to time especially when changes were made to the rollback procedures itself.

CONTINUITY PLANNING

8. The ability of the FI to continue the operations of its critical IT systems in case of major interruptions was in doubt due to outdated Business Continuity Plan (BCP) of critical business units (BUs), non-conduct of the annual FI-wide BCP testing and non- dissemination of the DRP manual to all authorized personnel.

8.1 ***The Business Continuity Plan for some business units were not updated.*** The FI conducts an activity known as Business Impact Analysis (BIA) that documents the prioritization of business functions/processes based on the assessed financial impact of disasters or incidents and the service level commitments to customers, counterparties and other stakeholders. According to the FI's BCM Program Manual, section II.200 - Business Continuity Management Policy on Recovery Strategies / Preventive Controls (BCP*): "The plan should be reviewed for accuracy and completeness by respective business units at least annually or when there were significant changes to organizational structure or any part of the plan, system, business processes or resources used for recovery procedures."*

8.2 The audit revealed that the BCP of the Remittance Department, Transaction Processing Department and Trust Financial Institution Group was not updated since 2016. The table below showed departments with outdated BCPs along with a description of their critical functions:

Table No. 3: Departments with out-of-date BCP

Department	Critical Functions
Remittance	Processing of FX (funding) transactions Updating of FX buying rates Processing of remittance transactions
Transaction Processing	Processing of release instructions and posting of collections Booking and servicing of Domestic Borrowings
Trust Financial Institution Group	Confirmation of maturities Canvassing of rates Collection and Issuance of OR for fresh fund

8.3 It was disclosed that the FI is in the process of re-organization and there were a lot of changes. The effectiveness of the BCP during disruption cannot be assured on these three critical business units due to the following outdated information:

- Disaster Declaration Process;
- Call Tree;
- Accountability, Roles, Responsibilities and Authority;
- Notification, Invocation and Escalation during emergencies;
- Evacuation Procedures;
- Implementation of Critical Activities;
- Recovery and Resumption Logistics;
- Recovery Action Plan;

- Contingency Measures; and
- Recovery Resource Profile

8.4 Important provisions in the BCP and DRP must always be updated to reflect the current changes in the organization and ensure FI's readiness in times of disruption. Updated BCP and DRP will provide reasonable assurance that normal operations will resume in a timely manner and minimize the impact of the disruption within the agency. Having an outdated BCP will only be to the disadvantage of the FI. Not only will the agency be exposed to the risks associated with the continuity of operations, it will also expose itself to legal and regulatory risks due to its non-compliance with pertinent laws and regulations.

8.5 ***Annual conduct of FI-wide BCP testing was not regularly performed.*** It was learned that a functional BCP testing was conducted in August 2018 by the BCP team for the Clearing Department. A functional Drill/Parallel Test is one of the testing methods performed by the CBSFIs. The results of the functional test showed result of "needs minor improvement (NMI)" due to the reason that the "access to CICS Module" activity came as minor problem but was immediately corrected by the IT personnel on BCP site. Minutes of meetings conducted after the functional test revealed that this was done in preparation for the full scale, FI-wide test scheduled in September 2018. Inquiry with ORMD personnel revealed that the schedule originally stated on the functional test result was only tentative and was not approved by the management. The official schedule for the FI-wide BCP testing was supposed to be in November 2018 but was already postponed due to insufficient test plans on how to deal with the criticality of the End-of-day processing for the core systems like the NIDSS. It is worthy to note that currently, they have initiated activities in preparation for the next FI-wide BCP testing like meeting with the critical Business Units and preparing their BCP test scripts, inspecting the DR site and Backup site, and preparing the list of skeletal personnel for the BCP testing.

8.6 Having an updated BCP is good but BCP testing is also equally important. Without regular testing, there is no assurance that the plan will work when an actual debilitating scenario did occur. Management will not be able to identify areas in the plan that need further discussion and improvement and will likewise not be able to respond proactively to disasters.

8.7 ***The availability of the IT DRP Manual was not assured in the Main Office and copies of the DRP were not disseminated to the DR Team and other authorized personnel.*** A draft copy, updating the DR Manual, has been prepared and is pending for approval as of this writing. However, since the IT DR Manual for 2018 is still pending for approval, the old IT DR Manual should still be present on both the main office/primary site and the DR site. The non-maintenance of the DRP at the main office or primary site increases the risk that DRP will not be readily available in the event of a disaster and crucial recovery procedures may not be properly executed in these scenarios.

Recommendations:

8.8 We recommended that the management:

a. Conduct an updated business impact analysis and risk assessment to evaluate risks and assess mission critical applications;

b. Develop an up-to-date BCP that is aligned with the strategy of the identified critical business units and the agency to ensure continuous operations and restoration of key business functions and services in the event of disruption in accordance with the requirements of laws and regulations and other relevant internal policies of the FI;

c. Perform regular annual FI-wide BCP testing with a comprehensive scope of testing to cover the major components of the plan as well as coordination and interfaces among important parties. Likewise, results of plan tests including successes, failures and lessons learned should be thoroughly analyzed, documented, monitored and corrected in a timely manner to promote continuous BCM improvement;

d. Ensure that the BCP and DRP were disseminated to concerned personnel; and

e. Properly and securely maintain copies of the BCP and DRP at strategic locations. Distribute hard and soft copies of the DRP to concerned personnel when and where needed. Attention should be made to making plans accessible under all disaster scenarios. Also, strengthen internal control on the issuance of the BCP and DRP by assigning control numbers and disseminate updated copies to Team Managers and appropriate Team Members.