PAKISTAN STOCK BROKERS ASSOCIATION

(A company setup under section 42 of the Companies Act 2017)

Regd Office: Mezzanine Floor, Trading Hall, Stock Exchange Building, Stock Exchange Road, Off I.I Chundrigar Road, Karachi.

Tel: 021-32401278, E-mail: secretariat@psba.pk, Web: www.psba.pk, Fax: 021-32401279

PSBA/Notice-099 June 5, 2023

NOTICE FOR MEMBERS

AWARENESS SESSION ON MINIMUM INFORMATION SECURITY STANDARDS AND BROKER FIDUCIARY RATING

Respected Members,

Reference is made to the awareness sessions on Minimum Information Security Standards held on June 01, 2023, and Broker Fiduciary Rating held on June 2, 2023.

As requested during the sessions please find enclosed herewith the presentations of the above-mentioned sessions.

Thank you,

_____**sd**_____
AKBER ALI
Officer - Secretariat

Copy to:

1. PSBA Website

MINIMUM INFORMATION SECURITY STANDARDS FOR COMPLIANCE BY SECURITIES BROKERS

JUNE 01,2023

PAKISTAN STOCK EXCHANGE LIMITED

KEY CONTENTS OF EXISTING INFORMATION SECURITY POLICIES

Pakistan Stock Exchange Limited (PSX) presently has two policies relating to information security, one pertaining to Internet Based Trading Services (IBTS) and the other Application Security Standards, Specification Requirements (ASSSR). The key requirements amongst other available in the documents are given below:

IBTS	ASSSR
Information Security Management	Responsibility of Multiple Stakeholders
Security Reviews and Penetration Testing	Testing and Certification
Security Incident Investigation and Reporting	Vendor Eligibility Criteria
Access Control	Access Control
Controls for Connectivity Devices	Web Application Security Controls
Anti Virus and Malware Protection	Data Preview Export and Transfer Controls
Server Controls and Security Monitoring	Input Handling

KEY CONTENTS OF INFORMATION SECURITY STANDARDS

The key contents in the proposed Standards are as following:

1. Responsibilities of Broad Of Directors
2. Human Resource Security Standards
3. Asset Management Standards
4. Access Controls Standards
5. Data Security Standards
6. Physical and Environmental Security Standards
7. Operations Security Standards
8. Network and Communications Security Standards
9. Patch Management Standards
10. Supplier Management Standards
11. Remote Connectivity Standards
12. Information Security Posture Review & Assessment Standards
13. Application Security Standards
14. Incident Management Standards
15. Testing and Certification Standards
16. Business Continuity Plan (BCP) and Disaster recovery (DR) Standards
17. Compliance and Audit Standards

GAP ANALYSIS

CONTENTS OF EXISTING POLICIES	REVISION IN STANDARDS
RESPONSIBILITIES OF BOARD OF DIRECTORS Not Available.	**RESPONSIBILITIES OF BOARD OF DIRECTORS** ▪ The Board shall review, approve and ensure implementation of a comprehensive Information Security Policy. ▪ The Board shall ensure proper allocation of resources, take remedial actions to address deficiencies and conduct periodic training for the awareness of employees.
HUMAN RESOURCE SECURITY STANDARDS Not Available.	**HUMAN RESOURCE SECURITY STANDARDS** ▪ Skilled staff with segregated duties and responsibilities. ▪ Protecting the data confidentiality. ▪ Security awareness trainings. ▪ Signing a confidentiality or non-disclosure agreement.
ASSET MANAGEMENT STANDARDS Not Available.	**ASSET MANAGEMENT STANDARDS** ▪ Maintain an asset inventory. ▪ Adequately protect assets from unauthorized access. ▪ Identification of assets owner. ▪ Information Classification Levels should be defined considering CIA. ▪ Formulation of internet access policy.

GAP ANALYSIS (continued)

CONTENTS OF EXISTING POLICIES	REVISION IN STANDARDS
ACCESS CONTROL STANDARDS Inactive sessions should be locked/terminated after **30 minutes of inactivity.**	**ACESS CONTROL STANDARDS** Inactive sessions should be locked/terminated after a maximum of **15 minutes of inactivity (even shorter time period is encouraged).** No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities unless authorized. All critical systems accessible over the internet should have **Multi-Factor Authentication (MFA).** Access provided to Employees and outsourced staff on critical systems, networks and other computer resources, should be subject to stringent supervision, monitoring and access restrictions. Any Application offered by brokers to Customers containing sensitive, private, or critical data such as IBTS, Back office, RDA etc. over the Internet should only be accessed via password requirement for users.

GAP ANALYSIS (continued)

CONTENTS OF EXISTING POLICIES	REVISION IN STANDARDS
ACCESS CONTROL STANDARDS Passwords shall be at least **8 characters in** length. Passwords shall include a mixture of at least three of the following, a. Uppercase characters (A, B, C …); b. Lowercase characters (a, b, c …); c. Numbers (0, 1, 2 …); and d. Special Characters (!, @, # …).	**ACESS CONTROL STANDARDS** Passwords shall be at least **10 characters** in length. Passwords shall include a mixture of at least three of the following, a. Uppercase characters (A, B, C …); b. Lowercase characters (a, b, c …); c. Numbers (0, 1, 2 …); and d. Special Characters (!, @, # …).

GAP ANALYSIS (continued)

CONTENTS OF EXISTING POLICIES	REVISION IN STANDARDS
Encryption Data shall be stored/transmitted encrypted at all times.	**DATA SECURITY STANDARDS** Critical Data should be stored/transmitted encrypted at all times. Implement strict data access controls amongst personnel. Ensure that the confidentiality of data is not compromised. Access policies for mobile phones, faxes, photocopiers, scanners, etc.
PHYSICAL AND ENVIRONMENTAL SECURITY STANDARDS Not Available.	**PHYSICAL AND ENVIRONMENTAL SECURITY STANDARDS** Unauthorized physical access. Electricity and power backups. Card access systems. Restricted access to removable storage media. Secure disposal or re-use of equipment. Emergency procedures.
OPERATIONS SECURITY STANDARDS Not Available.	**OPERATIONS SECURITY STANDARDS** Installation and configuration of systems. Handling and disposal of removable media. Regular update of malware detection software. Management of audit-trail and system log information. Backup.

GAP ANALYSIS (continued)

CONTENTS OF EXISTING POLICIES	REVISION IN STANDARDS
NETWORK AND COMMUNICATIONS SECURITY STANDARDS Partially available in IT Security Policy for IBTS.	**NETWORK AND COMMUNICATIONS SECURITY STANDARDS** Safeguard the confidentiality and integrity of data transmitting over public networks and mobile applications. Install network security devices, such as firewalls, proxy servers to protect IT Infrastructure exposed to internet. Ensure PSX provided antivirus solution remain installed and operational.
REMOTE CONNECTIVITY STANDARDS Available in IT Security Policy for IBTS.	**REMOTE CONNECTIVITY STANDARDS** Put in place appropriate security controls for remote access services. Protect critical data in-transit (e.g., encryption). Remote connectivity shall be authenticated, preferably by using one-time password such as a token device. Maintain detailed access log. Any software for VPN probes or other such tools shall not be used for any reason.

GAP ANALYSIS (continued)

CONTENTS OF EXISTING POLICIES	REVISION IN STANDARDS
INFORMATION SECURITY POSTURE REVIEW & ASSESSMENT STANDARDS	**INFORMATION SECURITY POSTURE REVIEW & ASSESSMENT STANDARDS** All systems must undergo an **independent security review** and may undergo additional periodic technical security reviews and pen-test. Ensure that the **interconnected systems have commensurate levels of security.**
PATCH MANAGEMENT STANDARDS Partially available in IT Security Policy for IBTS.	**PATCH MANAGEMENT STANDARDS** Patch management procedure to include **identification, categorization, and prioritization** of security patches and updates. Change Management Procedure should be strictly followed which should include testing of patches, where possible before deployment.
SUPPLIER MANAGEMENT STANDARDS Not Available.	**SUPPLIER MANAGEMENT STANDARDS** **Security risks** identification from outsourcing activities as per approved policy. Recovery and contingency arrangements with defined RTO. Suppliers background check engaged to handle sensitive information. Evaluate the feasibility of outsourcing to a Cloud Service Provider. Execute a **Service Level Agreement**. **Sign** a statement of confidentiality and Non-Disclosure Agreement.

GAP ANALYSIS (continued)

CONTENTS OF EXISTING POLICIES	REVISION IN STANDARDS
APPLICATION SECURITY STANDARDS Not Available.	**APPLICATION SECURITY STANDARDS** Encryption should be achieved using **secure algorithms**. Minimum **cryptographic key** length should be 128 bits. Self-signed Digital Certificates, if required, shall be created by applying recognized standards. Application should follow best practices to maintain the confidentiality of data in preview, exports or transfer processes.
WEB APPLICATION SECURITY CONTROLS The application should have protection against common threats, such as, **Injection flaws**, **Broken Authentication & Session Management**, **Cross-Site Scripting (XSS)**, **Insecure Direct Object References**, **Security Misconfiguration**, **Sensitive Data Exposure** , **Missing Function Level Access Control**, **Cross Site Request Forgery**, **Using Components with Known Vulnerabilities**, **Invalidated Redirects & Forwards**	**APPLICATION SECURITY STANDARDS** No Change

GAP ANALYSIS (continued)

CONTENTS OF EXISTING POLICIES	REVISION IN STANDARDS
INCIDENT MANAGEMENT STANDARDS Partially available in IT Security Policy for IBTS.	**INCIDENT MANAGEMENT STANDARDS** **Escalate and report** incidents of security breaches internally to the Board and Senior Management and externally to PSX and to customers if appropriate. Thoroughly **investigate any incident** of loss or destruction of data or systems and adopt measures to strengthen the security. **Maintain incident logs**.
TESTING AND CERTIFICATION STANDARDS To conduct vulnerability assessment or source code review of applications at least once in every two years or whenever there is major change in application/system. The critical and high-risk observations identified as a result of the testing must be rectified **within 6 months of identification.**	**TESTING AND CERTIFICATION STANDARDS** To conduct vulnerability assessment or source code review of applications at least once in every two years or whenever there is major change in application/system. The critical and high risk observations identified as a result of the testing must be rectified at the earliest **but not later than 2 weeks of identification.**

GAP ANALYSIS (continued)

CONTENTS OF EXISTING POLICIES	REVISION IN STANDARDS
BUSINESS CONTINUITY AND DISASTER RECOVERY (DR) STANDARDS High level requirement in PSX Rule Book clause 4.27	**BUSINESS CONTINUITY AND DISASTER RECOVERY (DR) STANDARDS** To have BCP and DR to maintain data and transaction integrity. A BCP and DR should be undertaken with business impact analysis/ assessment. Conduct/perform periodic drills to validate business continuity plan's effectiveness. Employees must be trained in the implementation of BCP/DR procedures. A BCP and DR must be kept up-to-date and reviewed once a year and signed off by the management. **Integrate** the disaster recovery plan with the business continuity plan.

GAP ANALYSIS (continued)

CONTENTS OF EXISTING POLICIES	REVISION IN STANDARDS
COMPLIANCE AND AUDIT STANDARDS Not Available.	**COMPLIANCE AND AUDIT STANDARDS** Ensure compliance with **Clause 4.25, Chapter 9** and **the Guide** on information security standards. Ensure the **audit, vulnerability assessment** and **penetration testing** of systems and procedures by an audit firm once in every two years for IBTS. PSX may conduct **verification, review or inspection of Brokers** to ensure their compliance with the requirements of PSX Regulations from time to time. PSX may require Brokers to **submit audit report** regarding compliance of this Information Security Guide or any part thereof.

THANK YOU

Broker Fiduciary Rating

The Pakistan Credit Rating Agency Limited

June 23

Contents

Securities Brokers Rating Requirements

Securities Brokers Rating Requirements

License	Trading only	Trading and Self-Clearing	Trading and Clearing
Security Brokers Category	-	Broker Fiduciary Rating	Broker Fiduciary Rating
Consultant to the Issue	-	Broker Fiduciary Rating	Broker Fiduciary Rating
Underwriter	-	Broker Fiduciary Rating	Broker Fiduciary Rating
Investment Advisor	-	Broker Fiduciary Rating	Broker Fiduciary Rating

*As defined by the Commission from time to time

Why Broker Fiduciary Rating

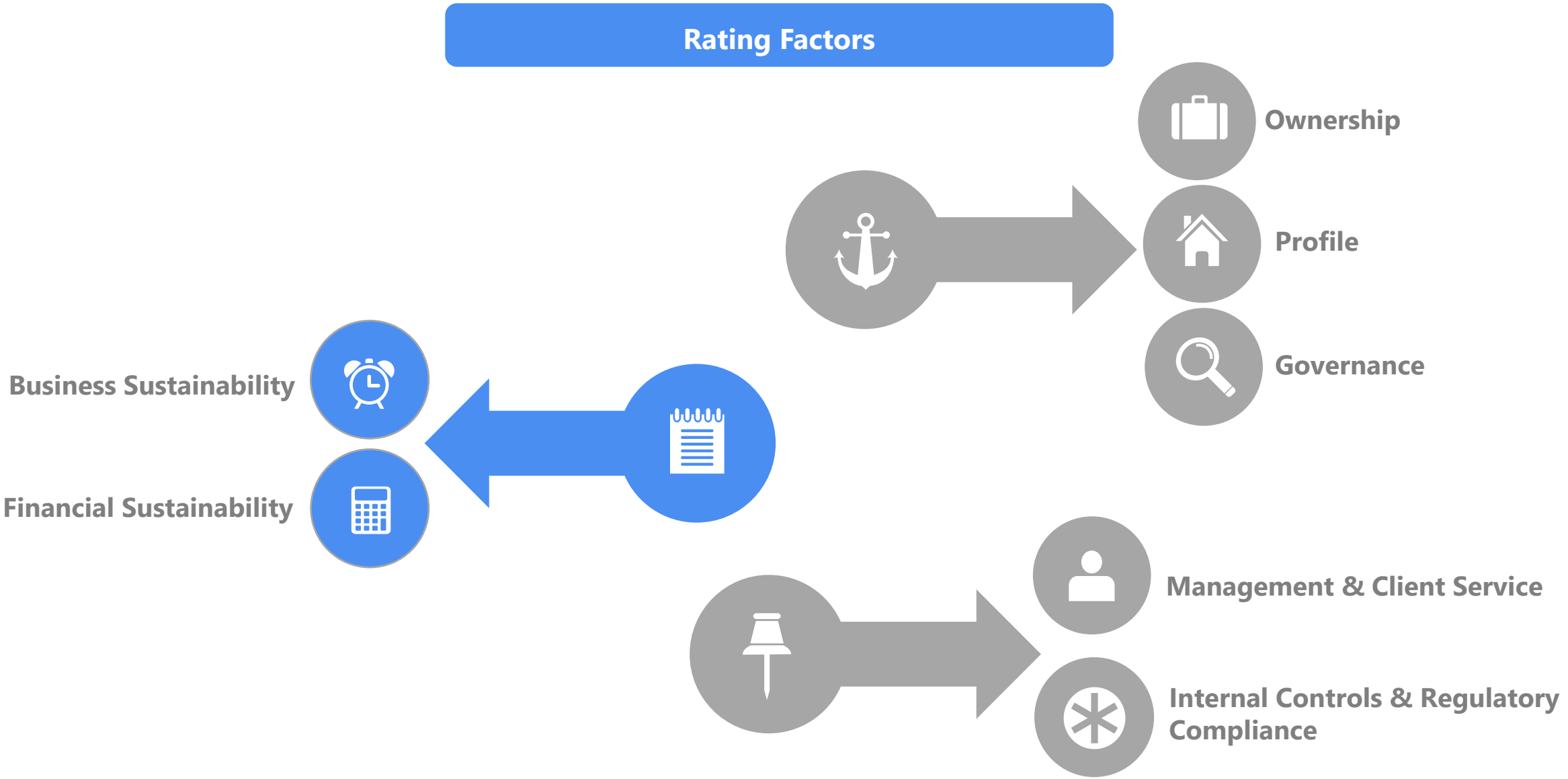
Why Broker Fiduciary Rating

Regulatory Compliance	Distinction within the industry	Benchmarking with best practices
A minimum licensing requirement for Security Brokers applying to: i) Trading & Self Clearing ii) Trading & Clearing A requirement for Consultant to the issue and Underwriter A requirement of Investment Advisors Increase in limit of Assets Under Custody for Trading & Self Clearing category	Differentiates Security Brokers on the basis of Rating More transparency	Improved Governance Practices Improved Client Services Improved Control Environment

*As defined by the Commission from time to time

PACRA's BFR Rating Approach

Rating Approach



Rating Factors

1. Profile

- Background
- Operations

2. Ownership

- Structure
- Stability
- Business Acumen
- Financial Strength

3. Governance

- Board Structure
- Board members profiles & effectiveness
- Transparency

4. Management & Client Services

- Organization Structure
- Management Team
- Client servicing & Complaint management
- Automation/Integration & Continuity of Operations

5. Internal Control & Regulatory Compliance

- Risk Management Framework
- Regulatory Compliance

6. Business Sustainability

- Operating Environment
- Performance
- Strategy

7. Financial Sustainability

- Credit Risk
- Market Risk
- Liquidity Risk
- Capitalization

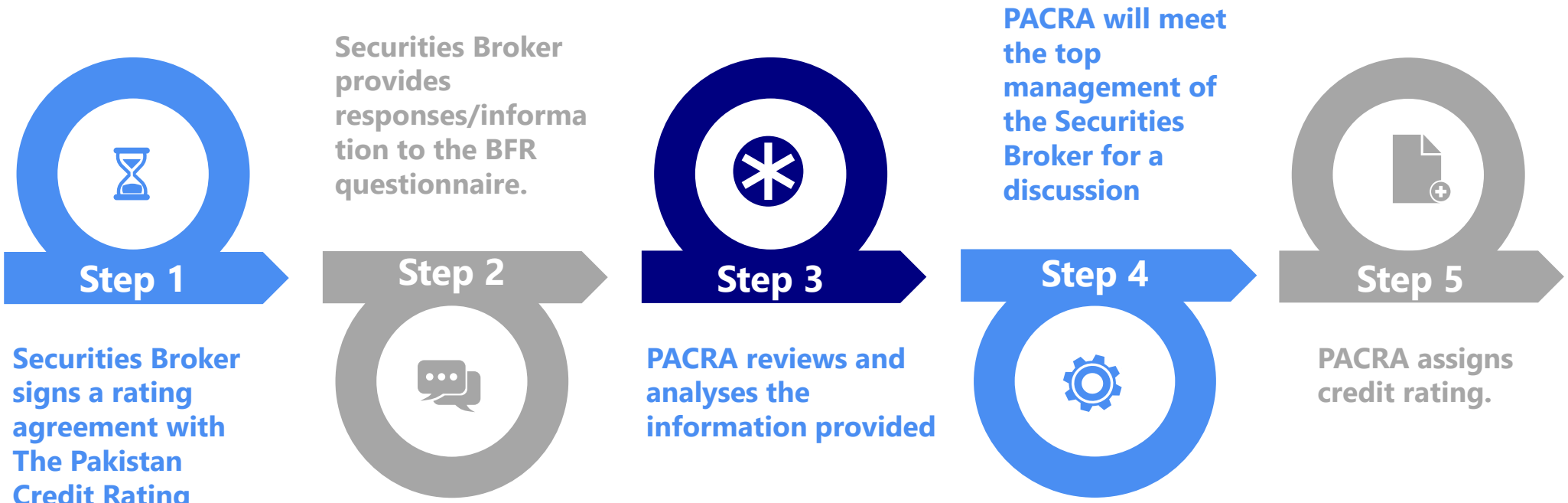
Rating Scale

BFR Rating Scale

Broker Fiduciary Rating Scale	
Symbols	**Definitions**
BFR 1	**Very Strong**. Very strong quality of management, client services and very high likelihood of sustaining operations
BFR 2++ BFR 2+ BFR 2	**Strong**. Strong quality of management, client services and high likelihood of sustaining operations
BFR 3++ BFR 3+ BFR 3	**Good**. Good quality of management, client services and above average likelihood of sustaining operations
BFR 4++ BFR 4+ BFR 4	**Adequate**. Adequate quality of management, client services and average likelihood of sustaining operations
BFR 5	**Weak**. Weak quality of management, client services weak likelihood of sustaining operations

BFR Rating Process Timeline

BFR Rating Process Timeline



* Normal timeline were additional information and discussion are involved time line may increase

Why PACRA

PACRA AT A GLANCE

Pakistan's First Credit Rating Agency | 1994
Initial Shareholding: IFC *(an arm of World Bank)*, Fitch *(one of world's leading rating agency)* and LSE *(Lahore Stock Exchange)*

PACRA - leading Credit Rating Agency in Pakistan with 8,200+ rating opinions spread across 11 financial and 51 corporate sectors - with 600+ outstanding opinions

Current Shareholding: A group of Professionals & LSE FSL

PACRA Rated outstanding instruments amount to PKR 234bln

Largest Analytical Team [A knowledge hub]

PACRA rates over 45% of the KSE 100 companies

Beyond the Borders

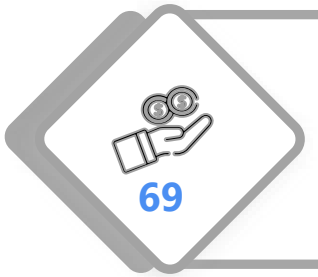
- Sri Lanka | Lanka Rating Agency Limited
- Bangladesh | National Credit Rating

Rating opinion on every third rupee of corporate debt through Banking industry of Pakistan

PACRA Credit Ratings 417

Entity Rating

Opinion on the ability and/or willingness of an entity to meet its financial commitments.



Instrument Rating

Opinion on probability of default on an Instrument

PACRA Specialized Ratings 184

Mutual Funds Rating

Stability Rating / Fund Performance Ranking, Capital Preservation Rating

98

Asset Manager Rating

Opinion on the quality and expertise deployed by an AMC

15

Broker Management/Fiduciary Rating

An independent opinion on the quality of management, client services and sustainability of operations & Performance

31

Insurer Financial Strength Rating

Opinion of an issuer's financial strength and business continuity from a policy holder's prospective.

31

Investment Advisor Rating

A management quality rating provides users with an independent opinion on the management quality, customer service, and investment process of an investment advisor.

1

Project Grading

Opinion on a specific project being managed by any real estate entity. PG differentiates projects on the basis of their individual attributes

1

REIT Manager Rating

Opinion on the quality and expertise deployed by a REIT Manager.

2

REIT Fund

Opinion on investment quality of fund and prospects of successful implementation of underlying real estate projects.

2

Trustee Fiduciary

Opinion on the quality of management, sustainability of operations, and adequacy of systems and controls deployed by a trustee

0

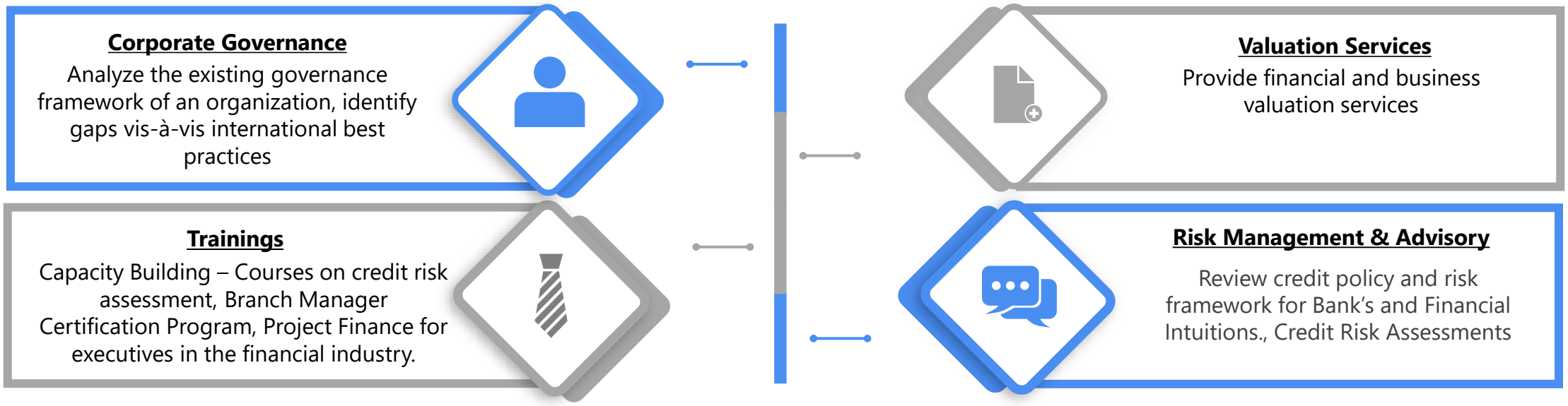
Social Impact & Performance Rating

Opinion on the ability of an entity to create intended social impact and achieve sustainable performance.

3

PACRA Solutions

Services are provided through PACRA Analytics (Pvt.) Limited wholly owned subsidiary of PACRA



Key Takeaways

Key Takeaways

- PACRA is the leading Credit Rating Agency in Pakistan
- PACRA has a rating opinion on every 4th rupee of corporate debt issued
- BFR is one of the minimum **requirements** for Trading & Clearing and Trading & Self-Clearing Brokers.
- A requirement for Consultant to the issue, Underwriter, and Investment Advisory Services
- Differentiates between brokers based on management quality, customer service and sustainability of operations
- BFR has five rating categories from “BFR1” to “BFR5” with BFR1 being the highest.

Fee Structure

Fee Structure

The Minimum Fee is PKR 150,000/- and Maximum Fee is PKR 450,000/-, for Securities Brokers.

The Fee range for each Category of Security Broker is as follows:

The Pakistan Credit Rating Agency Limited

Head Office

FB1 Awami Complex, Usman Block, New Garden Town, Lahore
sameer.khan@pacra.com
+92 333-5049155
Phone +92 42 3586 9504 – 6

Karachi Office

PNSC Building, 3rd Floor, M.T. Khan Road, Lalazar, Karachi
ali.shah@pacra.com
+92 346-2578624
Phone +92 21 35632601

www.pacra.pk