KUENSEL
THAT THE PEOPLE SHALL BE INFORMED

RAA points out lapses in BoB system

July 2, 2018 News Leave a comment 0 Views

Notwithstanding positive change the Bank of Bhutan (BoB) brought with the change in its core banking solution from flexcube to TCS BaBCS, the Royal Audit Authority (RAA) pointed out lapses pertaining to access control and validation.

The Bank of Bhutan shifted its CBS from Oracle FLEXCUBE to TCS BaNCS in 2016, which facilitated the introduction of innovative products and services.

The RAA has conducted an IT Audit of Core Banking Solution (TCS BaNCS) of the BoB.

The RAA acknowledged that the new CBS has reduced failure rate in transactions initiated through ATMs, B-Wallet, M-BoB and Internet Banking. It was also pointed out that many of the banking activities and services were automated in the new CBS and that the new system is embedded with numerous convenient features, which has enhanced the efficiency of banking services

RAA's review and analysis also showed that the Bank had followed requisite procedures in data migration and it was correctly carried out.

However, it was found that inappropriate access rights were granted to the users besides lack of comprehensive policies and guidelines on access management.

"Access control should be given generally based on principles of 'Need to know' and 'least privilege' so that users are assigned with privilege just to perform their roles and extra privileges are controlled and restricted," the RAA report stated.

In the new CBS, access right is divided into 32 user types according to their roles and function and these users are grouped into 11 groups. For instance, cashiers are not given the approving rights, which an approving officer has. Access rights go in a hierarchical manner, the top being super user rights, meaning this person have full administrative and management rights. This is to ensure check and balance.

The RAA, while reviewing the access control, found an instance where a user in Group 2 (basically teller agents and cashiers) has been given approving rights, which otherwise should be given to Group 3 (Approving officers including head cashier). Likewise, one user in Group 5 (Managers) was granted super user rights. This access, the RAA stated, should be restricted to limited number of users in order to minimize the risk of fraud and manipulation in the system and the activities performed by these users should be monitored regularly. However, the RAA found that 25 users have these rights

The RAA stated that giving more rights than required particularly creation and approving rights together defeats the principle of "least privilege" and at the same time increases the risk of overriding other controls and thus opening room for manipulation and fraud.

The BoB management, however, responded that observations made have been verified and necessary remedial action has been taken, which the RAA also verified. RAA pointed out that instituting proper long-term strategies such as policies and guidelines would further strengthen the controls related to system access.

The RAA also noted 16 cases of consumer loans where loan amount sanctioned by the bank after September 1, 2014 had exceeded the maximum ceiling of Nu 500,000 prescribed by the central bank. The Royal Monetary Authority issued Guidelines on Consumer Loans, Vehicle Loans, and Housing Loans, which came in effect from 1st September 2014.

The Guidelines on Consumer, Vehicle and Housing Loans stipulate a maximum term of five years, seven years, and 20 years respectively. Nevertheless, the analysis of loan details revealed that there were several instances where loan terms exceeded the maximum terms specified in the guidelines.

During the analysis, the RAA also observed 365 cases in terms of housing loans wherein loan terms exceeded 20 year ranging from 21 to 31 years before September 1, 2014. This happened in the system due to lack of proper validation controls in the system and non-incorporation of such requirements in the system.

RAA also checked the existence and implementation of approved policy statement on transactions with related parties as per the requirement of RMA's Prudential Regulations 2016 and Financial Service Act 2011. The RAA found no such policy was formulated and implemented by BoB.

The Audit while reviewing the data on staff loans, board of directors and its related parties, found all transactions within the specified range. But it was observed that controls required by Prudential Regulations are not captured in CBS.

On this observation, the management stated that the guidelines are strictly followed and other statutory requirements and internal appraisal processes are adhered to while approving loans. The management also agreed that policy statement would be included in the revised credit manual and explore on possibilities of capturing the controls required by PR in the CBS.

In May 2016, an intruder siphoned-off Nu 16.506M from a Letter of Credit account of a government agency maintained with BOBL. The intruder hacked the e-mail account of the accountant of the agency concerned, sent Branch Manager of BOBL forged documents and managed to get it approved for international transfers.

It was also found that the branch manager advised the maker-checker to process the transfer and they approved the forged fund transfer advice that was signed by an officer who was not the authorized signatory of the agency. It could have been avoided if the signature of the authorised signatory of the agency was uploaded in the CBS and that the officials verifying the documents cross-referenced it with the forged document before approving the transfer.

“This was partly due to lacuna in internal control and mostly due to lack of due diligence in part of the officials concerned,” the report stated.

Audit stated that some of the illegal transfers would have been prevented if the verifying officer had a checklist for minimum required documents embedded in the system. In all the three cases, the officials concerned had failed to exercise due diligence when verifying the documents and approving the transfers.

“In the security chain, people are considered to be the weakest link. Security breaches often occur due to lack of appropriate security measures instituted and ignorance of system users of their responsibilities,” said RAA Performance Audit Report.

Further, the RAA also noted that Business Continuity and Disaster Recovery Plans were never tested for its effectiveness and appropriateness in case of unplanned disaster causing interruption to the Bank’s business operations.

As required by Financial Services Act 2011, the BoBL had developed Disaster Recovery Plan in 2011 and prepared its Business Continuity Plan in 2014 defining procedures to respond to emergency situations and recover its critical processes and functions.

Upon review of BCP and Disaster Recovery Plans, the RAA observed that these documents were not updated even after adoption and implementation of new system.

Moreover, the audit also found several shortcomings in security of BoB’s data centre (DC) data recovery (DR) site.

The audit has recommended the BoB to develop and implement comprehensive long term policies and guidelines on system access management in addition to existing BoBL’s User Access Management Policy to ensure that business justified access is granted to users at all times.

BoBL is also asked to develop and implement long-term action plans related to business continuity, data recovery and security awareness. “BoBL must tighten the internal control related to international transfers by incorporating the controls in the CBS and institute proper accountability process for such lapses,” the report stated.

Tshering Dorji