STATE BANK OF PAKISTAN

BANKING CONDUCT & CONSUMER PROTECTION DEPARTMENT

NOTIFICATION

No. BCCPD/CBU-01/Policy /2016/**9436** April 15th, 2016

In exercise of powers conferred by Section 43 of the Credit Bureaus Act, 2015, the State Bank of Pakistan is pleased to make the following regulations-, namely:-

1. **Citation and commencement**. These regulations may be cited as the "Credit Bureaus Regulations" and shall come into force with immediate effect.

2. **Scope**. The regulations shall apply on all credit bureaus granted license by the SBP under the Credit Bureaus Act, 2015.

3. **Definitions**: In these regulations unless the context otherwise requires:-

"Act" means the Credit Bureaus Act, 2015.

"Chief Executive Officer (CEO)" means an individual who, subject to the control and directions of the Board of Directors, is entrusted with the whole, or substantially the whole, of the powers of management of the affairs of the credit bureau occupying the position of CEO and include any executive assuming charge of the bureau as an Acting CEO for interim period or by whatever name called, and whether under a contract of service or otherwise.

"**Control"** refers to an ownership directly or indirectly through subsidiaries, of more than one half of voting power of an enterprise.

"Director" includes any person occupying the position of a director on the board of a credit bureau and includes sponsor, nominee and alternate director or by whatever name called.

"Facility" includes fund based and non fund based facilities (extended in the form of Bank Guarantees, Acceptances and Letters of Credit etc.)

"Family Member" in relation to a person means his spouse, dependent lineal ascendants and descendants and dependent brothers and sisters.

"Group" means persons, whether natural or legal, if one of them or his / her dependent family members or its subsidiary, have control or hold substantial ownership interest over the other.

"Independent Director" is a director of the credit bureau:-

a) who is not linked directly or indirectly with the credit bureau or its sponsors or strategic shareholders; and
b) has not been an executive officer or employee of a subsidiary or associate company of the credit bureau or where directors of the credit bureau has substantial beneficial

interest (20% or more shareholding of director's own or combined with family members).

"Key Executive" means key executive of credit bureau entrusted with following functional responsibilities:-

a) Head of Internal Audit
b) Head of Compliance
c) Head of Information Technology
d) Any other executive reporting directly to CEO

"Sponsor Director" means the member of the Board of Directors of a credit bureau holding sponsor shares.

"Sponsor Shares" mean 10% or more paid-up shares of a credit bureau, acquired by a person(s) individually or in concert with his / her family members, group companies, subsidiaries, and affiliates/associates.

"Subsidiary" will have the same meaning as defined in section 3 of the Companies Ordinance, 1984.

"Substantial ownership" means beneficial shareholding of more than 25% by a person and/or by his dependent family members, which will include his/her spouse, dependent lineal ascendants and descendants and dependent brothers and sisters. However, shareholding in or by the Government owned entities and financial institutions will not constitute substantial ownership, for the purpose of these regulations.

The terms not defined in these regulations shall have the same meaning as ascribed in the Act.

Regulation 1

Corporate Governance

i. In addition to requirements set out in the Act; Sponsor Shareholder(s), Directors, Chief Executive Officer (CEO) and Key Executives of a credit bureau shall comply with the Fitness and Propriety Test (FPT) set out in Annexure-I.

ii. Credit bureaus are required to seek prior written approval of SBP for appointment of Directors and CEO. The Directors and CEO will not assume the charge of their respective offices until their appointments are approved in writing by SBP. All such requests should be addressed to the Director, Banking Conduct and Consumer Protection Department (BC & CPD), SBP along with information prescribed in Annexure-II, III and IV.

iii. If at any time the office of CEO becomes vacant, the credit bureau shall appoint any executive as an Acting CEO who meets FPT criteria and his / her FPT documents have been submitted to BC&CPD. The incumbent may operate the bureau as an Acting CEO until the appointment of a regular CEO upon fulfillment of regulatory requirements.

iv. The CEO and Key Executives shall be full time employees of the credit bureau.

v. The appointment of Key Executives will not require prior approval of SBP. However, the credit bureaus must themselves ensure while appointing Key Executives that they qualify FPT criteria in letter and in spirit. The information on appointment of Key Executives is required to be submitted to SBP on prescribed format as per Annexure-V within seven days of assumption of the charge of the post by the incumbent.

vi. FPT criteria prescribed in these regulations are continuous in nature. Therefore, all persons subject to FPT shall immediately submit any change in the information already submitted to SBP. Violation of the instructions, circumvention, concealment, misreporting and delay in submission of information to SBP may result in punitive action.

Regulation 2

Composition of the Board

At least one third or two members, whichever is higher, of the Board of Directors of a credit bureau must be independent.

Regulation 3

Restriction on Shareholding by Financial Institutions

No Financial Institution or its sponsor shareholders shall directly or indirectly own 10% or more shares of a credit bureau. This limit will be calculated by adding shareholding of Financial Institution and their sponsor shareholders.

Regulation 4

Compliance Officer
The credit bureau shall appoint an officer to ensure compliance with its operational procedures, relevant laws and regulations. The incumbent reporting to CEO should have necessary authority, access to relevant information and adequate resources.

Regulation 5

Information System Audit
Pursuant to section 24(3) of the Act; the credit bureau shall carry out Information System (IS) Audit every year through any third party audit firms included in the panel of auditors maintained by SBP. The report of such audit shall be shared with the credit bureau and submitted to SBP simultaneously. It must be ensured that the task is not assigned to an audit firm for more than three consecutive years. This IS Audit requirement is in addition to the annual audit of the books of account as required in terms of section 13 of the Act.

Regulation 6

Contents of Credit Information Report
The credit information report provided by the credit bureau shall not contain any information other than prescribed in Annexure-VI.

Regulation 7

Data Update Frequency
The credit bureau shall collect data from member entities on monthly basis within 10 days following the month to which it pertains. The credit bureau shall update the complete data within fifteen days following the month to which it pertains.

Any interim record update/amendment request by the member entities shall be made through a system generated process which will be updated on the same day it is received.

The information relating to credit application shall be processed and reflected in the database not later than next working day.

Regulation 8

Maximum Fee for Disclosure of Source of Credit Information
The credit bureau shall not charge fee exceeding Rs.100/- for disclosure of source of credit information to a debtor.

Regulation 9

Record Keeping
The credit bureau shall retain data as mentioned hereunder:-

	Nature of Data	**Retention Period**
1	Credit reports and related data	Minimum 15 years.
2	Complaints	Three years after disposal of the complaint.
3	Complaints escalated to courts	Three years after decision of the court.

Regulation 10

Agreement with Member Entities

The credit bureau shall enter into a formal agreement with the member entities with whom it has data sharing arrangements. The agreement should inter alia take into account:-

a) explicit clauses requiring the member entities to provide the credit bureau true, accurate, complete, and updated information as per defined frequency and timeframe.
b) confidentiality, privacy and security of information.
c) dispute resolution mechanism and responsibilities of each entity in relation to resolution of complaints.

The agreement shall not include any clause that is in contravention of any law, credit bureaus rules and regulations. The bureau shall keep SBP updated about the entities with whom it has data sharing agreement.

Regulation 11

Outsourcing Arrangement with Third Parties

The credit bureau may outsource any function, except data base management system, to a third party subject to the condition that the arrangement does not:-

a) breach privacy of credit information.
b) impede efficiency of credit bureau's services to the members.
c) compromise security standards as defined in regulation 12.

Regulation 12

Accuracy and Security of Credit Information Files and Credit Reports

The credit bureau shall take the necessary security and control measures to avoid unauthorized access, improper use or mismanagement of information without compromising efficiency of its services. Credit bureau is required to adhere to Information System Security Standards as prescribed in Annexure-VII of these regulations.

Regulation 13

Dispute Resolution

The credit bureau shall put in place complaint handling and dispute resolution policy and procedures. The credit bureau shall ensure that:-

a) the complaint handling function is given adequate resources to act effectively.
b) all complaints lodged are acknowledged.
c) complaints are taken up with the respective credit information provider at the earliest but not later than two working days.
d) complainant is provided reasonable explanation/resolution within 10 days.

The credit bureau shall place on their websites the address, phone & fax numbers and email address for lodging complaint. The name, designation and contact details (phone, fax, e-mail, mobile number, etc) of person so identified be sent to BC&CPD. The designated person shall also serve as the contact person for complaints forwarded to/by SBP.

The credit bureau shall:-

a) maintain record of all requests for correction and its updated status.
b) document the manner in which it was resolved.
c) maintain separate file for errors/omissions/delays occurred at bureaus own level.

ANNEXURE I

ASSESSMENT OF FITNESS AND PROPRIETY (FPT)

The "Fit and Proper Test" (FPT) criteria mentioned in this Annexure are in addition to requirements mentioned in sub section 1 of Section 5 of the Act. The FPT is applicable on the sponsors who apply for a credit bureau license, the investors acquiring more than 10% shares in the credit bureau and for the appointment of Directors, CEO, and Key Executives of the credit bureau.

(A) INTEGRITY, HONESTY AND REPUTATION:

To comply with FPT, it must be ensured that above mentioned person:-

i) has not been subject to any adverse findings or any settlement in civil/criminal proceedings particularly with regard to investments, financial matters/business, misconduct, fraud, formation or management of a corporate body etc by SBP, other regulatory authorities (within or outside Pakistan), professional bodies or government bodies/agencies.

ii) has not contravened any of the requirements and standards of SBP or the equivalent standards/requirements of other regulatory authorities (outside Pakistan as well), professional bodies or government bodies/agencies.

iii) has not been involved with (management or conduct of the affairs of) a company/firm or any other organization that has been refused registration/license to carry out trade, business etc.

iv) has not been involved with (management or conduct of the affairs of) a company/firm whose registration/license has been revoked or cancelled or gone into liquidation or other similar proceedings due to mismanagement of affairs, financial misconduct or mal practices.

v) has not been debarred for being Chief Executive, Chairman, Director, Controlling Shareholder/Sponsor or Key Executive of a company/firm or in similar capacity.

vi) has not been demoted, dismissed or forced to resign from employment or has not been removed by any regulator or government body, in the capacity of employee, director, chairman or key executive of the company/firm or any other position of trust.

vii) has not been associated as director and/or chief executive with the corporate bodies who have defaulted in payment of Government duties/taxes etc.

(B) QUALIFICATION & EXPERIENCE:

This section shall apply separately for Directors, CEO and Key Executives of credit bureau as under: -

i. **Directors on the Board**
   a. must have management/business experience of at least 5 years at senior level in an active capacity.
   b. minimum qualification for a person to be appointed as Director on the Board of a credit bureau is graduation. Higher education accomplished in finance may be an added qualification.

ii**. Chief Executive Officer /Managing Director**

a. must have at least 5 years of experience at senior level and posses expertise and skill set to undertake responsibilities of the position effectively and prudently.

b. should have minimum qualification of graduation or equivalent in the discipline of Information Technology, Management, or Finance.

iii**. Key Executive**

must be a qualified professional possessing relevant experience & degree relating to the position.

(C) CONFLICT OF INTEREST:

i. the CEO will not be the Chairman of Board of Directors of the credit bureau.

ii. no member of Senate, National/ Provincial Assembly, Local bodies shall be appointed/ recommended for appointment as Member of Board of Directors and/or Chief Executive Officer/Key Executive of any credit bureau.

iii. no Key Executive shall head more than one functional area. Furthermore, he/she shall not hold directorship in his /her personal capacity:-

a. in a business concern which is also a client of the credit bureau, and

b. in any other financial institution.

ANNEXURE-II

QUESTIONNAIRE FOR ASSESSING "FIT & PROPER TEST"

Please answer the following questions by entering a tick ( ) in the appropriate box. If answer of any of these questions in YES and need explanation, use a separate sheet with proper reference to the question.

Sr. No.	Description	Yes	No
1	Have you ever been convicted / involved in any fraud/forgery, financial crime etc, in Pakistan or elsewhere, or is being subject to any pending proceedings leading to any conviction?		
2	Have you ever been associated with any illegal activity in any business, deposit taking, financial dealing and other business?		
3	Have you ever been subject to any adverse findings or any settlement in civil/criminal proceedings particularly with regard to investments, financial/business, misconduct, fraud, formation or management of a corporate body etc by SBP, other regulators, professional bodies or government bodies/agencies?		
4	Have you ever contravened any of the requirements and standards of regulatory system or the equivalent standards or requirements of other regulatory authorities?		
5	Have you ever been involved with a company or firm or other organization that has been refused registration/license to carry out trade, business etc?		
6	Have you ever been involved with a company/firm whose registration/license has been revoked or cancelled or gone into liquidation or other similar proceedings?		
7	Have you ever been debarred for being Chief Executive, Chairman, Director or Sponsor/Strategic Investor of a company, especially financial institutions?		
8	Have you ever been dismissed/ asked to resign/resigned in Pakistan or elsewhere in order to avoid legal or disciplinary action?		
9	Have you ever been disqualified/ removed by regulators/Government bodies/ agencies?		
10	Have you ever been in default of payment of dues owed to any financial institution in individual capacity or as proprietary concern or any partnership firm or in any private unlisted/listed company?		
11	Have you ever been in default of taxes in individual capacity or as proprietary concern or any partnership firm or in any private listed/unlisted company?		
12	Have you ever been associated as director and/or chief executive with the corporate bodies whose corporate and tax record, including custom duties, central excise and sales tax has been unsatisfactory?		
13	Have you entered into any agreement with any other person(natural or legal) which will influence the way in which you exercise your voting rights or the way in which you otherwise behave in your relationship with the authorized entity?		

14	Are you a director on the Board of Directors of any Financial Institution(s)?		
15	Are you a Chairman, Chief Executive, Chief Financial Office, Chief Internal Auditor, Research Analyst or Trader (by whatever name/designation called) of a Exchange Company (firm or sole proprietorship), member of a Stock Exchange, Corporate Brokerage House?		
16	Are you owing/controlling any Exchange Company or Corporate Entity?		
17	Have you been or are you working as consultant or adviser of credit bureau in which you intend to become a director?		
18	Are you employee of the credit bureau?		
19	Are you employee of a company/entity/organization where sponsor shareholders of credit bureau/FI have substantial interest?		
20	Are you a member/office bearer of any political party or member of Senate/National/Provincial Assembly/Local Body?		
21	If independent director, have you enclosed declaration in this behalf?		
22	Any other information that is relevant for the purpose of SBP and needs to be mentioned?		

Signature_____

Name _____

Position _____

Date _____

ANNEXURE-III

PROFORMA – FITNESS & PROPER TEST for CEO/Directors/Sponsors

Photo 1 × 1 1/2

Full Name			
Father's Name			
Date of Birth	Place of Birth		Nationality (ies)
(dd/mm/yyyy)	(City and Country)		
NTN Number	C.N.I.C. No		N.I.C. No (Old)
Telephone Number(s)	Mobile Number (s)		Passport Number (for foreign national)
Present Residential Address in Full			
Permanent Residential Address in Full			
Academic Qualification			
Qualification	Name & Address of Degree Awarding Institution		Date of Completion
Professional Qualification			
Qualification	Name & Address of Degree Awarding Institution		Date of Completion
Training(s); if any			
Previous Employment(s) (date-wise)			
Designation	Department		Telephone Number (s)
Official Address			

Please provide complete and true particulars of all business(es), including proprietary concern / partnership firms , companies , in which you have been associated as a proprietor, partner or a director thereof during the last ten years and the accounts maintained by them:		
Name of the Proprietary Concern / Partnership Firm / Company	Name of Bank and / or NBFIs Together with Name of Branches	Account Number (s)

Position held during the last ten years (along with name and address of company / institution / body where appointment held, nature of the company / institution / body and dates of appointment)

Position of the shares held in the Credit Bureau	Number of shares held as of
As of Sponsor Shareholder • Own name • In name of your company • In name of your family member Other than Sponsor Shareholder • Own name • In name of your company • In name of your family member	

Amount of Subscription	
Subscription as % of total paid up capital	
Personal Net worth	

Relationship with other Sponsor Director

Name	Relationship

(Signature of Concerned Director / Sponsor)

ANNEXURE-IV

Affidavit

(On Non-Judicial Stamp Paper)

I, _____ son/daughter/wife of _____ adult, resident of_____

and holding CNIC No. _____ do hereby state on solemn

affirmation as under:-

a. that the deponent hereby confirm that the statement made and the information supplied in the attached questionnaire and the Annexure-I and the answers thereof are correct and that there are no other facts that are relevant for "Fit and Proper Test".
b. that the deponent undertake that the State Bank of Pakistan may seek additional information from any third party it deems necessary in view of assessing "Fit and Proper Test".
c. that the deponent undertake to bring to the attention of the State Bank of Pakistan any matter which may potentially affect my status as being someone fit and proper as and when it crops up; and
d. that whatever is stated above is correct to the best of my knowledge and belief and nothing has been concealed there from.

DEPONENT

The Deponent is identified by me

Signature_____

ADVOCATE (Name and Seal)

Solemnly affirmed before me on this _____ day of _____ at _____ by the Deponent above named who is identified to me by _____, Advocate, who is known to me personally.

Signature_____

OATH COMMISSIONER FOR TAKING AFFIDAVIT

(Name and Seal)

ANNEXURE-V

PROFORMA – FITNESS & PROPERIETARY OF KEY EXECUTIVES

Position and grade held by the executive	
Date of assumption of current position	(dd/ mm/ yy)

Photo 1 × 1 1/2			
Full Name			
Father's Name			
Date of Birth	Place of Birth		Nationality (ies)
(dd/mm/yyyy)	(City and Country)		
NTN Number	C.N.I.C. No		N.I.C. No (Old)
Telephone Number(s)	Mobile Number (s)		Passport Number (for foreign national)
Present Residential Address in Full			
Permanent Residential Address in Full			
Academic Qualification			
Qualification	Name & Address of Degree Awarding Institution		Date of Completion
Professional Qualification			
Qualification	Name & Address of Degree Awarding Institution		Date of Completion
Training(s); if any			
Previous Employment(s) (date-wise)			
Designation	Department		Telephone Number (s)
Official Address			
Telephone Number (s)			

Has ever been convicted of any offence		Yes	No
If yes, nature of offence and penalty imposed			

Has ever been censured or penalized by any financial regulator (local or foreign)?		Yes	No
If yes, reasons for adverse findings and amount of penalty imposed (if any)			

Have you ever been dismissed from employment		Yes	No
If yes, name of the employer and reason for dismissal			

(Signature of the concerned official) **(Signature and stamp of employer)**

Annexure-VI

Contents of credit information Report.

Individual Debtor/ Sole proprietorship Report (CNIC/PASSPORT Based)

- **Personal information**

1.	Title of the debtor. (i.e. Mr./ Mrs./ Ms/ Miss/ Mst. etc.)
2.	Name
3.	Father/Husband's name
4.	Gender
5.	Date of Birth
6.	Computerized National Identity Card /Passport Number
7.	Old National Identity Card number
8.	National Tax Number
9.	Nationality (in case of foreign national)
10.	Present Address
11.	Permanent Address
12.	Profession/Occupation

- **Borrower's Type** (Consumer/Small Enterprise/Medium Enterprise/Microfinance/Agriculture/Commercial)
- **Credit Details(Facility Wise)**

1.	Position as of (date)
2.	Date of sanction/approval
3.	Expiry/maturity date
4.	Product (i.e. cash finance, credit card, L/C, etc)
5.	Secured/Un-Secured
6.	Detail of security /collaterals
7.	Type of Loan (Term/Evergreen)

8.	Sanctioned Limit
9.	Repayment frequency
10.	Outstanding Balance (Principal, Markup, Fee/Penalty)
11.	Minimum Amount Due
12.	Date of Last Payment made
13.	Detail of overdue (30+, 60+, 90+, 120+ 150+, 180+)
14.	Nature of Loan Classification(Subjective/Objective)
15.	Type of Loan Classification(Regular/OAEM/Doubtful/Sub-Standard/Loss)
16.	Number of Repayment cheques bounced for last two years
17.	Detail of type of write off /waiver • Type (Forced/Settled) • Amount • Date
18.	Detail of recovery of write off /waiver • Date • Amount
19.	Amount under litigation
20.	Detail of Re-Scheduling/Re-Structuring • Date • Amount
21.	Detail of late payments (1-15 days, 16-20 days, 21-29 days, 30+days) for last two years

- **Details of settlement of loans for last five years**

1.	Relationship Date
2.	Product Name (i.e. cash finance, credit card, L/C, etc)
3.	Approval Date
4.	Maturity Date
5.	Total Limit
6.	Last Payment Made (Date of Settlement)

- **Detail of personal guarantees given by the debtor**

1.	Product Name (i.e. cash finance, credit card, L/C, etc)
2.	Name of principal borrower
3.	CNIC of principal borrower
4.	Amount of Guarantee
5.	Date of Guarantee
6.	Date of Invocation(if any)

- **Details of Co-borrower of debtor**

1.	Name of Principal Borrower
2.	CNIC of Principal Borrower

- **Details of Credit enquiries regarding debtor made by the users for last two years**

1.	Enquiring Financial Institution Category (i.e. Commercial Bank, Leasing Company, Modaraba etc.)
2.	Enquiry Date

- **Details of status of credit application(s) for last two years**

1.	Financial Institution Category (i.e. Commercial Bank, Leasing Company, Modaraba etc.)
2.	Date of application
3.	Amount of facility
4.	Product Name (i.e. cash finance, credit card, L/C, etc)
5.	Status(Approved/Rejected/In-process)

- **Details of Bankruptcy cases**

1.	Name of Court
2.	Date on which bankruptcy has been declared

- **Remarks column for reporting interim updates**

Corporate Debtor Report

- **Personal information**

1.	Name
2.	Type of Borrower (i.e. Listed Company, Partnership, Trust, Leasing company etc.)
3.	Type of Business (i.e. Agriculture, Sugar, Cement, Textile, etc)
4.	Registered address
5.	National Tax Number

- **Credit Details(Consolidated)**

1.	Position as of (date)
2.	Type of Credit/Exposure(Loans/Investments)
3.	Sanctioned Limit • Fund based • Non Fund based
4.	Outstanding Balance (Principal, Markup, Non fund based)
5.	Detail of Overdue (90+, 180+, 365+)
6.	Detail of type of Write off /Waiver • Type (Forced/Settled) • Amount
7.	Detail of recovery of Write off /Waiver • Date • Amount
8.	Amount under litigation
9.	No. of times Re-Scheduling/Re-Structuring

- **Names of Group Entities of debtor**
- **Details of Credit enquiries regarding debtor made by the users for last two years**

1.	Enquiring Financial Institution Category (i.e. Commercial Bank, Leasing Company, Modaraba etc.)
2.	Enquiry Date

- **Details of status of credit application(s) for last two years**

1.	Financial Institution Category (i.e. Commercial Bank, Leasing Company, Modaraba etc.)
2.	Date of application
3.	Amount of facility
4.	Product Name (i.e. cash finance, credit card, L/C, etc)
5.	Status(Approved/Rejected/In-process)

- **Details of Bankruptcy cases**

1.	Name of Court
2.	Date on which bankruptcy has been declared

- **Remarks column for reporting interim updates**

Annexure-VII

CREDIT BUREAUS INFORMATION SYSTEMS SECURITY STANDARDS
(In terms of Sub-section 2 of Section 24 of the Act)

This Annexure to the Credit Bureaus Regulations sets out Information Systems Security Standards to which credit bureau licensed under the Act must adhere to. These standards have been developed on the basis of the Control Objectives for Information Technology (COBIT) which are the most widely used Information Systems and Control and Security Standards.

1. Data Management

Critical databases and data should be protected so that data remains complete, accurate and valid during its collection, vetting and cleaning, storage, and reporting. There should be an effective combination of application and general controls over the IT operations and different data transmission modes to ensure the security and integrity of data. Transmission of Data to and from member entities should be protected against unauthorized access and corruption. Techniques such as encryption, checkpoint restarting and compression should be used. Electronic data transmission should include security for web based delivery channels using Internet or dial-up connectivity features. Integrity of credit databases should be ensured by automating data collection and reporting, and data consumption and analysis processes. The sensitive data is effectively encrypted in the databases using tools provided by the database vendors. Further, if the data is to be migrated to any environment other than production, such as development or test environment, the data should be irreversibly masked using techniques like anonymization and de-identification etc. The following should also be considered for ensuring data integrity and security:

- input, processing and output controls
- authentication and integrity
- data ownership
- data administration policies

2. Availability of Data

Data should be available at all times for both internal users who access the Bureau's databases via internal Local Area Networks and remote users who access the Bureau's System over a Wide Area Network. Data availability should be ensured to provide seamless Business to Business integration to strengthen relationships with partners and customers. The following should be considered for ensuring data availability:

- source document controls
- media identification, movement and library management
- data back-up and recovery
- data administration policies

3. Access Controls

There should be adequate logical access controls for internal users and remote users of member entities, which ensure that access to the Bureau's networks, systems, databases, data and programs is restricted to authorized users. User identification and authorization profiles should be maintained on a need-to-have and need-to-know basis. Appropriate authorization, user authentication and access controls should be implemented to control and monitor access to files and print services from remote locations.

4. Management of Physical Facilities

IT facilities, equipment, and personnel should be provided a suitable physical surrounding to protect against man-made and natural risks. The installation of suitable environmental and physical controls around the Bureau's servers should be in place, which should be regularly reviewed for their proper functioning taking into consideration:

- access to facilities
- physical security
- business continuity planning and crisis management
- personnel health and safety
- preventive maintenance policies
- environmental threat protection

  automated monitoring

5. Systems Security

System security should be ensured to safeguard information against unauthorized use, disclosure or modification, damage or loss. The systems security policies and procedures should take into consideration:

- the confidentiality and privacy requirements of the Bureau's data,
- audit and system logs,
- cryptographic key management,
- virus prevention and detection firewalls,
- firewalls for filtering remote user traffic and traffic coming from member entities
- centralized security administration,
- incident handling, reporting and follow-up
- tools for monitoring compliance, intrusion testing and reporting.
- data transmitted over wide area networks must be encrypted.

6. Assessment of Internal Controls

The Bureau should carry out an annual audit of its information systems controls and regular procedures for monitoring of audit logs and data change logs to ensure the achievement of internal control objectives set for its IT processes. The Bureau's commitment to monitoring internal controls, assessing their effectiveness, and reporting on them on a regular basis should take into consideration:

- responsibilities for internal control
- audit and system logs
- ongoing internal control monitoring
- benchmarks
- error and exception reporting
- self-assessments
- management reporting
- compliance with legal and regulatory requirements

7. Change Management

Change management policies and procedures should be developed and implemented to minimize the likelihood of disruption, unauthorized alterations and errors. A management system should be put in place, which provides for the analysis, implementation and follow-up of all change requests. The following should be considered:

- identification of changes
- categorization, prioritization and emergency procedures
- impact assessment

- change authorization
- release management
- software distribution
- use of automated tools
- configuration management

8. Business Continuity

Continuity and availability of IT services, Bureau databases and networks should be ensured to minimize business impact in the event of a major disruption. There should be an operational and tested IT continuity plan which is in line with the overall business continuity plan and its related business requirements. The plan should take into consideration:

- criticality classification
- assessment of single points of failure
- alternative procedures
- back-up and recovery
- systematic and regular testing and training
- monitoring and escalation processes
- internal and external organizational responsibilities
- business continuity activation, fallback and resumption plans
- risk management activities

9. Incident Management

IT security related problems and incidents should be managed appropriately to ensure timely resolution. The causes of such problems should be investigated to prevent any recurrence. A problem management system which records and escalates all incidents should take into consideration:

- audit trails of problems and solutions
- timely resolution of reported problems
- escalation procedures
- incident reports
- accessibility of configuration information
- supplier responsibilities
- coordination with change management

10. Software Acquisition and Maintenance

The Bureau must have documented standard policies and procedures for acquisition and maintenance of software applications taking into consideration:

- functional testing and acceptance
- application controls and security requirements
- documentation requirements
- enterprise information architecture
- System Development Life Cycle methodology
- user-machine interface
- package customization

11. Software Implementation and Quality Assurance

Installing and accrediting systems, including formal software installation migration, conversion and acceptance plans, should be in place to verify and confirm that the solution is fit for its intended purpose.

12. Configuration Management

Configuration management controls should be implemented to account for all IT components of the Bureau's system, prevent unauthorized alterations, verify physical existence and provide a basis for sound change management. These controls should identify and record all IT assets and their physical location, and a regular verification program which confirms their existence.

13. Process Monitoring

IT processes and system logs should be monitored by the Bureau's technical team on a regular basis to ensure achievement of the performance objectives. They should incorporate the definition of relevant performance indicators, the systematic and timely reporting of performance and prompt action upon deviations. They should take into consideration:

- scorecards with performance drivers and outcome measures
- participating banks and FIs satisfaction assessments
- management reporting
- knowledge base of historical performance
- external benchmarking

14. Service Level Agreements

A formal process for defining and managing service levels should be followed by the Bureau's management to establish a common understanding of the level of service required by the Bureau and member entities. The establishment of service-level agreements should formalize the performance criteria against which the quantity and quality of service would be measured. Formal agreements should consider:

- definition of responsibilities
- response times and volumes
- integrity guarantees
- non-disclosure agreements
- customer satisfaction criteria
- monitoring and reporting

15. Third Party Services

It should be ensured that the roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy the Bureau's data security, integrity and availability requirements.

16. Risk Assessment

Risks should be assessed for responding to threats by reducing complexity, increasing objectivity and identifying important decision factors. The Bureau should engage itself in IT risk-identification and impact analysis, involving multi-disciplinary functions and taking cost-effective measures to mitigate risks by taking into consideration:

- risk management ownership and accountability
- different kinds of IT risks (technology, security, continuity, regulatory, etc.)
- defined and communicated risk tolerance profile
- root cause analyses and risk brainstorming sessions
- quantitative and/or qualitative risk measurement
- risk assessment methodology
- risk action plan
- timely reassessment

17. Independent Assurance

Independent assurance should be obtained by the Bureau's management to establish confidence and trust among the organization, member entities, and third-party providers. Independent assurance reviews should be carried out at regular intervals that should consider :

- independent certifications and accreditation
- independent effectiveness evaluations
- independent assurance of compliance with laws and regulatory requirements such as the Electronic Transaction Ordinance, SBP's IT Security and Business Continuity Guidelines etc.
- independent assurance of compliance with contractual commitments
- third-party service provider reviews and benchmarking
- performance of assurance reviews by qualified personnel
- proactive audit involvement

18. Compliance with External Requirements

The Bureau's management should ensure compliance with external requirements, such as legal, regulatory and contractual obligations which should provide the framework for security policies and procedures. External requirements should be identified and analyzed for their impact on IT controls and security, and appropriate measures should be taken to comply with them by taking into consideration

- laws, regulations and contracts
- monitoring legal and regulatory developments
- regular monitoring for compliance
- privacy
- intellectual property

(Muhammad Akmal)
Director