BDO Roxas Cruz Tagle and Co.
Audit | Tax | Consulting | BSO

THE NEW INDIA ASSURANCE CO. LTD.

INTERNAL AUDIT REPORT

JUNE 03, 2021

Table of Contents

Page

List of Appendices

BDO Roxas Cruz Tagle and Co.
Audit | Tax | Consulting | BSO

2nd Floor Multinational Bancorporation Centre
6805 Ayala Avenue, Makati City 1226 Philippines
t: +632 844 2016
f: +632 844 2045
www.bdo-roxascruztagle.ph

03 June 2021

The New India Assurance Co. Ltd.
Room 405, ITC Building
337 Sen Gil Puyat Ave
Makati, 1209 Metro Manila

Attention: **Mr. Rullie B. Payapaya**
Senior Accounts Manager

We submit, for your information and appropriate action, our final report on the results of our internal audit of relevant processes of The New India Assurance Co. Ltd. Our audit was performed in accordance with the International Standards for the Professional Practice of Internal Auditing.

We have received written comments and actions taken or planned from the Company's management on May 11, 2021 and May 20, 2021, in response to our observations and recommendations. Pertinent comments and actions taken or planned have been considered or are included in this report.

Management is primarily responsible for the implementation of adequate internal controls and appropriate management of risks in each area of responsibility.

The matters raised in this report are those that have come to our attention arising from our review that we believe need to be addressed by Management. It is not a comprehensive record of all the matters arising and in particular, we cannot be held responsible for reporting all risks and all internal control weaknesses. The extent of our work and completeness of the results are based on the level and quality of information provided to us and the support from the Company's Management.

This report has been prepared solely for the use by the management of The New India Assurance Co. Ltd. We do not accept responsibility to any third party to whom the contents may be disclosed or who at their own accord may decide to rely on it as the report has not been prepared for, and is not intended for, any other purpose.

Very truly yours,

ROXAS CRUZ TAGLE AND CO.

Jay D. Fernandez
Partner

EXECUTIVE SUMMARY

Objective

The main objective of this audit is to assess the adequacy and effectiveness of the design and operation of internal controls over the relevant processes, which was agreed with you during the audit planning phase.

Scope

Our audit covered the following Company's processes:

1. Agent Hiring/ Broker Accreditation and Renewal
2. Billing and Collection
3. Claims
4. Commission
5. Payroll, Payables and Disbursements
6. Underwriting & Reinsurance
7. Financial Reporting
8. IT Controls
9. Compliance

Status of Previous Audit's Observations and Recommendations

Status of Implementation as of March 2021	No.	Percentage
2018		
Implemented	17	90%
Partially Implemented	1	5%
Not Yet Implemented	1	5%
TOTAL	19	
2019		
Implemented	9	76%
Partially Implemented	1	8%
Not Yet Implemented	1	8%
Not Applicable	1	8%
TOTAL	12	

Conclusion

Based on audit procedures performed, we noted key process and control observations requiring management's attention and implementation of actions plan.

We checked the status of implementation of management-agreed action plans related to our 2018 and 2019 audit. We noted that there are still actions plans that were not implemented and remained outstanding. These include compliance to Data Privacy Act (DPA) of 2012 and performance of periodic review of users in Geniisys accounting system. The Company has not conducted a privacy impact assessment, has not finalized its privacy policy manual, and has not yet obtained consent from its employees and insurance agents to allow collection and processing of personal data for purposes required under employment or agent hiring. In addition, the Company has not implemented a firewall to enhance security and protect the Company from vulnerabilities and information security attacks.

There are no additional review procedures made for the manual computation and recording of depreciation expenses, accruals, adjustments, and bank reconciliation prepared by Senior Accounts Officer.

We reviewed the open transactions of the Company and noted a number of outstanding transactions. Because of these open transactions, journal entries and trial balance at month-end cannot be posted and finalized in Geniisys. To compensate for this error, management maintains manual general ledgers and prepares financial reports outside the system.

We observed that access to the data center is not restricted. Absence of security over data center may result to compromised infrastructure that may result to theft and loss of Company's data.

Detailed discussions of these observations are presented in Section B of the attached Detailed Report.

There are a number of moderate and low risks issues as shown in Appendix 2 and 3, respectively, were presented for management action and considerations.

Section A: Details of Observations and Recommendations

PRIOR YEAR OBSERVATIONS	
Data Privacy Act (Compliance); IT General Controls	
Observation No. 1: Implement firewall to protect the Company from malicious external attacks and enhance information security measures to limit vulnerability, breach, or leakage of data *(2018 audit); Not yet implemented*	
Criteria: Section 25 of Data Privacy Act states "Personal information controllers and personal information processors shall implement reasonable and appropriate organizational, physical, and technical security (firewalls, encryption, access control policy, security of data storage, and other information security tools) measures for the protection of personal data." **Condition:** As of audit date, it was noted that the Company does not have firewall in place to protect the Company from external vulnerabilities such as internet attacks, malicious and unauthorized access to private information. As discussed by the IT personnel, the request to purchase or acquire firewall has already been sent to the Head Office since 2018. However, there is no response from Head Office regarding the matter. **Risks:** Leakage of data (e.g., company information, personal information) and compromised Company IT network from external factors. Theft or breach of data that may result to the following: a. Damage reputation or goodwill that may result to loss of customer b. Penalties and possible lawsuit due to unauthorized access to personal information	
Recommendation: Moving forward, the Company should implement the usage of firewall security and enforce appropriate policies to control inbound and outbound traffic. In addition, the Company may consider implementing, but not limited to, the following: 1. Install and activate malicious software protection tools (e.g., Sophos, Kapersky, etc.) on processing facilities, with malicious software definition files that are updated. 2. Filter incoming malicious traffic, such as email and downloads, to protect against unsolicited information (e.g., spyware, phishing emails) using anti-virus. 3. Communicate malicious software awareness and enforce prevention procedures and responsibilities. Conduct periodic training about malware in email and Internet usage. Train users to not open, but report, suspicious emails and to not install shared or unapproved software. 4. Encrypt information in transit according to its data classification 5. Regularly review and evaluate information on new potential threats (e.g., reviewing vendors' products and services security advisories) 6. Perform vulnerability assessment and penetration testing, as applicable	**Risk Levels** Likelihood - Moderate Impact - High
Management Comment / Agreed Action Plan: The Company will follow-up on the request to purchase firewall and anti-virus to the Head Office.	**Responsible Person / Timeline:** Dexter Maglalang (IT Personnel) / Q4 2021

IT General Controls

Observation No. 2: Implement and document the periodic review of active users and their access - 2019; Not Implemented

Criteria:

Existence of periodic review of active users and their access.

Condition:

Based on the prior year's internal audit, the management included in its response to conduct quarterly review of system user access with formal documentation.

However, based on our review, the implementation of quarterly review is not yet performed as of audit date.

Risk:

Unauthorized individuals may have access to system transactions and data.

Unauthorized individuals may use the access of separated employees to perform unauthorized transactions.

Recommendation:	**Risk Levels**
The IT personnel should initiate coordination with HR in verifying the existence of active users in the system based on HR list of active employees. In addition, document the periodic review of user access. The result of review must be properly signed off by concerned department head to verify that access rights assigned to users are authorized and correct.	Likelihood - Moderate Impact - High
Management Comment / Agreed Action Plan:	**Responsible Person / Timeline:**
The IT Personnel will implement periodic review on an annual basis and submit to management.	Dexter Maglalang (IT Personnel) / Q4 2021

Data Privacy Act (Compliance)

Observation No. 3: Partial Compliance with the Data Privacy Act (DPA) - 2019; Partially Implemented

Criteria:

National Privacy Commission requires personal information collectors and processors to comply with the provisions of RA 10173 or Data Privacy Act of 2012.

Condition:

As of review date, the following were noted:

a. The Company has not conducted Privacy Impact Assessment.
b. Absence of consent form signed by the data subjects (e.g., employees, agents)

As discussed by the Senior Account Officer, the Company hired an outsourced lawyer for the creation of privacy policy manual. The drafted privacy policy manual is forwarded to the COO for approval.

Risk:

May incur penalties for non-compliance with the National Privacy Commission (NPC)

Unauthorized processing and improper disposal of sensitive personal information, which are penalized under RA 10173.

Recommendation:	**Risk Levels**
Moving forward, the company should: 1. Conduct Privacy Impact Assessment 2. Finalize and formalize Privacy Policy Manual 3. Implement Privacy Policy (e.g., upholding the rights of the data subjects, existing and new employees, by getting consent prior to the collection and processing of data)	Likelihood - Moderate Impact - High

Management Comment / Agreed Action Plan:	Responsible Person / Timeline
The Company has an existing data privacy policy from the Head Office and will be localized. The Company cannot perform the Privacy Impact Assessment yet due to the lack of firewall and anti-virus.	Rullie Payapaya (Senior Accounts Officer) Q4 2021

Current Year Observations

Financial Reporting and Closing Process (FRCP)

Observation No. 4: No review procedures made for the manual computation and recording of depreciation expenses, accruals, and other adjustments prepared by Senior Accounts Officer

Criteria:

Journal entry transactions including depreciation expense are properly reviewed and approved by a person independent of the preparer prior to posting.

Condition:

Computation for the depreciation of Property and Equipment is manually prepared and computed by the Senior Accounts Officer. Adjusting entries for accruals, investments, bank reconciling items and other manual adjustments is also prepared by the Senior Accounts Officer. No further review is done for the computations and journal entries made.

A review of the manual computation of depreciation, accruals and other adjustments is necessary in order to detect or prevent errors that may result to incorrect balances in the financial records of the Company.

Risk:

Risk of human error in the preparation of the report and mistake may go undetected due to lack of review.

Errors will not be prevented or detected if work is not reviewed in a timely manner.

Recommendation:	Risk Levels
We recognize that the accounting department has a limited number of employees and therefore the Company is somewhat restricted in obtaining maximum segregation of duties. However, we believe the system could be strengthened by requiring the computation of depreciation of Property and Equipment, accruals, investments, bank reconciling items and other manual adjustments be prepared by other employee under the accounting function and the Senior Accounts Officer should only review the results of computation thereof, to help prevent and detect errors and accurately reflect the financial balances of the Company.	Likelihood - Moderate Impact - High

Management Comment / Agreed Action Plan:	Responsible Person / Timeline
The Company has requested for additional manpower. However, due to the pandemic, this may not be approved. Instead, the Company plans to delegate the workload of the Senior Accounts Officer (i.e., preparation and computation of depreciation, amortization, accruals, and investments) to other accounting personnel for him to perform review functions. The management plans to gradually transfer the tasks of the Senior Accounts Officer to other accounting personnel before the end of the year 2021. The Company will still follow-up the request for additional manpower.	Rullie Payapaya (Senior Accounts Officer) Accounting Personnel: 1. Del Sanggalang 2. Diana Pascua 3. Kristine Cervantes 4. Clarise Letrodo Q4 2021

Financial Reporting and Closing Process (FRCP)

Observation No. 5: Enhance review procedures for bank reconciliations

Criteria:

Review of the bank reconciliation statements by an independent personnel to detect and prevent misstatements in the accounting records.

Condition:

The Senior Accounts Officer reviews the bank reconciliation of the following banks as prepared by the Accounting staff:

Bank Account	Preparer
METRO BANK SAVINGS ACCOUNT	Del Sanggalang
HSBC-CURRENT ACCOUNT	Del Sanggalang
BDO-SAVINGS ACCOUNT	Mary Jane Viray
BANK OF PHILIPPINE ISLAND	Del Sanggalang

However, it was noted that the Senior Accounts Officer also prepares bank reconciliation and adjusting entries for the following bank accounts:

1. BDO Dollar Account
2. Asia United Bank Savings Account
3. Landbank_ Tax payment account
4. Union Bank Savings Account

The bank reconciliation statements above prepared by the Senior Accounts Officer has no evidence of review by an independent person. It was confirmed with the Senior Accounts Officer that the bank reconciliation is not subjected to an independent review.

Risk:

Bank reconciliation statements may not be completed on a timely basis due to existence of numerous bank accounts and bank transactions. Risk of human error in the preparation of the report and mistake may go undetected due to lack of review.

Recommendation:	**Risk Levels**
Reconciliations should be reviewed and approved on a monthly basis by a personnel independent of the preparer.	Likelihood - Moderate Impact - High
Management Comment / Agreed Action Plan: The Company has requested for additional manpower. However, due to the pandemic, this may not be approved. Instead, the Company plans to delegate the workload of the Senior Accounts Officer (i.e., preparation and computation of depreciation, amortization, accruals and investments) to other accounting personnel for him to perform review functions. The management plans to gradually transfer the tasks of the Senior Accounts Officer to other accounting personnel before the end of the year 2021.	**Responsible Person / Timeline** Senior Accounts Officer and Accounting Personnel: 1. Del Sanggalang 2. Diana Pascua 3. Kristine Cervantes 4. Clarise Letrodo Q4 2021

Financial Reporting and Closing Process (FRCP)

Observation No. 6: Timely closing and posting of the Open Transactions in Geniisys.

Criteria:

Timely closing and posting of open transaction to reflect performance of monthly closing activities.

Condition:

We have noted the following number of Open Transactions per branch as of May 6, 2021:

Branch	No. of Open Transactions
Head Office (Makati)	64
Pampanga (Angeles)	3
Bacolod Branch	6
Cebu Branch	1
TOTAL	74

Open transactions included items from disbursements, claims, underwriting, and journal vouchers that were not posted and completed in Geniisys. Because of these open transactions, journal entries at month-end cannot be posted in Geniisys. Due to this error, the journal entries and trial balance in the system cannot be processed. To compensate for this error, management prepares manual entries and prepare trial balance and financial reports outside the system.

The issue was already reported to third-party provider (CPI) but has not been addressed.

Risk:

Untimely closing and posting of open transactions can result to unrecognized valid transactions, which may lead to a misstatement in the balance recorded in the Company's books.

Recording outside the system may affect the efficiency in the preparation of the reports and manual recording of transactions is prone to human error.

Recommendation:

The Company may opt to:

1. Timely review of all the open transactions prior to closing or posting in Geniisys to utilize the system for the performance of the monthly closing activities of the Company.

2. Report the problems encountered in the system (Geniisys) through tickets to CPI for assistance.

Risk Levels

Likelihood - Moderate

Impact - High

Management Comment / Agreed Action Plan:

Moving forward, the Company will include the review of open items in its month-end closing activities.

Responsible Person / Timeline

All responsible process owners / Q4 2021

IT Generals Control	
Observation No. 7: Access to data center is not restricted	
Criteria: Access to data center is restricted to authorized personnel. **Condition:** During the course of audit, noted that data center is located in the IT room. The IT room is not restricted/limited to the IT personnel and any Company personnel may enter. We further observed the following: 1. There is no signage in the IT Room to signify restriction of the area. 2. The door of the IT room is always open. 3. Other personnel were stationed on the server area. **Risk:** Proper security of infrastructure may be compromised which may result to loss of data.	
Recommendation: The Company shall limit access to IT Room; If the Company cannot limit the access to the IT Room, install CCTV inside the server room for proper monitoring. Also, conduct periodic review (e.g., weekly) of CCTV footages to detect unauthorized access; or Utilize logbooks to document the in and out of personnel in the IT Room.	**Risk Levels** Likelihood - Moderate Impact - High
Management Comment / Agreed Action Plan: The Company will follow-up on the existing proposal to purchase CCTV to Head Office.	**Responsible Person / Timeline** Dexter Maglalang (IT Personnel) / Q4 2021

Appendix 1: Risk Classification Criteria

RISK CLASSIFICATION CRITERIA			
LIKELIHOOD	High	Moderate	Low
	Almost certain	Possible	Unlikely
	Risk has already occurred in the past and is expected to recur anytime	Risk may occur anytime	Risk has not yet occurred in the past and / or probability of occurrence is very low
IMPACT	High	Moderate	Low
Legal Exposure	Habitual non-compliance (5x a year)	Occasional non-compliance (2x a year)	Without non-compliance
Image	Global	Local / National	Internal
Cost / Revenue Implication	Increased cost or loss of revenue of > 10%	Increased cost or loss of revenue of > 3% but < 10%	Increased cost or loss of revenue of < 3%
Financial / Operational Reporting	Intentional misstatement or unintentional misstatement of financial results with > 5% impact on EBITDA or Net Income	Unintentional misstatement of financial results with > 2% but < 5% impact on EBITDA or Net Income	Unintentional misstatement of financial results with < 2% impact on EBITDA or Net Income
Manpower	Customer servicing is fully stopped (e.g., Strike) or seriously affecting productivity (> 10% decline)	Significantly affecting productivity (< 10% but > 5% decline) (e.g., High turnover rate)	Low productivity (< 5% decline)
Property	Loss of Data / Property (from theft, hacking, fire or calamity); Industrial accident (to employees or external parties)	System / equipment failure resulting to significantly delayed customer servicing (> 2 days delay	Equipment / system failure or breakdown but with ready alternative
Procedural	No established procedure or with procedures but not implemented	Being practiced but no written procedure	With procedure but needs revision

Appendix 2: Observations with Moderate Risk requiring enhancement in controls

PRIOR YEAR OBSERVATION	
IT General Controls	
Observation No. 1: Update the IT policies and procedures - 2018; Partially Implemented	
Condition: The documented IT policies and procedures consists of the following: a. Access Controls b. Password Controls c. Backups d. System Update However, noted that the practice in addressing issues or concerns raised by the end-users is not included in the policy. In addition, there is no documented policy on periodic review of user access. **Risk:** Outdated policies and procedures may cause inefficient and inconsistent application of processes resulting to errors or internal control weaknesses, and inability to enforce employee accountability	
Recommendation: Update the documented IT policies and procedures to include the process in addressing the issues or concerns raised by the end-user and periodic review of user access. Subsequently, it must be approved as evidenced by signoffs of authorized personnel on the physical document. The policies and procedures should be available to relevant personnel for reference when needed. In addition, perform periodic review of manual (e.g., annually) to ensure that such policies and procedures are still effective up to date and to prevent any confusion or misunderstanding that may arise resulting from its non-revision (if update is necessary). Approved changes made shall form part of the revision history of the Company's policies and procedures manual.	**Risk Levels** Likelihood - Moderate Impact - Moderate
Management Comment / Agreed Action Plan: It is under the process of updating. The Company will include in the policy the ticketing system. Email request will also be implemented and included in the policy.	**Responsible Person / Timeline** Dexter Maglalang (IT Personnel) / Q4 2021

CURENT YEAR OBSERVATIONS

Data Privacy Act *(Compliance)*

Observation No. 2: Data Privacy Act registration is expired

Condition:

RA 10173 or Data Privacy Act of 2012 requires collectors and processors of information/data to register with the National Privacy Commission.

Noted that the Company is registered with the National Privacy Commission dated May 3, 2019 with effectivity date until March 8, 2020.

Risk:

The Company may incur penalties for non-compliance with the National Privacy Commission (NPC)

Recommendation:	**Risk Levels**
To comply with the Data Privacy Act of 2012, the Company should renew its registration. Moving forward, the Company should develop a monitoring tool for the periodic renewal of required licenses and registrations (e.g., Business permits, National Privacy Commission (NPC) annual registration, etc.)	Likelihood - Moderate Impact - Moderate
Management Comment / Agreed Action Plan: The Company will renew its registration with the National Privacy Commission.	**Responsible Person / Timeline** Rullie Payapaya (Senior Accounts Officer) and Dexter Maglalang (IT Personnel) / Q4 2021

IT General Controls

Observation No. 3: Consistent use of User Access Forms

Condition:

Based on the documented IT policies and procedures, user access of resigned employees is deactivated through request based on the accomplished User Access Forms.

However, out of the three (3) sampled resigned employees, all are not evidenced by the duly accomplished User Access Forms. *Please refer to the table below for the list of samples.*

Per inquiry with the IT Personnel, the request for user access deactivation for the sampled three (3) users was communicated verbally by HR and the documented policy for the use of User Access Forms in requesting deactivation of user access is not yet fully implemented as of scoped period of review.

Resigned Employee	Branch	Date of Exit
Jeanive Permale	Cebu	02/04/2020
Ma. Regina Purugganan	Bacolod	10/11/2019
Emilio Gopio, Jr.	Makati	05/07/2019

Risk:

Unauthorized deactivation of user access

Untimely deactivation of user accounts of resigned employees

User IDs of resigned employees may be utilized to submit and process unauthorized transactions and/or perform other unauthorized or fraudulent activity

Recommendation:	**Risk Levels**
Consistent use of User Access Form to ensure changes made to user access is duly authorized.	Likelihood - High Impact - Low
Management Comment / Agreed Action Plan: Moving forward, the Company will include the request to deactivate user access in the clearance form of the resigning employees.	**Responsible Person / Timeline** Dexter Maglalang (IT Personnel) and Jana San Luis (HR) / Q4 2021

Appendix 3: Other Recommendations for Management Considerations

(with Management Comment / Agreed Action Plan, Responsible Person and Timeline)

FINANCIAL REPORTING AND CLOSING PROCESS (FRCP)

- **Inconsistent documentation of review of Management Information System (MIS) Reports**

  A review should be conducted prior to sending the monthly reports to Head Office. This will help in the monitoring of possible actions that should be made for further improvements in the operations. Review must also be made to determine validity, accuracy, completeness, and presentation of the account balances. / *There was an email review conducted. / COMPLETED*

- **Update the name of the preparer in the MIS Reports**

  Update the name of preparer from Rullie B. Payapaya "RBP" to the actual personnel who analyzed and processed the data.

Reports	Preparer
Snap Report Outstanding Premium Balance Statement of Operational results Fund Position for the month Expenses for the month	Del Sanggalang
Outstanding Agency Balance Sheet	Kristine Cervantes
Summary of Premiums	Del Sanggalang (Reinsurance) Kristine Cervantes (Direct)

By doing so, the preparer exercises accountability in the presented balances in the reports. / *The preparer was updated per reports. / COMPLETED*

UNDERWRITING (REINSURANCE - INWARD)

- **Inefficient filing system**

  We recommend the Company's filing system be organized to ensure that all documents and records are properly filed on a timely basis. In addition, employees should be required to sign for records removed from the files. This practice will reduce the possibility of records being misplaced or misfiled. / *Moving forward, documents will be filed after the completion of required documents. The assigned personnel for filing will make use of logbooks to properly monitor the transfer of documents and accountability. / All responsible process owners; Q4 2021*

Makati
2nd Floor Multinational Bancorporation Centre
6805 Ayala Avenue, Makati City
1226 Philippines
Tel. No. (+632) 844 2016
Fax No. (+632) 844 2045 cpas@bdo-roxascruztagle.ph

Cebu
Unit 707, 7th Floor AppleOne Equicom Tower
Mindanao Avenue corner Biliran Road
Cebu Business Park, Cebu City
6000 Philippines
Tel. No. (+6332) 340 4033 / 401 1248
Fax No. (+6332) 340 4037 cebu@bdo-roxascruztagle.ph

Cagayan de Oro
2nd Floor ATC Building
A. Luna corner A. Velez St.
9000 Philippines
Tel. No. (+6388) 856 4532 / 852 4214
Tel. No. (+638822) 727 431
Fax No. (+63882) 725 082 cdo@bdo-roxascruztagle.ph

Isabela
King Street Mall
105 Rizal Avenue, District III (Pob.),
Cauayan City, Isabela, Cagayan Valley
3305 Philippines
isabela@bdo-roxascruztagle.ph