বাংলাদেশ ব্যাংক
প্রধান কার্যালয়
ঢাকা ।

ডিওএস সার্কুলার লেটার নং- ১৭

তারিখ ঃ ২৩ কার্তিক, ১৪১৯ / ৭ নভেম্বর, ২০১২

চেয়ারম্যান, পরিচালনা পর্ষদ
ও
প্রধান নির্বাহী/ব্যবস্থাপনা পরিচালক
বাংলাদেশে কার্যরত সকল তফসিলি ব্যাংক

প্রিয় মহোদয়,

জালিয়াতি/প্রতারণামূলক কার্যক্রম প্রতিরোধের জন্য ব্যাংকের অভ্যন্তরীণ নিয়ন্ত্রণ ব্যবস্থার স্বমূল্যায়ন প্রসঙ্গে ।

বিগত ০৪ ফেব্রুয়ারি ২০১০ তারিখের বিআরপিডি সার্কুলার নং-০৬ এর প্রতি আপনাদের দৃষ্টি আকর্ষণ করা যাচ্ছে ।

এ সার্কুলারে ব্যাংক ব্যবস্থাপনায় কর্পোরেট সুশাসন নিশ্চিত করার লক্ষ্যে ঋণ ও ঝুঁকি ব্যবস্থাপনাসহ ব্যাংকের সামগ্রিক ব্যবসায়িক কার্যক্রম, অভ্যন্তরীণ নিয়ন্ত্রণ, মানবসম্পদ ব্যবস্থাপনা ও উন্নয়ন, আয়-ব্যয় ইত্যাদিসহ সার্বিক আর্থিক, পদ্ধতিগত এবং প্রশাসনিক নীতি-নির্ধারণী ও নির্বাহী কার্যক্রমে পরিচালনা পর্ষদ, পর্ষদের চেয়ারম্যান ও ব্যাংকের প্রধান নির্বাহীর দায়-দায়িত্ব ও জবাবদিহিতা সুনির্দিষ্টভাবে নির্দেশিত হয়েছে। এছাড়াও ব্যাংকের বিবিধমুখী কর্মকাণ্ডে জড়িত বিভিন্ন ঝুঁকি চিহ্নিতকরণ, মূল্যায়ন ও নিয়ন্ত্রণের জন্য ঝুঁকি ব্যবস্থাপনা গাইডলাইন অবলম্বন ও অনুসরণের জন্য বিভিন্ন সময় নির্দেশনা দেয়া হয়েছে ।

উপর্যুক্ত নির্দেশনাবলির আলোকে ব্যাংকগুলোর জালিয়াতি/প্রতারণামূলক তৎপরতার প্রবণতা প্রতিরোধে আপনাদের অবলম্বিত অভ্যন্তরীণ নিয়ন্ত্রণ ব্যবস্থাদির কার্যকারিতার স্বমূল্যায়ন ত্রৈমাসিক ভিত্তিতে বাংলাদেশ ব্যাংকের পর্যালোচনা এবং প্রয়োজনবোধে সরেজমিনে যাচাইয়ের জন্য সংগ্রহের সিদ্ধান্ত নেয়া হয়েছে । এতদ্সংযোজিত ছকে এ স্বমূল্যায়ন ব্যাংকের প্রধান নির্বাহীর স্বাক্ষরে এবং পর্ষদের অডিট কমিটির চেয়ারম্যানের প্রতিস্বাক্ষরে ডিসেম্বর,২০১২ থেকে প্রতি ত্রৈমাসিকের মূল্যায়ন পরবর্তী এক মাসের মধ্যে এ বিভাগে দাখিল করতে হবে ।

অনুগ্রহপূর্বক প্রাপ্তি স্বীকার করবেন ।

আপনাদের বিশ্বস্ত,

সংযুক্তি ঃ বর্ণনামতে (ছয় পৃষ্ঠা)

(এস, এম, রবিউল হাসান)
মহাব্যবস্থাপক
ফোন ঃ ৯৫৩০০৯৩

Date :

From : Managing Director/CEO/Country Head

To : General Manager
Department of Off-site Supervision
Bangladesh Bank, Head Office, Dhaka

Quarter ended on :

Sub: <u>Self-Assessment of Anti-Fraud Internal Controls.</u>

Dear Sir,

I would like to confirm you in terms of your DOS circular letter no.17 dated 07-11-2012 that the annexed self-assessment of anti-fraud internal controls has been carried out with due diligence under the purview of best practices or safety and soundness standards in the banking industry. The information contained in the self-assessment sheet truly and faithfully reflects the actual position of the bank's internal control practices.

Sincerely Yours,

Signature and date:
(Name :----------)
Managing Director/CEO)

Counter signature and date
(Name:----------)
Chairman, Audit Committee of the
Board of Directors

Self-Assessment of Anti-Fraud Internal Controls

Sl. No.	Particulars	Yes	No	Remarks (if any)
	Internal Control & Compliance (ICC):			
01	Is the bank's Internal Control and Compliance Department well equipped with policy[1] support and adequate[2] manpower including IT skilled personnel for preventing and detecting fraud/forgery?			
02	Were there incidents of fraud/forgery detected by your Internal Control & Compliance Department in the last 03 (three) months (if Yes, fill up the attached sheet)?			
03	Does the Management Committee review the overall effectiveness of the internal control system of the bank on a yearly basis as per ICC guidelines?			
04	Does the Monitoring Unit properly monitor the operational performance of the branches by reviewing the Quarterly Operations Report (QOR)?			
05	Are the employees provided with clear authority/delegation of power and job description to perform the daily activities of the bank with proper documentation of handover and takeover of charges when applicable?			
06	a) Does the bank have risk-based auditing system?			
	b) Does the Audit and Inspection Unit of the bank regularly[3] audit bank branches and divisions/departments/sections (Such as Card, IT, Retail, Mobile Banking, SME etc). as per ICC guidelines?			
07	Are there admonitory/reproving measures for internal auditors in case of their failure of detecting fraud and forgery?			
08	Are all the complaints received at branch and head office level properly recorded and redressed?			
09	Are job rotation, transfer, posting and 15-day mandatory leave for the employee strictly followed as per Bangladesh Bank guidelines?			
10	Is there any mechanism[4] to monitor the staff accounts and other accounts operated by the staff to prevent fraud and forgery made by the bank's own employees?			
11	Does internal audit review wire transfers, general ledger suspense accounts, correspondent bank reconciliations, and write-off loans as part of its regular and recurring audit scope?			
12	Does internal audit regularly report suspicious activity to the Chief Anti-Money Laundering Compliance Officer (CAMELCO) and/or the Board of Directors?			
	General Banking and Operation:			
13	a)Are Cheque/Fixed Deposit Receipt (FDR)/Payment Order (PO)/Traveller Cheque (TC), Savings Instruments etc. recorded/issued/paid as per manual/policy/guidelines?			
	b) Does the account opening branch maintain records of cross reference of the allied or sister concerns on the respective account opening form?			
14	Does the bank ensure Balance Confirmation for both loan and deposit accounts to the customer at least once in every six months?			
15	Is effective[5] reconciliation of inter branch/General Account in place and necessary actions are taken on long-pending (three months) items?			
16	Are the reconciliation activities carried out by various division/departments/sections of the bank audited at least once in a year?			

[1] Internal policy/guidelines, circulars, process etc. with continual review and development.
[2] In line with the business volume, branch network etc.
[3] According to the frequency depending on the risk grade of the branches as per ICC guidelines.
[4] A mechanism/system/practice by which bank management can have oversight on employees' accounts.
[5] Which keeps the un-reconciled entries at a minimum level and can detect any fraudulent entry timely.

Sl. No.	Particulars	Yes	No	Remarks (if any)
17	Are Suspense Accounts, Sundry Debtor Accounts, Sundry Creditors, Sundry Deposits, Government Utility Accounts, Development Expenditure & Miscellaneous Expenses duly monitored?			
18	Are the individual employees' Activity Reports (Computer posting listings) tallied with vouchers by the respective branch managers on a daily basis?			
19	Are precautions taken to inoperative/dormant accounts for 2-3 years and ageing unclaimed deposits and valuable goods of 10 years and above?			
20	Does the bank ensure reimbursement within 24 hours regarding debit of accounts even though the ATMs have not disbursed cash?			
21	a) Does the bank display telephone numbers of help desk/contact persons at all of their ATM booths to lodge complaints or seek assistance?			
	b) Does the bank redress each call for complaint/assistance within 24 hours??			
22	a) Does the bank have adequate security measures like CC TV, Alarm System etc. in places like excess point, vault area, cash transaction area, ATM booth etc.?			
	b) Does the bank take and preserve regular back-ups of CC TV records?			
	c) Are the CC TV recorders[6] placed in a secured place?			
23	Does the bank maintain security of lockers as per Bangladesh Bank Guidelines ?			
	Loans and Advances:			
24	Does the Credit Administration Department send a summary report of all past dues, new facilities, renewed, rescheduled, or enhanced facilities to senior management/Board of Directors?			
25	Are credit facilities availed by the borrower in his own name and /or in the name of his allied/sister concerns from all other banks & financial institutions clearly stated in the credit proposal?			
26	Are all credit lines under the purview of CRG (Credit Risk Grading) Guidelines and CRG are done properly considering all information including CIB data?			
27	a) Does the bank have enough control mechanism to prevent fake issuance of debit/credit cards and other fraud/forgery in this area?			
	b) Does the bank ensure regular audit of the card department/division, as it is a highly technology based sensitive area?			
28	Is there any mechanism to ensure that the properties offered as collateral security are physically verified by the appropriate branch official to ensure physical existence of the property and it's possession by the proposed borrower/mortgager?			
29	Does the bank ensure proper control and security regarding credit files and security documents with proper documentation of handover and takeover?			
30	Does any mechanism exist to ensure that unauthorized or fraudulent credit facilities (including non- funded) are not given at branch level?			
31	a) Does the bank ensure that Local Bills Purchased/Accepted are under genuine trade and according to Bangladesh Bank Guidelines?			
	b) Are payment against accepted Local Bills made within due time?			
	c) Are bank employees who are authorized to disburse funds (paying officer) separate from employees who process loan requests (loan officers / underwriters)?			
	d) Are loan disbursements made only when all required approvals have been received and verified?			
	e) Does the bank discourage or prohibit loan proceeds from being disbursed in cash?			

[6] The device in which the video footages are recorded.

Sl. No.	Particulars	Yes	No	Remarks (if any)
	f) Do the loan files contain documentation on how the loans were disbursed, including complete documentation for individuals receiving amounts in cash?			
	g) Does the bank conduct cross-checking of loan files, and cross-checking of applications with existing loan files, for the presence of same borrower with different/fake name?			
	h) Does the bank take steps to prevent loan proceeds from being disbursed to locations far from the borrower's stated business area?			
	i) Is single borrower exposure limit specified by BB followed before sanction of any credit facility?			
	j) Does the bank follow the instruction of BB during rescheduling of classified accounts?			
	Information and Communications Technology (ICT):			
32	a) Does the bank have an 'ICT Security Policy' which is fully implemented and in compliance with the ICT Security Guideline by Bangladesh Bank?			
	b) Does the bank update its 'ICT Security Policy' each year to cope with the evolving changes in the ICT environment and have it approved by the Board of the bank?			
33	Does the bank carry out an internal system audit periodically or at least once a year with sufficient ICT skilled persons to find out loop holes and weaknesses in the systems and take appropriate measures to mitigate the risk?			
34	Has the bank introduced logical access[7] controls to computer systems?			
35	Does the information security officer, system auditor or any other concerned person undertake periodic penetration[8] tests of the system, which may include:			
	a) Attempting to guess passwords using password cracking tools.			
	b) Searching for back door traps in the programs.			
	c) Attempting to overload the system using DDoS (Distributed Denial of Service) & DoS (Denial of Service) attacks.			
	d) Checking if commonly known holes in the software, especially the browser and the e-mail software, exist.			
	e) Checking the weaknesses of the infrastructure.			
	f) Taking control of ports.			
	g) Cause of application crash.			
	h) Injecting malicious codes to application and database servers.			
36	Are there appropriate risk mitigation measures like operating time schedule for the users, transaction limit, transaction frequency limit, fraud checks, AML checks, etc. depending on the risk perception, unless otherwise mandated by the Bangladesh Bank?			
37	Does the bank establish a process to log the information system related problems and incidents, and also ensure real-time security log[9] for unauthorized access?			
38	Is there any system to monitor all types of account holders, especially internal			

[7] Logical Access means valid user ID and password, smart cards, biometric technologies or other industry standards to access the computer system, operating systems, networking system, application software, database, datacenter, Digester Recovery Site (DRS) utilities etc. observing the following rules: (i) different group user should be created with level of access right, (ii) whenever a user logs on to the system all of his operations to the system must be automatically logged by system, (iii) system administrator must be able to analyze every access information of specific user point to point, and)iv) critical operations should be performed by different level of users.

[8] A penetration test is a method of evaluating the security of a computer system or network by simulating an attack from malicious outsiders (who do not have an authorized means of accessing the organization's systems) and malicious insiders (who have some level of authorized access).

[9] Log file store the information of Access Person (Using User ID) Access Time and Operation that is performed on that time.

Sl. No.	Particulars	Yes	No	Remarks (if any)
	employees' accounts, in case of large transactions on a daily/weekly/monthly basis?			
39	a) Are the large transactions authorized by different levels of personnel with their own user ID?			
	b) Does the IT system generate and send to internal audit a daily report of large transactions (amount may vary by institution)?			
40	a) Does a Strong Security System apply to the Account Transfer Process?			
	b) Are an automated Account Transfer monitoring system and Customer notification system (about their Account Transfer by email or mobile message) are in place?			
41	Is there a provision[10] for monitoring the Database Log file for searching malicious attempts to access the database, retrieve passwords, seek/change personal information etc.?			
42	Is there any system to detect any suspicious transactions using any ATM/Debit/Credit card at any delivery channel like ATM, POS, or Internet Payment Gateway?			
43	Is there any ATM monitoring system to supervise ATM balance, loading, unloading functions, disputes, ATM non-functioning, disorder etc?			
44	Is there any policy to segregate the ATM card personalization duties such a way that one individual employee will not be able to duplicate the whole card personalization process?			
45	Is there any compulsory system requiring first time card users to change their PIN number?			
46	Are the appropriate measures taken to prevent skimming and/or trapping of cards at ATM?			
47	Are the appropriate measures taken to prevent card counterfeiting?			
48	Are measures taken to protect phishing attract (Phishing is collection of user's PIN by presenting a fake internet banking website to the users).			
49	Is a 2-factors authentication system (authorization of transactions by the customers using 2 means) in place for on-line fund transfer?			
50	Is a dual control system is in place for the following:			
	a) SWIFT transmission?			
	b) ATM vault opening for loading/unloading cash?			
	c) Posting of high value teller transactions in the system?			
51	Does the bank's IT official accompany the vendor personnel while attending an IT related problem?			
52	Is a mechanism in place to encrypt and decrypt sensitive data travelling through a public network?			
53	Are all the external connections to the datacenter routed through a firewall?			

[10] Provision to analyze the database LOG file for any malicious script specially update operation that is used to change or modify customer account.

Confidential

Bank Name: ……..

Statement of Fraud and Forgeries occurred in our Bank for the period ……

Sl.No.	Particulars of the fraud & forgery including the modus operandi	Name of the Branch	Date of		Amount involved	How the defrauded amount has been accounted for	Name of the Officers/Employees/ others involved	Action taken against the delinquent Officers/ Persons	Present position of the case	Action taken against recurrence of the incident	Remarks
			Occurrence	Detection							
1		3	4	5	6	7	8	9	10	11	