



KFIN TECHNOLOGIES LIMITED

Business Process and general IT controls related to inscope infrastructure

SOC 1 Type 2 Report for the period from 1st April 2021 to 31st March 2022

[As per Statement on Standards for Attestation Engagements ('SSAE') No. 18 and International Standards on Assurance Engagements ('ISAE') No. 3402]



Table of Contents

1.	Report of Independent Service Auditor	3
2.	KFintech's Assertion	8
3.	KFintech's Description of its System and Controls.....	11
3.1.	Scope and Purpose of the Report	11
3.2.	Company history and Overview of Services.....	12
3.3.	Internal Control Framework	13
3.4.	Control Environment	13
3.5.	Risk Assessment Process	16
3.6.	Monitoring Activities.....	16
3.7.	Information and Communications	17
3.8.	Control Activities	20
3.9.	Complementary Subservice Organization Controls	31
3.10.	Complementary User Entity Controls	31
4.	Description of KFintech's Control Objectives and Related Controls	33
A.	Types and Description of Tests of Operating Effectiveness	33
B.	Control Objectives, Control Activities, and Tests Performed	35
4.1.	Unit Corpus Reconciliation	35
4.2.	Net Asset Value	38
4.3.	Branch CPZ	42
4.4.	Non Commercial Transactions	44
4.5.	SIP	49
4.6.	STP	52
4.7.	SWP	54
4.8.	Application Development and Change Management.....	56
4.9.	Operations Management	59
4.10.	Physical Security	61
4.11.	Environmental Safeguards and Backup	64
4.12.	Logical Security	68
4.13.	Third Party Management	72

1. Report of Independent Service Auditor

To: The Board of Directors of KFin Technologies Limited

Scope

We have examined KFin Technologies Limited's (the 'Company' or 'KFintech' or 'Service Organization') description of its Business Process and general IT controls related to inscope infrastructure across the systems used by KFintech (Formerly known as KFin Technologies Private Limited) to provide Qualified Registrar and Transfer Agent (QRTA) Services, Global Fund Services (GFS), Corporate Registry Services, Global Business Services (GBS), Mutual Funds Services and Central Record Keeping Agency (CRA)-National Pension System (NPS) services etc. throughout the period 1st April, 2021 to 31st March, 2022 (the 'Specified Period') (the 'Description'), and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description, based on the criteria identified in "KFintech's Assertion" (the 'Assertion'). The controls and control objectives included in the description are those that management of the Company believes are likely to be relevant to User Entities' internal control over financial reporting, and the description does not include those aspects of the System that are not likely to be relevant to User Entities' internal control over financial reporting.

The scope of this report is limited to Services provided by KFintech from its following facilities:

KFin Technologies Limited – Hyderabad	
1	Selenium Tower B, Plot number 31 and 32 Financial District, Nanakramguda, Serilingampally Mandal, Hyderabad - 500032 Telangana India.
KFin Technologies Limited – Chennai	
2	9th Floor, Capital Towers, 180, Kodambakkam High Road, Nungambakkam, Chennai – 600034

The Company uses Sify Technologies Limited, a subservice organization to avail Physical Infrastructure Security and Datacentre for DR services and CtrlS Datacenters Ltd, a subservice organization to avail DC and IT Infrastructure Datacenter hosting, security implementation and infrastructure and SOC/Cyber Security Managed Services. The description indicates that certain control objectives specified by the Company can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. Our examination did not extend to controls of the subservice organization(s), and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls

The Description indicates that certain control objectives specified in the Description can be achieved only if Complementary User Entity Controls ('CUEC') contemplated in the design of KFintech's controls are suitably designed and operating effectively, along with related controls at the Service Organization.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Our examination did not extend to such CUECs, and we have not evaluated the suitability of the design or operating effectiveness of such CUECs.

Service Organization’s Responsibilities

In Section II of this report, the Company has provided an assertion about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The Company is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; selecting the criteria stated in the assertion; and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (‘AICPA’) and International Auditing and Assurance Standards Board (‘IAASB’). These standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management’s assertion, the Description is fairly presented and the controls were suitably designed and operated effectively to achieve the related control objectives stated in the Description throughout the Specified Period. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a Service Organization’s system and the suitability of the design and operating effectiveness of controls involves the following:

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management’s assertion;
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- Evaluating overall presentation of the description, suitability of the control objectives stated therein, and suitability of criteria specified by the Service Organization in its assertion.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Service auditor's independence and quality control

We have complied with the independence and other ethical requirements of Code of Professional Conduct established by the AICPA.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of User Entities and their auditors who audit and report on User Entities' financial statements and may not, therefore, include every aspect of the System that each individual User Entity may consider important in its own particular environment. Because of their nature, controls at Service Organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, projection to the future of any evaluation of fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a Service Organization may become ineffective.

Description of Tests of Controls

The specific controls tested, and nature, timing, and results of those tests are listed in Section IV of this report.

Emphasis of Matter

Physical security controls have been operational prior to the COVID-19 pandemic and partial based on business requirement post COVID-19. However, due to the pandemic, the Company has been operating in a Work From Home model since early 2020 with minimal occupancy in both HO and Chennai location based on business requirement and including in the specified period. Therefore, most physical security controls were not applicable and did not operate for a majority of the specified period for on-premises verifications.

KFintech in its control activity 10.2 under control objective 10 states that, 'Authorized personnel raises the batch job creation, modification and deletion request through e-mail to the DB team. Upon receiving the request, the jobs are scheduled by designated team'. However, the service auditor noted that this control did not operate during the specified period, as there were no occurrences of batch jobs created during the specified period. Therefore, this control activity could not be tested for operating effectiveness.

KFintech in its control activity 13.4 under control objective 13 states that, 'On a periodic basis, HR Team generates a list of absconding employees those who are continuously absent for more than 2 weeks and uploads the same in HR System and relevant team disables the system, email, door access'. However, the service auditor noted that this control did not operate during the specified period, as there were no occurrences of absconding cases during the specified period. Therefore, this control activity could not be tested for operating effectiveness.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

KFintech in its control activity 1.5 under control objective 1 states that, KFin tech team initiates rectification process if there were any mismatch or changes encountered in the transactions logs during the specified audit period. However, the service auditor noted that this control did not operate during the specified period for the selected sample dates, as there were no occurrences of rectification process done during the specified period. Therefore, this control activity could not be tested for operating effectiveness.

KFintech in its control activity 1.7 under control objective 1 states that, UCR team initiates rectification process within Transaction (T)+1 days to close the batches if any deviant transaction were identified in the transactions logs during the specified audit period. However, the service auditor noted that this control did not operate during the specified period for the selected sample dates, as there were no occurrences of rectification process done during the specified period. Therefore, this control activity could not be tested for operating effectiveness.

KFintech in its control activity 2.7 under control objective 2 states that, KFin tech team raises incident if any deviations were identified then it is moved to the objection queue to resolve the issue. However, the service auditor noted that this control did not operate during the specified period for the selected sample dates, as there were no occurrences of deviation identified and moving it to the objection queue during the specified period. Therefore, this control activity could not be tested for operating effectiveness.

KFintech in its control activity 3.6 under control objective 3 states that, Any deviations between the maker and checker entries are flagged by the system as an objection and are put on objection queue where objection team analyse it and resolves within the same day. However, the service auditor noted that this control did not operate during the specified period for the selected sample dates, as there were no occurrences of deviation identified and moving it to the objection queue during the specified period. Therefore, this control activity could not be tested for operating effectiveness.

KFintech in its control activity 6.4 under control objective 6 states that, the Special Products team registers STP and entries are performed by selecting source and destination scheme for STP if no deviation are identified. However, the service auditor noted that this control did not operate during the specified period for the selected sample dates, as there were no occurrences of deviation identified in the STP process done during the specified period. Therefore, this control activity could not be tested for operating effectiveness.

Opinion

In our opinion, except for the matters of facts described in above paragraph, in all material respects, and based on the criteria described in KFintech's Assertion in section 2:

- a) The description fairly presents the Business Process and general IT controls related to inscope infrastructure across used by KFin Technologies Limited to provide Qualified Registrar and Transfer Agent (QRTA) Services, Global Fund Services (GFS), Corporate Registry Services, Global Business Services (GBS) and Central Record Keeping Agency (CRA)-National Pension

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

KFIN TECHNOLOGIES LIMITED

SOC 1 Type 2 Report – Business Process and general IT controls related to inscope infrastructure

- System (NPS) services, Mutual Funds Services etc. that was designed and implemented throughout the Specified Period.
- b) The controls related to control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls implemented effectively throughout the Specified Period and if the subservice organization and user entities applied the complementary controls assumed in the design of KFinTech controls throughout that period.
 - c) The controls tested, which were those necessary to provide reasonable assurance that the controls stated in the Description were achieved, operated effectively throughout the Specified Period if CUECs and CSOCs assumed in the design of Service Organization's controls operated effectively throughout the Specified Period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV of this report, is intended solely for the information and use of management of the Company, User Entities of the Company's System during some or all of the specified period, and their auditors who audit and report on such user entities financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by User Entities themselves, when assessing the risks of material misstatement of User Entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.



GRANT THORNTON BHARAT LLP

(formerly Grant Thornton India LLP)

Mumbai, India.

08 October, 2022

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

2. KFinTech's Assertion

We have prepared the description of KFin Technologies Limited's ('KFinTech or 'the Company' or 'Service organization') for its Business Process and general IT controls related to inscope infrastructure across the systems used by KFinTech (Formerly known as KFin Technologies Private Limited) to provide Qualified Registrar and Transfer Agent (QRTA) Services, Global Fund Services (GFS), Corporate Registry Services, Global Business Services (GBS), Mutual Funds Services and Central Record Keeping Agency (CRA)-National Pension System (NPS) services etc. throughout the period 1st April, 2021 to 31st March, 2022 (the 'Specified Period') (the 'Description'), for user entities of the system during some or all of the Specified Period, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, when assessing the risks of material misstatements of the user entities' financial statements.

The Company uses Sify Technologies Limited, a subservice organization to avail Physical Infrastructure Security and Datacenter for DR services and CtrlS Datacenters Ltd, a subservice organization to avail DC and IT Infrastructure Datacenter hosting, security implementation and infrastructure and SOC/Cyber Security Managed Services. The description indicates that certain control objectives specified by the Company can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. Our examination did not extend to controls of the subservice organization(s), and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Description indicates that certain control objectives specified in the Description can be achieved only if Complementary User Entity Controls ('CUEC') contemplated in the design of KFinTech's controls are suitably designed and operating effectively, along with related controls at the Service Organization. Our examination did not extend to such CUECs, and we have not evaluated the suitability of the design or operating effectiveness of such CUECs.

We confirm, to the best of our knowledge and belief, that:

- a. The description fairly presents the Business Process and general IT controls related to inscope infrastructure made available to user entities of the system during some or all of the Specified Period as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description:
 - i. Presents how the system made available to user entities of the System was designed and implemented, including:
 - 1) the type of services provided;
 - 2) the procedures, within both automated and manual systems, by which requests for services are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities of the system;
 - 3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

KFin Technologies Limited

(Formerly known as KFin Technologies Private Limited)

Registered & Corporate Office:

Selenium, Tower B, Plot No- 31 & 32, Financial District, Nanakramguda,
Serilingampally Hyderabad Rangareddi, Telangana – 500032, India

CIN : U72400TG2017PLC117649

compliance.corp@kfintech.com

- 4) how the System captures and addresses significant events and conditions, other than transactions;
 - 5) the process used to prepare reports or other information for user entities of the System;
 - 6) the specified control objectives and controls designed to achieve those objectives assumed in the design of the service organization's controls.; and
 - 7) other aspects of our control environment, risk assessment process, information and communication, control activities, and monitoring activities that are relevant to the services provided.
- ii. Includes relevant details of changes to the service organization's system during the period covered by the Description; and
 - iii. Does not omit or distort information relevant to the scope of the KFintech's IT Infrastructure Support Services system, while acknowledging that the Description is presented to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the facility level controls system that each individual user entity of the system and its auditor may consider important in its own particular environment
- b. The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the Specified Period, to achieve those control objectives, if the subservice organization applied the complementary controls assumed in the design of KFintech's controls throughout the Specified Period. The criteria we used in making this assertion were that:
- i. The risks that threaten the achievement of the control objectives stated in the Description have been identified by KFintech;
 - ii. The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved
 - iii. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.
- a) Physical security controls have been operational prior to the COVID-19 pandemic and partial based on business requirement post COVID-19. However, due to the pandemic, the Company has been operating in a Work From Home model since early 2020 with minimal occupancy in both HO and Chennai location based on business requirement and including in the specified period. Therefore, most physical security controls were not applicable and did not operate for a majority of the specified period for on-premises verifications.
 - b) KFintech in its control activity 10.2 under control objective 10 states that, 'Authorized personnel raises the batch job creation, modification and deletion request through e-mail to the DB team. Upon receiving the request, the jobs are scheduled by designated team'. However, the service auditor noted that this control did not operate during the specified period, as there were no occurrences of batch jobs created during the specified period. Therefore, this control activity could not be tested for operating effectiveness.
 - c) KFintech in its control activity 13.4 under control objective 13 states that, 'On a periodic basis, HR Team generates a list of absconding employees those who are continuously absent for more than 2 weeks and uploads the same in HR System and relevant team disables the system, email, door access'. However, the service auditor noted that this control did not operate during the specified

period, as there were no occurrences of absconding cases during the specified period. Therefore, this control activity could not be tested for operating effectiveness.

- d) KFintech in its control activity 1.5 under control objective 1 states that, KFintech team initiates rectification process if there were any mismatch or changes encountered in the transactions logs during the specified audit period. However, the service auditor noted that this control did not operate during the specified period for the selected sample dates, as there were no occurrences of rectification process done during the specified period. Therefore, this control activity could not be tested for operating effectiveness.
- e) KFintech in its control activity 1.7 under control objective 1 states that, UCR team initiates rectification process within T+1 day to close the batches if any deviant transaction were identified in the transaction's logs during the specified audit period. However, the service auditor noted that this control did not operate during the specified period for the selected sample dates, as there were no occurrences of rectification process done during the specified period. Therefore, this control activity could not be tested for operating effectiveness.
- f) KFintech in its control activity 2.7 under control objective 2 states that, KFintech tech team raises incident if any deviations were identified then it is moved to the objection queue to resolve the issue. However, the service auditor noted that this control did not operate during the specified period for the selected sample dates, as there were no occurrences of deviation identified and moving it to the objection queue during the specified period. Therefore, this control activity could not be tested for operating effectiveness.
- g) KFintech in its control activity 3.6 under control objective 3 states that, Any deviations between the maker and checker entries are flagged by the system as an objection and are put on objection queue where objection team analyze it and resolves within the same day. However, the service auditor noted that this control did not operate during the specified period for the selected sample dates, as there were no occurrences of deviation identified and moving it to the objection queue during the specified period. Therefore, this control activity could not be tested for operating effectiveness.
- h) KFintech in its control activity 6.4 under control objective 6 states that, the Special Products team registers STP and entries are performed by selecting source and destination scheme for STP if no deviation are identified. However, the service auditor noted that this control did not operate during the specified period for the selected sample dates, as there were no occurrences of deviation identified in the STP process done during the specified period. Therefore, this control activity could not be tested for operating effectiveness.

Very truly yours,

KFIN Technologies Limited



Venkata Giri Vonkayala
Chief Technology Officer
October 08, 2022

KFin Technologies Limited

(Formerly known as KFin Technologies Private Limited)

Registered & Corporate Office:

Selenium, Tower B, Plot No- 31 & 32, Financial District, Nanakramguda,
Serilingampally Hyderabad Rangareddi, Telangana – 500032, India

CIN : U72400TG2017PLC117649

3. KFinTech’s Description of its System and Controls

3.1. Scope and Purpose of the Report

This report describes the control structure of KFinTech as it relates to the Business Process and general IT controls related to inscope infrastructure throughout 1st April, 2021 till 31st March, 2022 (the ‘Specified Period’). This report, including the description of controls in Section 4 of this report, is intended solely for the information and use of the management of KFinTech, the User Entities of the KFinTech’s system as of Specified Period, and their auditors who audit and report on such User Entities’ financial statements or Internal Control over Financial Reporting (‘ICFR’) and have a sufficient understanding to consider it, along with other information, including information about the controls implemented by User Entities themselves, when assessing the risks of a material misstatement to the User Entities’ financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

The scope of this report is limited to Business Process and general IT controls related to inscope infrastructure rendered by KFinTech offices located as follows:

KFIN Technologies Limited – Hyderabad	
1	Selenium Tower B, Plot number 31 and 32 Financial District, Nanakramguda, Serilingampally Mandal, Hyderabad - 500032 Telangana India.
KFIN Technologies Limited – Chennai	
2	9th Floor, Capital Towers, 180, Kodambakkam High Road, Nungambakkam, Chennai – 600034

Section 4 of this report entails testing of the following domains:

- Unit Corpus Reconciliation;
- Branch CPZ;
- Non Commercial Transactions;
- SIP;
- STP;
- SWP;
- Application Development, Change Management and Infrastructure Change Management;
- Operations Management;
- Physical Security;
- Environmental Safeguards and Backup;

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

- Logical Security; and
- Third Party Management.

The review does not include any other operating environments, locations or delivery centers of KFinTech besides the scope mentioned in section 1 of this report. User Entities and their independent auditors are responsible for determining if services provided to them by KFinTech are in the scope of this report.

3.2. Company history and Overview of Services

KFin Technologies Limited referred as KFinTech throughout this document) Service Organization is located with head office in Hyderabad, and also operates from its Chennai location and serves the essential needs of asset managers with clients spanning mutual funds, AIFs (alternative investment funds), pension (National Pension Scheme), wealth managers and corporates in India and abroad. The company provides Software-as-a-Service (SaaS) based end-to-end transaction management, channel management, compliance solutions, data analytics and other digital services to asset managers across segments, as well as outsourcing services for global players.

The operations expand across 400+ branches in India and 9 countries globally in USA, Canada, UK, Bahrain, Oman, Philippines, Malaysia, Australia, and Maldives. Servicing over 90 million investors, including banks, Public Sector Undertakings (PSU) and mutual funds. This is attainable with a diverse and robust workforce. The key proprietary reporting tools are effective with the relevant business intelligence tools and AMC web applications to take care of key comparative market insights and other MI needs, all with a click.

Corporate Registry Services

KFinTech acts as an agent i.e., Registrar and share transfer agents for listed/unlisted and private company to take up registrar and share transfer related activity in addition to resolving investor grievances and executing corporate action from time to time. On behalf of listed/unlisted and private companies, KFinTech maintains list of shareholders, resolve investor grievances, execute all the corporate actions (bonus issue, rights issue, dividend, redemption of bonds and interest payment etc.) on behalf of clients. In addition, KFinTech offers tech-based solutions and value-added services such as AGM/EGM/NCLT meeting services to KFinTech's clients, E-voting and insta-poll services, Insider trading regulations, Investor Education and Protection Fund (IEPF) claims managing services, Notify general meeting and e-voting, Initial Public Offering (IPO) allotment status, Dividend, and interest pay-out services etc.

Central Record Keeping - National Pension Scheme (NPS)

KFinTech has been serving as a CRA for the NPS for more than 5 years. It acts as an operational interface for all intermediaries in NPS. KFinTech is responsible for record keeping and customer service functions for subscribers of NPS.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Global Business Solutions (GBS)

KFintech's GBS is a Business Process Outsourcing (BPO) and Knowledge Process Outsourcing (KPO) Company providing effective workflow management systems. Its flexibility to scale up outsourcing operations can help optimize delivery capabilities and enhance the value of services. The solutions include Mortgage Services, Transfer Agency Services, Finance and Accounting Services, Legal Services etc.

Global Fund Services (GFS)

Under international investor solutions business, KFintech offer a wide range of services to global asset managers across Malaysia, Philippines and Hong Kong, Middle East and Maldives. KFintech also offer full-fledged localized solutions encompassing core services and digital platforms. KFintech cater to international mutual funds, employee provident funds, private retirement schemes and fund distributors.

KFintech provide the following comprehensive suite of solutions across the ecosystem:

- *Investors:* KYC onboarding, applications processing, online transacting using the mobile application and portals, viewing of statement of account online and supporting all transaction types such as sales and redemption;
- *Distributors:* Agent boarding, commission management, agents' portal and mobile application, statistical summary of investor position and tax statement

3.3. Internal Control Framework

This section provides information about the four interrelated components of internal control at KFintech Service Organization, including KFintech Service Organization's

- Control environment
- Risk assessment process
- Monitoring activities
- Information and communications

3.4. Control Environment

The control environment sets the tone of KFintech Service Organization, influencing the control awareness of the organization. The control environment is embodied by KFintech's awareness of the need for controls and the emphasis given to the appropriate controls through management's actions supported by KFintech Service Organization's policies, procedures, and organizational structure.

The following are the primary elements of the KFintech Service Organization's control environment:

- a. Commitment to integrity and ethical values;
- b. Oversight responsibility of the board of directors;

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

- c. Assignment of authority and responsibility;
- d. Commitment to competence; and
- e. Accountability.

a. Commitment to Integrity and Ethical Values

KFintech Service Organization operates in a highly regulated environment. To this end, KFintech Service Organization has developed a formal code of ethics available on its intranet that contains rules about employee conduct while under the employment of KFintech Service Organization. Employees are required to read and evidence their knowledge and receipt of the KFintech service organization’s code of ethics upon hire and annually thereafter.

The KFintech Service Organization offers its employees a number of channels through which potential breaches of ethical behaviour may be reported.

Reporting to multiple email addresses including but not limited to:

- whistleblower@KFintech.com;
- posh@KFintech.com;
- infosec@KFintech.com;
- incidents@KFintech.com;
- risk@KFintech.com;
- legal@KFintech.com; and
- Compliance@KFintech.com.

b. Oversight Responsibility of the Board of Directors

The control environment at KFintech Service Organization originates with and is the responsibility of the board of directors (board), chief executive officer (CEO), and executive management. The board provides oversight of KFintech Service Organization operations and activities including oversight of the service organization’s investment, Risk Subcommittee and audit committees. The investment committee supervises and controls the service organization’s investment and related financial matters, approves service organization investment policies and guidelines, and reviews the service organization’s investment strategies and investment performance. The audit committee is responsible for reviewing the service organization’s policies and practices related to accounting, financial, and operational controls, and financial reporting. The audit committee is also responsible for directing the activities of KFINTECH Service Organization’s internal audit department and coordinating the activities of the service organization’s external financial auditors.

The internal audit department performs internal audits that help the service organization maintain an effective system of internal control, manage risk, improve customer service, and enhance business performance.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

In addition to the internal audit department, the service organization has established several other Risk and compliance groups dedicated to effective risk management and oversight.

c. Assignment of Authority and Responsibility

Executive management recognizes its responsibility for directing and controlling operations, managing risks, and establishing, communicating, and monitoring control policies and procedures, under the ultimate oversight of the board. Management recognizes its responsibility for establishing and maintaining sound internal control and promoting integrity and ethical values to all personnel on a day-to-day basis.

d. Commitment to Competence

The service organization's commitment to employee competence begins with background checks for all employee candidates and formal hiring practices designed to ensure that new employees are qualified for their job responsibilities. Management has established written competence and performance levels for each job function, including formal promotion and development criteria that help foster professional development for its employees. These criteria are also used to measure employee performance and identify areas for improvement and additional training.

The service organization follows regulatory rules concerning the licensing of personnel in the securities business. Compliance teams monitor license renewals and send update reminders to employees and their supervisors regarding license renewal dates.

The service organization also offers a comprehensive training program including but not limited to:

- NISM (National Institute of Securities Markets) Exam preparation course which is mandatory for Mutual Fund Services;
- Information Security Awareness Training;
- POSH – Prevention Of Sexual Harassment;
- Employee Code of Conduct; and
- Business Service Operations specific process trainings.

e. Accountability

KFintech Service Organization's commitment to an effective system of internal control begins with the service organization's board and its audit committee. The audit committee meets four times a year to fulfill its oversight responsibilities related to the financial reporting process, the system of internal control, internal and external audit activities, and the service organization's process for managing risk and monitoring compliance with applicable laws, regulations, and internal policies and procedures.

The service organization's executive committee meets periodically to oversee critical business operations.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

3.5. Risk Assessment Process

The service organization operates in an environment faced with a variety of risks from internal and external sources.

Objectives

The service organization's risk assessment approach involves an iterative process for identifying and assessing risks to the achievement of the service organization's objectives. This approach forms the basis for determining how risks will be managed by the service organization.

Identification and Analysis of Risks

Risk management is primarily the responsibility of individual business units, which perform periodic risk assessments that identify and document the significant risks facing the service organization, including any fraud risks. The results of these risk assessments determine how the business units develop and implement controls, operating procedures, and compliance processes for addressing and mitigating such risks. Service organization policies require that any instances of suspected or actual fraud be brought to the immediate attention of senior management, the internal audit department, and the service organization's legal department.

3.6. Monitoring Activities

KFintech Service Organization employs a combination of ongoing and periodic monitoring activities to monitor that controls are functioning effectively and that risks are appropriately mitigated.

Ongoing Monitoring

The service organization uses a variety of reports and monitoring mechanisms to help ensure that controls are functioning as intended; these include

- electronic display of pending transactions and their status;
- deficiency and incident reporting;
- suspense account reporting;
- daily pricing variances;
- financial reconciliations;
- quality review results and reporting;
- system processing monitoring and reporting;
- logical security incident logging and review;
- Information and Cyber security weekly dashboards; and

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

- Operations, IT and ITINFRA weekly dashboards.

Management regularly reviews and assesses business operations to determine that reporting and monitoring mechanisms are used and effective in managing the operations of the business, controls, and related risks.

Periodic Assessments and Monitoring

In addition to ongoing monitoring activities described above, each business unit conducts specific evaluations of risks and controls to maximize the effectiveness of its operations.

The internal audit department performs internal audits of operations and controls to assess the effectiveness of controls. The results of audits and any identified deficiencies are reported to management as well as the audit committee. Management prepares and implements corrective measures to address any significant deficiencies.

3.7. Information and Communications

KFintech Service Organization communicates its policies and procedures and other information necessary to help achieve the service organization's business objectives through several means, including the service organization's intranet, emails, newsletters, memoranda, meetings, Infosec awareness, Advisory, Change, Patch, Capacity, Incident, BCP/DR drill, and training sessions. The service organization's policies and procedures enforce the importance of adherence to and compliance with rules and regulations that govern its business and operations.

KFintech Service Organization has also implemented methods of communication to inform User Entities of the role and responsibilities of KFintech Service Organization in processing their transactions and to communicate significant events to User Entities in a timely manner. These methods include KFintech Service Organization's active participation in quarterly user group meetings; the monthly KFintech Service Organization newsletter, which summarizes the significant events and changes during the month and planned for the following month; and the user liaison, who maintains contact with designated User Entity representatives to inform them of new issues and developments. User Entities are also encouraged to communicate questions and problems to their liaison, and such matters are logged and tracked until resolved, with the resolution also reported to the user entity.

For information provided to User Entities, such as reports, statements, data, and other information provided to User Entities, service organization policies and procedures require that all such information be tested to ensure it is sufficiently complete and accurate.

Information Systems Overview

The service organization employs the following IT applications and hardware to provide its defined plan contribution recordkeeping services to its User Entities:

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

- **Antivirus – McAfee EDR for Desktops and TrendMicro for Servers**
 - To prevent malware from causing damage to the KFinTech's Information systems (Desktops/Laptops/Servers) and to detect, neutralize or eradicate malware (malicious software)
- **Microsoft Intune- Mobile Device Management (MDM)**
 - To prevent data leakage on mobile devices, causing damage to KFinTech's Information stored on end points (Mobile devices, Laptops and Desktops)
- **End Point DLP – McAfee**
 - To prevent the accidental exposure of KFinTech's confidential information across all devices, wherever data lives, in transit on the network, at rest in storage, or in use, and to monitor the data and significantly reduce the risk of data loss.
- **Email DLP – Force Point**
 - To manage sensitive data in email messages and to detect content that violates KFinTech's DLP policies
- **PAM – Arcon**
 - To control, monitor, secure and audit all human and non-human privileged identities and activities across KFinTech's IT environment
- **DAM – McAfee**
 - To protect data from all threats by monitoring activity locally on each database server and by alerting or terminating malicious behaviour in real time, even when running in virtualized or cloud computing environments
- **SIEM – IBM Qradar**
 - To aggregate and analyze activity and log data from many different resources such as network devices, host assets and operating systems, applications, vulnerabilities, and user activities and behaviours across KFinTech's entire IT infrastructure
- **Endpoint Web Security – CISCO Umbrella**
 - To proactively block requests to malicious destinations before a connection is even established or a malicious file is downloaded
- **Service Desk Plus / Manage Engine**
 - A ticketing tool implemented in KFinTech, which is an integrated console to monitor and maintain the assets and IT requests generated from the users of the IT resources within KFinTech

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

- **KBOLT (KBolt Plus and KBolt Nxt)**

- KFinTech Branches Online Transaction System. KBOLT is a full-featured application for all ISC needs. One can use this system to enter mutual fund applications, print account statements, get reports or just query investor data. KBOLT has a subscription service for account statements, frequently used reports that enable ISC to set-up an auto-email and get the frequently needed information to their desktops at the time they need it.
- KBOLT has a host of transaction/MIS reports ranging from simple DTR to other complex reports like inflow/outflow reports. KBOLT's online inflow/outflow report empowers AMC's and clients to know the subscription, redemption position at any time. It's drill-down capabilities enable users to get the micro granular information about the underlying transactions. KBOLT's management console empowers head office executives and accounts to monitor the nationwide fund/transaction activity.

- **KBOSS**

- KFinTech Brokerage online system services (BOSS) is the brokerage commission processing platform of KFinTech to support the commission processing team to incorporate the new rate structures received from the AMC and clients, provide access to the AMC to view the existing rate structures and brokerage commission annexures, Processing of commission, provide access to retrieve the commission payment details at folio, transaction level. This tool also provides the tracking of broker empanelment information, AMFI renewal information, Partner Loyalty Program related information to the processing team.

- **TaskMF**

- Transaction accounting system for KFinTech mutual fund (TASKMF). This is an integrated transfer agency platform for providing services to asset management companies (AMC's) and clients based on regulatory requirements.

- **EQRS**

- Electronic Quick Response System (EQRS), is an inhouse developed Back Office System. This application is used to handle the requests of investors without requirements of physical presence or a copy of documents. A complete Scan Image driven application avoiding handling and movement of physical documents across teams. Queries and grievances lodged across all KFinTech branches are immediately available in EQRS for a quick resolution. Also, have built-in mechanisms to trigger alerts to investors and clients regarding the transactions processed at different levels. It has built-in triggers for MIS reports for both Client Relationship Managers and Management. All high-value transactions are routed through the Audit and Surveillance System. In Dividend processing, all payment data is uploaded to payment banks SFTP server from within the application without any manual interaction and checksums

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

provided to the banker for verification of file integrity. User activity and access levels are monitored periodically and are reviewed by Group Relationship Managers. Privileged users' activities are monitored and alerted by email and SMS triggers.

- **Suprema**

- Suprema application has been designed to full fill the needs of CRA operations. This application caters the need of frontend office and back-office operations. All the stake holders like Trustee bank, PFMs, Nodal office and corporates use this application for their day-to-day activities like Subscriber Registration, contribution, service requests and settlement process. It also covers CRA H.O backend operations like Grievance's resolution tracking and extract the reports.

- **iWapp**

- Integrated wealth management, asset and portfolio management platform, Offers wide range of features and services to its clients.
- An online web-based solution for tracking wealth of customers and their families, based on predefined parameters. The application supports decision making on optimizing and rebalancing the customer portfolio.

- **eDost**

- An online web-based solution for tracking wealth of customers and their families, based on predefined parameters. The application supports decision making on optimizing and rebalancing the customer portfolio.

3.8. Control Activities

The service organization has developed variety of policies and procedures including related control activities to help ensure the service organization's objectives are carried out and risks are mitigated. These control activities help ensure that defined contribution plans are administered in accordance with the service organization's policies and procedures.

Control activities are performed at a variety of levels throughout the organization and at different stages during the relevant business process. Controls may be preventive or detective in nature and may encompass a range of manual and automated controls, including authorizations, reconciliation, and IT controls. Duties and responsibilities—such as duties related to the processing and recording of transactions, investment trading, reconciliation activities, application development, compliance, and control monitoring—are allocated among personnel to ensure that a proper segregation of duties is maintained.

A formal program is in place to review and update the service organization's policies and procedures on at least an annual basis. Any changes to the policies and procedures are reviewed and approved by management and communicated to employees.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

- **Central Processing Zone (CPZ)**

CPZ is a key department with the responsibility to create Customer folios, a new purchase, updating additional purchase, redemption registration etc. This is the first department where the investor commercial transactions are processed for further action. **(Control ref. 3.1,3.2,3.5, 4.1,5.1,6.1,7.1)** CPZ transactions.

Activities at CPZ:

- Purchase transactions.
- Redemption.
- Switches.

All purchases, redemptions and Switches (Liquid and non-liquid) are processed at CPZ. Carrying out the above transactions in a timely manner is essential for the generation of Unit Capital Report (UCR) which would form the input document for NAV calculations and also customer Service.

The CPZ team is responsible for processing of all Commercial Transactions through workflow Processing termed as TP. CPZ team performs all the critical activities across subscriptions, redemptions and switched. The team is responsible for the reconciliation of the DTR and to ensure that all the transactions reported for the day from the branches are reconciled and processed as per the request of the unit holder. **(Control ref. 2.4, 3.7)** Timely carrying out the above transactions is essential for the generation of Unit Capital Report (UCR) that would form the input document for NAV calculations and also customer Service. **(Control ref. 2.3, 3.7)** The department carries out the below activities team-wise.

- **Subscription Processing**

The subscription processing team ensures that all subscriptions received for the day are checked for the correctness of documentations and processed. **(Control ref. 3.3, 3.5,3.6,4.12)** All critical investor data is captured at the time of TP, The profile of the investor is created at the time of subscription processing and this critical to data quality in all areas of service. **(Control ref. 4.13, 4.14, 4.16, 5.3, 5.4, 7.2, 7.3, 7.4, 7.5)**

The transactions processed by the team include New Purchases, Additional Purchases, ULIP IC's and RC's, New Purchase with SIP, Existing folios with SIP's, ZSIP's and FMP's.

- **Funding Processing**

Funding is a core process which involves sending funding files to AMC, pay-out files to the banks and finally passing credits to the investors.

- **Dividend Processing**

Dividend Process that is Calculation of Dividend, Dividend funding and SOA/electronic confirmation/rejections to Investors.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

- **Switch Processing**

The switch processing team is responsible for the processing of Switch transactions. The team also ensures the critical activity of reporting high-value NIFTY purchases to the fund manager at regular intervals. This is a critical activity as this has a high impact on UCR.

- **Redemption Processing**

The redemption processing team is responsible for the processing of all repurchase transactions. The team ensures that all repurchase transactions are processed after verification of documents submitted by the unitholders. **(Control ref. 3.3, 3.5,3.6,4.12)** Once the processing is done, the same is confirmed to the UCR team to avoid financial impact.

- **Liquid Purchase processing**

Liquid purchase is a key department with responsibility to create Customer folios, new purchase, updating additional purchase, Liquid purchase banking reconciliation, Date Entry, High-value credit confirmation etc. This is the first department where the investor commercial transactions are processed for further action.

- **Online Web transactions**

The online web transaction team is responsible for the processing of all the commercial transactions done by the investors in online mode. This includes purchases, additional purchases, redemptions and switches. These transactions, reported on the website are ported, endorsed by the team and confirmations are arranged to the investors. This is an automated process, but for the cases where allotment has to be made after the credit is marked to the investments.

- **SIP/ STP/ SWP related**

The special products team is responsible for new registrations of SIP, SWP through Transaction Processing termed as TP. The process is similar to the CPZ as the special Product team functions are just extension of Purchase, Redemption and Switch. The unit also processes cycle transactions through Endorsement activity. In SIP and STP, it is on all four-cycle dates 01st, 07th, 15th and 25th, however, under the daily frequency of STP, transactions are endorsed on a daily basis apart from the specified cycle dates. Timely carrying out the above transactions is essential for the generation of Unit Capital Report (UCR) that would form the input document for NAV calculations and also customer Service. **(Control ref. 7.1, 7.2, 7.3, 7.4, 7,5)**

The department also carries out registration-related activities of all new SIP and STPs reported from Branches through K bolt. Basis on the DTR transactions are getting ported and registered, keeping in view of 15 days TAT for SIP registration, activity is to be completed in time, however, any delay in a day or two can be accommodated as final registration depends on receipt of physical mandates which the department get from across branches within a time frame of 4-7 days depending on the locations.

Registration of a new SIP / STPs is carried out by registering the SIP mandates in the system, generating bank-wise statements listing down the mandates and sending them to the respective

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

banks/Clearing banker, after the bank registration of ECS mandate is confirmed, transactions are ready to be sent in Transaction feed. The SIP cycle is activated. The total TAT for this activity is 21 days. **(Control ref. 6.1, 6.2, 6.3, 6.4)**

Once the above activities are completed, transactions are ready for unit allotment on due dates. This is one of the most critical and crucial activity and needs to be closed within 4-6 hours to avoid any financial impact or delay in updating UCR. **(Control ref. 5.1,5.2, 5.3, 5.4, 5.5, 5.6)**

- **National Pension Scheme (NPS)**

NPS is operated through different intermediaries at different stages, as given below:

- Registration of Subscribers – Application is submitted by the Subscriber and routed through Nodal Offices – to CRA. Permanent Retirement Account is created in the CRA system and PRAN is allotted to the Subscribers by the CRA.
- Deposit of contribution is made by Subscribers to the Nodal Offices (Contribution is deducted from the salary by the Nodal Offices, for Government employees). The funds are remitted by Nodal Offices to the Trustee Bank, with details being uploaded in the CRA system by the Nodal Offices.
- Transfer of funds from Trustee Bank to PFM (as selected) – On reconciliation and as per settlement instructions from CRA
- Changes in Subscriber details (address, scheme preference etc.) - are intimated by Subscribers – routed through Nodal Offices – to CRA system. In case of changes in scheme preference etc., new instructions are accordingly implemented in the daily settlement run by CRA.
- On Exit/ withdrawal - Application is submitted by Subscribers and routed through Nodal Offices – to CRA. On processing, CRA gives instructions to the PFM to transfer the funds to the Trustee Bank. The Trustee Bank would transfer the lump-sum withdrawal to the Subscriber's Bank account and the 'Annuity' amount to the ASP. The Subscriber would thereafter receive monthly payouts from the ASP.

- **Asset Management**

The information assets at KFin Technologies Limited are controlled by identifying owners, custodians and make them accountable for requesting, acquiring, managing, transferring, retrieving, and disposing of assets. KFinTech has identified all its information assets associated with its information and information processing facilities, owners for these assets are identified and an inventory of these assets is maintained, reviewed, and updated for the accuracy and consistency. ITINFRA team will review the inventory of assets at least once in a year. Information assets of KFinTech are classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. All assets are identified and labelled for tracking and identifying. Media that is identified as no longer required by any group or employee of KFinTech is secured by IT team. Facilities, Admin, CISO with the help of the ITINFRA team shall dispose the assets and all such disposal activities must be approval of concern unit head and or Management of KFinTech.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

- **Physical Structure Overview**

KFintech's power systems are designed to provide uninterrupted power, regardless of the availability of power from the local public utilities supplying the office premises; UPS units and backup generators supply power **(Control ref. 11.4)** to the center in the event of a power failure. All components are covered by maintenance contracts and tested regularly. **(Control ref. 11.2)**

Fire Extinguishers and smoke detectors are installed at all sensitive points. Regular check on the working condition is done, warranty is checked, and AMC **(Control ref. 11.4)** is entered on completion of Warranty. Yearly fire drills are conducted in coordination with Admin and HR personnel. **(Control ref. 11.3)** The fire drills reports are collected, and analysis made upon them. Fire and emergency instructions are displayed at prominent locations. **(Control ref. 11.5)**

Media Disposal process ensures that the disposal of unwanted CD's etc., are disposed timely to protect and maintain the security of the information and data.

- **Physical Access**

KFintech has its development center at KFin Technologies Limited, Hyderabad. The entrance is secured with a security person **(Control ref. 10.2)**, Face recognition access control and CCTV surveillance. Physical and Environmental Security of KFintech is controlled and governed by KFintech's ISMS Policy.

Entry to the KFintech offices is restricted to authorized personnel by a Face recognition access control system. **(Control ref. 10.3)** All employees are provided with Employee ID cards. Attendance is recorded through HRIS system. All visitors have to sign the visitors register and are given inactive visitor card. **(Control ref. 10.6)**

The Company's work areas are secured by means of Face recognition access control systems. **(Control ref. 10.3)** Additionally, employees are issued a physical Identity card bearing the employee ID, name and the photograph of the employee.

Employees are subjected to show their ID cards at the Security entrance and get their face recognition in the system to get the access to respective floors. **(Control ref. 10.5)** Employees are granted access only to those areas which they require to access. Some members of the IT Support Team and Administration team have access to the entire facility. The management team has access to all areas except the server rooms. Employees are required to wear their access cards / employee identification cards at all times while within the facility.

CCTV is implemented to monitor the activities in server room and main entrance and other secure zones. Admin Team monitors the CCTV recordings. Logs are generated and communicated to the management periodically. **(Control ref. 10.4)**

ID cards are issued to new employees based on an access requisition initiated by the Human Resource (HR) group. The HR group creates a ticket in helpdesk ticketing application requesting the IT team and Administration / Facilities team to issue an access card to the new employee. The

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

IT / Administration team ensures that the access card/ face recognition in the system controls configured with the appropriate access rights.

On separation of an employee from the organization, the HR group initiates the 'Exit Process' and circulates it to all the concerned groups. Based on this, the employee's privileges in the access control system are revoked. **(Control ref. 10.7)**

The Employee ID card is surrendered by the employee on exit/ termination/ onsite transfer is recovered and face recognition is disabled by the Administration group after providing sign-off on the final clearance form. **(Control ref. 10.7)**

Access by visitors, contractors and/or third-party support service personnel's both entry and exit are monitored by security personnel. Photography, video, audio or other recording equipment, are not allowed inside secure premises, unless specifically authorized. Such accesses are recorded, authorized and monitored. Visitor, contract and/or third-party service personnel to sensitive areas such as data centers are strictly on "need to have" basis and subject to the principle of least privileges.

Visitors to KFinTech premises are required to report in reception area. Visitor's name, Mobile Number, In/Out Time, Purpose of visit, Person to meet, Device details are captured in the visitor register. Visitor details are captured by the main building security facility. Further, for provision of logical access cards for visitors, a formal request must be raised from the business team specifying the number of days for which the access is required. Accordingly, logical access cards are issued for visitors.

- **Access to the Server Room**

Access to the server room is controlled by face recognition access control system. KFinTech policies protect sensitive equipment such as servers, communication and power hubs and controls by locating them in secure and data centers and bonded areas that are not easily visible / accessible to public and apply appropriate controls to mitigate risks from physical and environmental threats and hazards and opportunities for misuse or unauthorized access. Only Authorized personnel are allowed to enter such sensitive areas controlled with face recognition systems. Third parties are allowed access to the server room only under the supervision of IT team members. All KFinTech's critical infrastructure is placed in Datacenters of Primary and DR and access to these Datacenters are restricted to common users.

Access to the datacentre are controlled by logical access cards. Authorized list of users to the datacentre is maintained and the access is reviewed on a quarterly basis and duly recorded.

The building management and Cyber Gateway Building Security is responsible for the initial screening of all employees and visitors entering the shared building premises, as well as capturing the details of the visitors in the building security registers, and confirming whether visitors are expected with the relevant KFinTech employees and KFinTech office security.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

- **User Access Management**

KFintech has established a process for granting, controlling, monitoring, reviewing, and revoking of access to employees, external users of KFintech (KFIN Technologies Limited). **(Control ref. 12.1)** This includes controlling access to Logical, physical, network, system and information resources of KFintech and ensuring their proper usage and safety from being mishandling or destroying through unauthorized manner. Access to the KFintech information assets is allowed based on the requirements of the business applications, information asset classification, and legal and contractual requirements of KFintech. Access to all information assets is generally denied and is granted selectively to only those assets permitted by the information asset owner. Access is controlled by accessibility at Physical perimeter, for the information assets and ensured that access rights to information systems are controlled appropriately, authorized, allocated and maintained as per business requirement. All the employees are provided with basic access to access KFintech information, and any additional access are provided on receiving approval from concern reporting authority and or unit head based on the business requirement and availability of concern authority. **(Control ref. 12.10)** User registration and de-registration shall be controlled, authorized, and a record for controlled passwords shall be maintained by IT team for all critical IT assets. All the access provided to OS, network, databases, storage, and applications are of role based and privileges granted are restricted, controlled and reviewed periodically by concerned authorized, and or Head of ITINFRA. The IT systems team shall deactivate all the user-ID upon termination or resignation of an employee. **(Control ref. 12.3, 12.11)** Access of the employees who are formally transferred from unit or department to other within KFintech shall be modified on formal approval from respective unit Head or reporting authority. Access to the KFintech information systems or services will be provided by ITINFRA team based on the email received from HR team and or approval from concern unit Head. **(Control ref. 12.2)** User access rights shall be reviewed on monthly basis and after any changes, such as users moving or transferring to other units or departments, user getting promoted or demotion or terminated from employment. **(Control ref. 12.5)** On a periodic basis, HR Team generates a list of absconding employees those who are continuously absent for more than 2 weeks and uploads the same in HR System and relevant team disables the system, email, door access. **(Control ref. 12.4)** KFintech has defined and documented password policy stipulating minimum length, password history, password expiry, minimum password age, complexity and account lockout threshold. The password policy is enforced within KFintech system including Databases, Servers and workstations. **(Control ref. 12.6)** Password protected screensavers are enabled on all workstations including desktops and laptops. Servers are also configured with Idle session timeout capability. **(Control ref. 12.7)**

- **IT Infrastructure**

KFintech has defined and documented the procedure related to Infrastructure change and configuration management process. **(Control ref. 8.1)**. KFintech LAN is segregated into different zones like Application, Database, DMZ, and Management under different subnets. Accesses to these zones are restricted and are allowed to authorize users only. The systems of KFintech are grouped in same LAN and are configured. These environments use static and dynamic protocol

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

configurations as required in the LAN. The client dependent networks are configured using DHCP. Data sharing is possible among the users belong to same unit or process or department with controlled access privileges. Unit or department or team specific folders are created on file server to store project specific work data, access to these folders are controlled based on requests received from respective managers. Where, access to these folders is provided to respective user or users belonging to same group and are restricted to other users. All the users of KFintech are allowed to store data only on their respective folders. Access to the respective team or department or unit folders are reviewed on quarterly bases. IT server or service desk team should be contacted in case of any problem in accessing these shared folders or for any IT related issues in the inter or intra network. All additional requirement of additional access privileges are fulfilled by IT team post receiving approval from respective reporting authority or Head IT and CISO. KFintech internal issues are raised through IT service desk ticketing system <https://servicedesk.KFintech.com:8090/> Application related issues are raised through ticketing tool <https://servicedesk.KFintech.com:8090/>. All the requests are raised internally, KFintech internal teams shall raise issues in the said tools on behalf of AMC's or clients in case there is a business requirement. IT team will address and resolve all the issues or requests raised in these ticketing systems.

- **Communication Equipment Operating Procedure**

Firewall: WAN port is connected to WAN router of service provider, respective ports are connected to Application, Database, DMZ, and Management zones under different subnets. Datacentre (DC) network is connected through the core switch port for internal LAN. All the links from the service providers are terminated on ISP provider equipment located in the ISP room of DC. Open and restricted internet traffic is routed through dedicated LAN ports on Firewall with configured policies. Firewall rules are reviewed at least once in six months, any changes to the setting to the configuration are followed through change process. All the network devices of KFintech are configured by IT Team, who are custodians of these assets.

Web content: At KFintech Internet usage is filtered based on the policies defined on CISCO umbrella for web filtering, by default a basic internet access is provided to all KFINTECH users and any additional access are provided based on the business requirement and on receiving approval from respective unit or department reporting authority or Head IT and CISO. A single policy database holds client, filter, policy, and general configuration information, whether there is a single policy server or multiple policy servers, web security is stored in the central database, policy information is automatically available to all policy servers associated with that Policy database. Any policy changes, updated to CISCO umbrella must be authorized by Head IT.

Users in the KFintech LAN are connected behind a Firewall. A secure LAN is established within KFintech which is used by the users to access services like http, email and configuration management system. Authorized users with admin privileges in IT team are allowed to access critical network resources like routers, firewalls, servers and other network devices, access to core router and firewall are limited and restricted. All the access privileges are reviewed and approved by Manager IT or Head IT. Default configuration and passwords are changed for the first login, when the device is connected for the first time to the KFintech network by the ITINFRA team.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Backup of existing configurations are taken by the IT team prior to making any changes to the configurations, all such changes are reviewed and approved by Head IT. All local administration account passwords are changed once in every 3 Years.

Switches: KFintech has both managed and unmanaged switches, desktops, servers, network devices like firewall and other network resources like printer are connected to through different ports of these switches. LAN segments are segregated, and access are controlled using these switches. Issues related to this communication equipment are escalated to IT team for further actions and resolutions. IT team maintains stock of equipment's, in case of failure of any switch, IT team replaces with one in the stock and updates the asset register accordingly or in case of non-availability they will initiate the procurement process.

Server and end-user computing operating procedure: KFintech use a Windows server as domain controller with failure servers at different locations along with servers with VMware, etc. for different applications and database servers like SQL. Static IP Configuration is done on Servers with different subnet mask, gateway. KFintech follows industry best practiced for hardening servers and network appliances. Passwords for all the servers are managed by KFintech ITINFRA team; Local admin ID is renamed, and guest accounts are disabled. Root password escrow is maintained under custody of IT team and root passwords of these servers are changed at least once in every 3 years. All such changes are tracked and updated by Head IT. Access to server configuration documents is provided to only authorize personals within IT team and CISO. These documents can be used as a reference for any new similar installations or at the time of disaster. Passwords of all critical servers are maintained in a sealed, waterproof envelop. This envelop is maintained under dual custody by IT INFRA and InfoSec of KFintech Based on requirement or at the time of disaster, ITINFRA Head and InfoSec Head are authorized to use or share these passwords to authorized personnel within the team members. Head IT ensured that an updated password file is maintained at any point of time. Antivirus is installed on all workstations and Servers along with Latest signatures are automatically downloaded and pushed from KFintech centralized antivirus Server. Scheduled updates are configured to push the patches to the workstations and Servers on a periodic basis. **(Control ref. 12.8)** All incoming and outgoing e-mails are scanned for virus and spam through the installed e-Mail scanner. **(Control ref. 12.9)**

In case of server failure another system in production environment can be configured using backups. These backup's is taken on daily bases by the IT team. As part of Business Continuity Plan (BCP) IT team takes full backups of all the critical servers **(Control ref. 12.6)**. All such backups are stored in a secured manner in tape / Disk media **(Control ref. 12.7)** under fireproof locker and are used at the time of disaster or for any requirements of backup restoration. Access to these tapes /Disk is provided to authorize persons of IT team with and to Head IT of KFintech.

KFintech has defined and documented the job schedule / batch process within their policies and procedure documents **(Control ref.10.1)**

Authorized personnel raises the batch job creation, modification and deletion request through e-mail to the DB team. Upon receiving the request, the jobs are scheduled by designated team. **(Control ref. 10.2)**

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

- **Data Transmission:**

Data in transit is through SSL/ TLS 1.2 and data at rest is encrypted using AES 256 encryption methods. Files are transferred through secured Sftp, emails are encrypted through the inbuilt features of 0365 and data at rest is encrypted using Microsoft TDE and using AES 256 encryption. KFinTech follow secured coding standards of OWASP.

- **Change Management:**

The change control process is formally defined and documented (**Control ref. 8.1**) at KFinTech to control changes to all critical assets, Changes can in both internal or request raised by AMC (**Control ref. 8.2**), client or by concerns authorized person from KFinTech on behalf of AMC or client, vendors and other resources placed or hosted in the Production environment (such as Infrastructure, hardware, software, application systems and operating procedures). (**Control ref. 8.4, 8.5**) On a periodic basis, designated team comprising of Senior Management and Development Team, performs analysis of the Changes for technical and operational feasibility, risk factors, compliance and security issues for potential impact. (**Control ref. 8.3**). Test and Production environments of in-house applications are segregated. (**Control ref. 8.6**)

- **Backup Procedure:**

Backup is critical part of KFINTECH and is scheduled for incremental back up on daily bases. All the backups are taken on the backup Tapes /Disks and are moved to the offsite (**Control ref. 12.7**) by an authorized person and placed in fireproof cabinet. Please refer KFINTECH backup policy for more information in backups. KFinTech has defined and documented the Environmental Safeguards and backup related policies and procedures. (**Control ref. 12.1**) Restoration testing is performed for backups of identified IT systems are performed as per the documented backup policy and schedule. (**Control ref. 12.8**)

- **Incident Management Procedure:**

KFinTech has a formal, focused, and coordinated approach to responding to incidents, which includes an incident response plan that provides the roadmap for implementing the incident response capability. KFinTech's Incident response plan shall meet its unique requirements, which relate to the organization's mission, size, structure, and functions. This incident Management process layout the necessary resources which include the leadership team and management support. All the impacted stakeholders are communicated from the initiation to the closure of the incident respective Head of the departments or Unit Head.

Based on the business impact the communication includes, communication to the applicable law firm(s), or other organization(s) that will determine the applicability of state or federal laws, organization(s) that will provide mailing or other notification services, organization(s) that will provide public relations services, organization(s) that will provide credit or other monitoring services, organization(s) that will provide forensic services, etc.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

- **SDLC**

All KFinTech software developers must address security threats. Computer users now require trustworthy and secure software, and developers who address security threats more effectively than others can gain a competitive advantage in the marketplace. Also, an increased sense of social responsibility now compels developers to create secure software that requires fewer patches and less security management. SDLC process is followed or invoked to address the new developments, meeting requirements of regulator or clients, enhancements and changes to the applications and digital platforms used to provide KFinTech services as a RTA.

KFinTech Secure software development has three elements—best practices, process improvements, and metrics.

KFinTech Secure software development is mandatory for software that is developed for the following uses:

- In a business environment
- To process personally identifiable information (PII) or other sensitive information
- To communicate regularly over the Internet or other networks.

The KFinTech Security Development Lifecycle consists of the proven best practices and tools that were successfully used to develop recent products. However, the area of security and privacy changes frequently, and the Security Development Lifecycle must continue to evolve and to use new knowledge and tools to help build even more trusted products. But because product development teams must also have some visibility and predictability of security requirements in order to plan schedules, it is necessary to define how new recommendations and requirements are introduced, as well as when new requirements are added to the SDL.

All KFinTech members of software development teams shall receive appropriate training to stay informed about security basics and recent trends in security and privacy. Individuals who develop software programs should attend at least one security training class each year or go through the knowledgebase. Security training can help ensure the software is created with security and privacy in mind and can also help development teams stay current on security issues. Project team members are strongly encouraged to seek additional security and privacy education that is appropriate to their needs or products.

- **Third Party Management**

Company enters a contract with Vendor / Business partners which includes scope of services or product specifications, roles and responsibilities, compliance requirements, service levels, communication Protocols and termination clause permitting the company to terminate any services from Vendor/ Business Partners Contracts are reviewed by Business and Legal team before sign-off. **(Control ref. 13.1)**

Vendor / Business Partner assessment is performed during vendor on boarding and company annually assesses the performance of critical vendors and business partners. **(Control ref. 13.2)**

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Service Level Agreements (SLAs) are defined for vendors and any deviations from SLAs are reviewed and approved by the Authorized Personnel. **(Control ref. 13.3)**

The performance of critical vendors and business partners is assessed at least on annual basis. **(Control ref. 13.4)** Company enters a contract with Information Security Vendor / Business partners which includes scope of services or product specifications, roles and responsibilities, compliance requirements, service levels, communication Protocols, termination clause permitting the company to terminate any services from Vendor/ Business Partners and confidentiality clause. Company obtains an NDA from the vendors before on boarding. **(Control ref. 13.5)**

3.9. Complementary Subservice Organization Controls

Certain controls that should be designed and implemented by subservice organization (which are carved out in this report) in operation at User Entities to complement the controls at KFinTech, have been listed in this section. These user control considerations should not be regarded as a comprehensive list of all controls, which should be employed by User Entities. There may be additional controls that would be appropriate for the User Entities, which are not identified in this report.

KFinTech uses CtrlS and Sify as Datacenters hosting service for its in-scope IT Infrastructure.

Subservice Organization	Services Provided / Complementary Controls / Monitoring Controls	Associated Control Objective
CtrlS Datacenters Ltd. Sify Technologies Limited	Subservice organization - 'CtrlS Datacenter Ltd.' and 'Sify Technologies Ltd.' is responsible to provide SOC reports for the services rendered to Service Organization.	Control Objective 1*

3.10. Complementary User Entity Controls

The controls at KFinTech that are applicable to the processes as detailed in the scope, were designed with the assumption that certain controls would be designed and placed in operation at User Entities. In certain situations, the application of specified internal controls at User Entities is necessary to achieve certain control objectives included in this report.

Certain controls that should be designed and placed in operation at User Entities to complement the controls at KFINTECH, have been listed in this section. User Entities auditors are expected to consider whether all these controls have been designed and placed in operation at User Entities. These user control considerations should not be regarded as a comprehensive list of all controls, which should be employed by User Entities. There may be additional controls that would be appropriate for the user entities, which are not identified in this report.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

KFIN TECHNOLOGIES LIMITED

SOC 1 Type 2 Report – Business Process and general IT controls related to inscope infrastructure

Complementary User Entity Controls	Associated Control Objective(s)
<ul style="list-style-type: none">User Entity is responsible to intimate KFinTech for any access provisioning and de-provisioning request.	Control Objective – 12.1, 12.2, 12.4, 12.10 and 12.11

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

4. Description of KFinTech's Control Objectives and Related Controls

A. Types and Description of Tests of Operating Effectiveness

This report, when combined with an understanding of the controls at User Entity and subService Organizations, is intended to assist auditors in planning the audit of User Entity's financial statements or User Entity's internal control over financial reporting and in assessing control risk for assertions in User Entity's financial statements that may be affected by controls at the Company.

Our examination was limited to the control objectives and related controls specified by the KFinTech in Sections III and IV of the report and did not extend to the controls in effect at User Entity and subService Organizations.

It is the responsibility of User Entity and its independent auditor to evaluate this information in conjunction with the evaluation of internal control over financial reporting at the User Entity in order to assess the internal control environment. If the internal controls are not effective at a User Entity, the Company's controls may not compensate for such weaknesses.

KFinTech's system of internal control represents the collective effect of different factors on establishing or enhancing the effectiveness of the controls specified by the Company. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by the Company, we considered aspects of the Company's control environment, risk assessment process, monitoring activities, and information and communications.

Procedures for Assessing Completeness and Accuracy of Information Produced by The Entity (IPE)

For tests of controls requiring the use of Information Produced by the Entity (IPE), procedures were performed to assess the reliability of the information, including completeness and accuracy of the data or reports, to determine whether the information can be relied upon in the examination procedures. This includes IPE produced by KFinTech and provided to User Entity (if relevant and defined as part of the output control objectives), IPE used by KFinTech management in performance of controls (i.e., periodic review of user listings), and IPE used in the performance of our examination procedures.

Based on the nature of the IPE, a combination of the following procedures were performed to address the completeness and accuracy of the data or reports used:

- (1) inspect source documentation relating to the IPE,
- (2) inspect the query, script, or parameters used to generate the IPE,
- (3) agree data between the IPE and the source, and/or

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

(4) inspect the IPE for anomalous gaps in sequence or timing.

The following table clarifies certain terms used within this section to describe the nature of the tests performed:

Type	Description
Inquiry	Inquired of appropriate personnel and corroborated with management
Observation	Observed the application, performance, or existence of the control as represented in remote/ virtual walkthroughs leveraging the technologies like camera, Microsoft teams.
Inspection	Inspected documents, records, or other evidence indicating performance of the control
Reperformance	Reperformed the control, or processing of the application control, for accuracy of its operation

This space has been intentionally left blank

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

B. Control Objectives, Control Activities, and Tests Performed

4.1. Unit Corpus Reconciliation

Control Objective 1			
Controls provide reasonable assurance that Unit Corpus Reconciliation is performed on a daily basis and batches are closed accurately.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
1.1	On a daily basis, the list of transactions reported the previous date are sent by the banking team to the UCR team.	Inspection For selected samples of dates, inspected the transaction reports of the previous days to verify that opening units were matching with previous day's closing units.	No exception noted.
1.2	UCR team uploads the Approved Transaction list received from the banking team to the UCR module	Inspection For the selected samples dates within the audit period inspected the UCR modules and verified that approved transaction list was uploaded by UCR team.	No exception noted.
1.3	UCR Team closes the batch for both liquid and non liquid transaction types using the UCR Module before 6:30 PM for liquid and non-liquid 5:30 PM	Inspection For selected sample of dates inspected the UCR module and verified that UCR team closed the batch for liquid 6:30 PM and for non liquid at 5:30 PM.	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 1			
Controls provide reasonable assurance that Unit Corpus Reconciliation is performed on a daily basis and batches are closed accurately.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
1.4	Once the batches have been closed the UCR team verifies the closing balance of the previous date and the opening balance of the batch	Inspection For selected sample of dates inspected the batch validation records by UCR team and verified that UCR team reconciled previous date closing date with opening balance for batch on the current date.	No exception noted.
1.5	If there is a mismatch in the balances the UCR team verifies the transaction logs to identify and remediate the deviation.	Inquiry Inquired with the KFin tech team were there any mismatch encountered in the transactions logs during the specified audit period. Further, if there were any mistakes or changes required in the transaction or balances were noted to initiate the rectification process.	No occurrence during the specified period.
1.6	The report of the verified batches is sent by the UCR team to fund accounting or AMC	Inspection For selected samples of dates, within the specified period, inspected that the batch report generated by UCR team and verified if report were sent to fund accounting in a given format by the fund accounting team.	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 1			
Controls provide reasonable assurance that Unit Corpus Reconciliation is performed on a daily basis and batches are closed accurately.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
1.7	if any changes are required for the closed batches the UCR team follows the rectification process within T+1 days	Inquiry Inquired with the UCR team, were there any deviant transaction identified in the transactions logs during the specified audit period. Further, the team has initiated the rectification process within T+1 day to close the batches.	No occurrence during the specified period.

This space has been intentionally left blank

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

4.2. Net Asset Value

Control Objective 2			
Controls provide reasonable assurance that the daily Net Asset Value transactions are processed accurately.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
2.1	Emails are received from Fund accounting team to KFintech team personnel on a daily basis.	Inspection For the selected samples of dates within the specified period, we inspected and verified that KFintech team personnel receives emails from the fund accounting team on a daily basis.	No exception noted.
2.2	Files contained in the automated emails are saved on the desktop by the maker (KFintech team).	Inspection For the selected samples of dates within the specified period, we inspected and verified that maker (KFintech team personnel) saves the attachments contained in the emails on the desktop for further processing in TaskMF application.	No exception noted.
2.3	On a daily basis, emails are imported by the Maker into TaskMF, and NAV transactions are confirmed for the same date.	Inspection For the selected samples of dates within the specified period, we inspected and verified that maker (KFintech team personnel) imports the emails attachments into the TaskMF application on a daily basis and NAV transactions are checked and confirmed for the same date.	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 2 <i>Controls provide reasonable assurance that the daily Net Asset Value transactions are processed accurately.</i>			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
2.4	The checker verifies if the NAV transactions are of the same date, and confirms transactions in an hour using the TASKMF portal/system/application.	Inspection For the selected samples of dates within the specified period, we inspected and verified that the checker verifies the NAV transactions uploaded by the maker on the same day itself. Then the transactions are confirmed in an hours' time using the TASKMF portal/system/application.	No exception noted.
2.5	Automated emails are generated by TaskMF to the internal audit team to verify the NAV transactions.	Inspection For the selected samples of dates within the specified period, we inspected and verified that the TaskMF application generates NAV audit report. Confirmation emails with the required details and are sent to the internal audit team where all the NAV transactions are verified.	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 2			
Controls provide reasonable assurance that the daily Net Asset Value transactions are processed accurately.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
2.6	Internal Audit team downloads the NAV data from TaskMF and compares it to the NAV data received from the fund accountant/AMC. The NAV value is verified for each combination of the scheme code and plan code. If no deviations are identified the NAV is saved in TaskMF.	<p>Inspection</p> <p>For the selected samples of dates within the specified period, we inspected that the Internal Audit team downloads the NAV data from TaskMF application into their respective folders and compares the same data with the NAV data received from the fund accountant/AMC through emails. Further, it was verified that the confirmation email was sent by the audit team post verification of the scheme code and plan code were matching with the NAV value for the selected sample dates.</p>	No exception noted.
2.7	If there is deviation, then Fund accountant team raises incident with KFin tech team.	<p>Inquiry</p> <p>Inquired with KFin tech team that if any deviations were identified during the specified period then it is moved to the objection queue and incident are raised with to resolve the issue.</p>	No occurrence during the audit period.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 2 <i>Controls provide reasonable assurance that the daily Net Asset Value transactions are processed accurately.</i>			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
2.8	Unit team performs the final endorsement by saving the NAV file in TaskMF. An automated email is generated confirming the endorsement	Inspection For the selected samples of dates within the specified period, we inspected and verified that the unit team performs the final endorsement. If no deviations are detected after the QC check has passed then the transactions are endorsed, units are allocated based on NAV, SoA is generated and saved in TaskMF.	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

4.3. Branch CPZ

Control Objective 3 <i>Controls provide reasonable assurance that the details filled by the investor in investor forms are accurately captured in the organization's IT systems, the transactions are endorsed, and units are allocated based on NAV.</i>			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
3.1	Physical forms filled by Investors are assigned timestamp and barcode at the branch level	Inspection For the selected samples of dates within the specified period, inspected the physical forms were filled by the investor and were assigned timestamp & barcode at the branch level.	No exception noted.
3.2	Physical forms are scanned at the branch level and uploaded to KBOLT Plus application within Same day	Inspection For the selected samples of dates within the specified period, inspected the KBOLT consolidation report and verified that the form were scanned at the branch level and uploaded to KBOLT Plus application on the same day by the branch team.	No exception noted.
3.3	CPZ Team member performs the checker and objection level not the maker level activity by populating the form details such as transaction type, purchase type, amount, barcode number, cheque number as applicable.	Observation During the walkthrough of KBOLT application with CPZ team, it was observed that the objection level activities were available to checkers for populating the form details such as transactions type, purchase type, amount, barcode number, cheque number.	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 3 <i>Controls provide reasonable assurance that the details filled by the investor in investor forms are accurately captured in the organization's IT systems, the transactions are endorsed, and units are allocated based on NAV.</i>			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
3.4	A unique identifier (In House Number - IHNo) is generated by the application once the necessary details are entered by the maker in the application.	Observation Observed during process walkthrough that a unique identifier were generated by the application once the necessary details were entered by the maker in the application	No exception noted.
3.5	CPZ Team member performs the checker activity by confirming the details from the physical form	Inspection For the selected samples of dates within the specified period, inspected the physical forms and verified that the checker had entered correct information.	No exception noted.
3.6	Any deviations between the maker and checker entries are flagged by the system as objections which are further moved to an objection queue assigned to the Objection team for closure within same day	Inquiry Inquired with the objection team whether any deviation was identified between the checker and maker entries within the specified period. Further, any objections were noted by the team in objection queue during specified period.	No occurrence during the specified period.
3.7	The transactions are endorsed and units allocated based on NAV if there are no deviations identified.	Inspection For the selected samples of dates within the specified period, inspected transaction records and verified units were allocated based on NAV, if no deviations were identified.	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

4.4. Non Commercial Transactions

Control Objective 4 Controls provide reasonable assurance that Non Commercial Transactions including change requests submitted by the investors are processed in an accurate and timely manner.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
4.1	NCT Physical forms for any changes to the Investor profile details are filled by Investors and assigned timestamp and barcode by the branch team within T+1 days.	Inspection For the selected samples of dates within the specified period, inspected the NCT physical forms received from the investor by the branch team. Further the verification were performed for the timestamp and barcode by branch team within T+1 days.	No exception noted.
4.2	The Branch team verifies the completeness of the forms against the verification checklist, and the information is entered into the KBOLT - NCT portal.	Observation Observed during process walkthrough that the branch team verifies completeness of the form as per the defined checklist. Also, observed during the KBOLT NCT portal that data validators were defined as per the checklist maintained by the branch team.	No exception noted.
4.3	The IH No is generated by KBOLT once the details are entered into KBOLT by the Branch team, and the forms move automatically to the KNUM application.	Observation During the walkthrough of KBOLT application with the branch team observed that insersation of complete details leads to IH No. generation. Subsequent to IH No. generation the forms are automatically moved to KNUM application.	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 4 Controls provide reasonable assurance that Non Commercial Transactions including change requests submitted by the investors are processed in an accurate and timely manner.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
4.4	Physical forms are scanned at the branch level and uploaded to KBOLT application by Branch team which flows to KNUM.	Inspection For the selected samples of dates within the specified period, inspected and verified that the KBOLT consolidation report for a specified period where the form were scanned at the branch level and uploaded to KBOLT application. Observation Observed during the walkthrough and verifies, that the forms were automatically moved to KNUM application.	No exception noted.
4.5	Unit team downloads the previous day change report from KNUM by 10 AM of current day.	Observation Observed during the walkthrough of KNUM application with NCT that previous day change report were downloaded in the respective folders by 10 AM of the current day.	No exception noted.
4.6	Process Unit team verifies the signature in the scanned physical form in KNUM with the signature in the initial investment form. Post signature verification if the request is found In Good Order (IGO), it is sent for further processing.	Observation Observed during the process walkthrough that products unit team retrieves the scanned physical forms from TaskMF and validated investor signature, transaction date and In House Number.	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 4 Controls provide reasonable assurance that Non Commercial Transactions including change requests submitted by the investors are processed in an accurate and timely manner.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
4.7	Verification of the supporting documents submitted by the investor with the request form is performed by the maker team. The document verification is performed as per the "Application Completeness and Verification Checklist". Post verification if the request is found In Good Order (IGO), it is sent for further processing.	Inquiry Inquired operation team to determine supporting documents submitted with the request form are verified by the team as per the "Application Completeness and Verification Checklist". Also, checked whether it is sent for further processing, if found In Good Order(IGO) post verification. Inspection Inspected selected samples dates of request forms, within the specified period that the maker team verifies the supporting documents submitted by the investor.	No exception noted.
4.8	Maker team verifies the folio number in the scanned physical form in KNUM with the folio number entered by the branch	Inspection For selected samples dates within the specified period, inspected the scanned physical form and verified that the folio number in the scanned physical form and in KNUM application were same.	No exception noted.
4.9	Based on the change request form the maker team enters the updated details in the KNUM system	Observation Inquired during the process walkthrough that whether the change request form in the KNUM application were updated by the maker team.	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 4			
Controls provide reasonable assurance that Non Commercial Transactions including change requests submitted by the investors are processed in an accurate and timely manner.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
4.10	The Checker team confirms the updated details in the KNUM System within applicable TAT	<p>Inquiry</p> <p>Inquired the operation team to determine whether the Checker team confirms the updated details in the KNUM System within applicable TAT.</p> <p>Inspection</p> <p>For selected sample, within the specified period, inspected the KNUM application for the updated request received by the checker team and verified the updated details were confirmed in the KNUM application within the applicable TAT.</p>	No exception noted.
4.11	The KNUM system compares the entries made by the maker and the checker to verify if they match. If a mismatch is identified, the checker is informed and required to re verify and enter the correct information.	<p>Observation</p> <p>During the walkthrough of KNUM application we noted maker-checker entries are compared by the system. Further observed that, in case of mismatch were identified, the checker were informed to reverify and enter the correct information.</p>	No exception noted.
4.12	Post checker stage, the change request is sent to the QC team who verify the final correctness of the details captured in the system comparing with the scans of the physical form.	<p>Inquiry</p> <p>Inquired during the walkthrough of operation team to whether the change request is sent to the QC team for verification of final correctness of the details captured in the system.</p>	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 4			
Controls provide reasonable assurance that Non Commercial Transactions including change requests submitted by the investors are processed in an accurate and timely manner.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
4.13	<p>QC clearance is performed on the same day.</p> <p>After QC clearance, the change request is closed and can be verified through KBOLT</p>	<p>Inquiry</p> <p>Inquired the operation team to determine whether, QC clearance is performed on same day. Once QC is cleared, CR is closed and can be verified through KBOLT.</p>	No exception noted.
4.14	<p>In case QC clearance is not obtained, the change request is moved back to the Checker stage.</p>	<p>Inquiry</p> <p>Inquired with the operation team to determine if QC clearance is obtained or not, the change request is moved back to the Checker stage.</p> <p>Observation</p> <p>Observed the KBOLT application to determine in case the QC is not cleared, the change request is moved back to the Checker stage.</p>	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

4.5. SIP

Control Objective 5			
Controls provide reasonable assurance that the requests obtained from investors regarding special products including SIP are processed in an accurate and timely manner.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
5.1	Physical forms are filled by Investors at the branch and are assigned timestamp and barcode by the KFinTech branch team within same business days of receipt of the forms.	Inspection For the selected samples of dates within the specified period, inspected the physical forms received from the investor by the branch team. Further the verification were performed for the timestamp and barcode by branch team on the same business day.	No exception noted.
5.2	Physical forms are scanned by KFinTech branch team. The scans are uploaded to KBOLT application and details are entered into KBOLT within Same days by the branch team.	Inspection For the selected samples of dates within the specified period, inspected the KBOLT consolidation report and verified that the form were scanned at the branch level and uploaded to KBOLT Plus application on the same day by the branch team.	No exception noted.
5.3	The Special products team retrieves the scanned physical forms from TaskMF signed by the investors and performs checker activity including confirmation of signature, transaction date and In House Number within T+1 days of upload.	Observation Observed during the process walkthrough that Special products team retrieves the scanned physical forms from TaskMF and validated investor signature, transaction date and In House Number.	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 5			
Controls provide reasonable assurance that the requests obtained from investors regarding special products including SIP are processed in an accurate and timely manner.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
5.4	Unit team performs a review of data verified and confirmed by the checker by comparing it with the scanned physical form.	<p>Inspection</p> <p>For a sample of days, for a sample of systematic requests, inspected the physical forms and the information updated within TaskMF to confirm that physical forms within TaskMF were validated for completeness and accuracy.</p>	No exception noted.
5.5	QC team verifies folio number, scheme code, plan code and other SIP details and confirms the transaction details on TASKMF portal within T+3 days.	<p>Inquiry</p> <p>Inquired the operation team to determine whether, QC team verifies folio number, scheme code, plan code and other SIP details.</p> <p>Inspection</p> <p>Inspected selected samples of dates, within the specified period that transaction details on TaskMF portal were confirmed within T+3 days.</p>	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 5			
Controls provide reasonable assurance that the requests obtained from investors regarding special products including SIP are processed in an accurate and timely manner.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
5.6	LOT is generated by the SIP team and stored with the respective images in the SFTP path every day or within T+5 days. Email confirmation of lot generation and SFTP upload is sent to billdesk or other aggregators.	<p>Observation</p> <p>Observed during process walkthrough that SIP team were generated the LOT and stored the images in the respective folders within T+5 days.</p> <p>Inspection</p> <p>For selected sample of dates, within specified period, inspected the email confirmation of LOT generation and SFTP upload were sent to billdesk or other aggregators within T+5 days.</p>	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

4.6. STP

Control Objective 6			
Controls provide reasonable assurance that the requests obtained from investors regarding special products including STP are processed in an accurate and timely manner.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
6.1	Physical forms filled by Investors at the branch and are assigned the timestamp and barcode by the KFinTech branch team within same business days of receipt of the forms.	<p>Inspection</p> <p>For the selected samples of dates within the specified period, inspected the physical forms received from the investor by the branch team. Further the verification were performed for the timestamp and barcode by branch team on the same business day.</p>	No exception noted.
6.2	Physical forms are scanned by the KFinTech branch team. The scans are uploaded to the KBOLT application and details are entered into the system within same days by the branch team.	<p>Inspection</p> <p>For the selected samples of dates within the specified period, inspected the KBOLT consolidation report and verified that the form were scanned at the branch level and uploaded to KBOLT Plus application on the same day by the branch team</p>	No exception noted.
6.3	The Special products team retrieves the scanned physical forms from TaskMF signed by the investors and performs checker activity including confirmation of signature, transaction date and In House Number within T+2 days of upload.	<p>Observation</p> <p>Observed during the process walkthrough that Special products team retrieves the scanned physical forms from TaskMF and validated investor signature, transaction date and In House Number.</p>	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 6			
<i>Controls provide reasonable assurance that the requests obtained from investors regarding special products including STP are processed in an accurate and timely manner.</i>			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
6.4	If there are deviations identified by the Special Products team the STP is registered and entries are performed for the STP by selecting source and destination scheme.	Inquiry Inquired with the special product team for the registered STP whether any deviation was identified for the entries performed after selecting source and destination scheme.	No occurrence during the specified period.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

4.7. SWP

Control Objective 7 <i>Controls provide reasonable assurance that the requests obtained from investors regarding special products including SWP are processed in an accurate and timely manner.</i>			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
7.1	Physical forms filled by Investors at the branch and are assigned the timestamp and barcode by the KFinTech branch team within Same business days of receipt of the forms.	Inspection For the selected samples of dates within the specified period, inspected the physical forms received from the investor by the branch team. Further the verification were performed for the timestamp and barcode by branch team on the same business day.	No exception noted.
7.2	Physical forms are scanned by the KFinTech branch team. The scans are uploaded to the KBOLT application and details are entered into the system within Same days by the branch team.	Inspection For the selected samples of dates within the specified period, inspected the KBOLT consolidation report and verified that the form were scanned at the branch level and uploaded to KBOLT Plus application on the same day by the branch team.	No exception noted.
7.3	The Special products team retrieves the scanned physical forms from TaskMF signed by the investors and performs checker activity including confirmation of signature, transaction date and In House Number within T+2 days of upload.	Observation Observed during the process walkthrough that Special products team retrieves the scanned physical forms from TaskMF and validated investor signature, transaction date and In House Number.	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 7			
Controls provide reasonable assurance that the requests obtained from investors regarding special products including SWP are processed in an accurate and timely manner.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
7.4	Checker enters the In House Number in TaskMF application and validates the withdrawal form with the initial purchase form.	<p>Observation</p> <p>observed during the process walkthrough that checker enters validated the withdrawal form with the initial purchase form by entering the In House Number in TaskMF application.</p>	No exception noted.
7.5	Based on the withdrawal cycle date, withdrawal is performed and payment is released to the investor's payout bank.	<p>Observation</p> <p>During the walkthrough we observed the withdrawal cycle for one sample date wherein the withdrawal request was received and processed which was completed once the payment were released to the payout bank.</p> <p>Inspection</p> <p>For sample withdrawl cycle, the payout report was referred and verified that</p> <p>the withdrawl against the payment release of the specific Mutual fund.</p>	No exception noted.

This space has been intentionally left blank

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

4.8. Application Development and Change Management

Control Objective 8			
Controls provide reasonable assurance that application changes to KFin business applications are recorded, analyzed, tested, approved and implemented.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
8.1	KFintech has defined and documented policy and procedure related to application change management and Infrastructure change & configuration management process within the Quality Procedure Manual.	<p>Inspection</p> <p>Inspected Quality Procedure Manual document and verified that the procedures to be followed for Application Development Changes and Infrastructure change & configuration management process were established and documented.</p> <p>Additionally, inspected that the policies and procedures were available to KFintech intranet portal.</p>	No exception noted.
8.2	New development requirements / enhancements / changes to existing applications are identified by the user group. Based on the discussion, the change management team prepares 'Requirements document' and uploads within the Enhancement Tracker.	<p>Inspection</p> <p>For selected sample of application changes, inspected the Change request (CR) tickets and verified that development / enhancements requirements were documented and uploaded within the Enhancement Tracker by KFintech change management team.</p>	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 8			
Controls provide reasonable assurance that application changes to KFin business applications are recorded, analyzed, tested, approved and implemented.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
8.3	On a periodic basis, designated team comprising of Senior Management and Development Team, performs analysis of the Changes for technical and operational feasibility, risk factors, compliance and security issues for potential impact.	<p>Inspection</p> <p>For selected sample of weeks, inspected the minutes of meeting from the e-mail communications and verifies that Master Craftsman Guild (MCG) comprising Unit Managers, General Manager and Development Team discussed and analyzed the change requests.</p> <p>Additionally, for selected sample of application change requests within Enhancement tracker, inspected the ticket and verified that the change request were approved by the MCG.</p>	No exception noted.
8.4	Upon completion of development, UAT is performed by the change requestor or a unit team member and sign-off is provided within the UAT Track. After obtaining sign-off, the Change management team updates the status of the ticket in the Tracker as "Signed-off".	<p>Inspection</p> <p>For selected sample of application change requests within the specified period in Enhancement tracker, inspected the corresponding ticket within UAT tracker and verified that UAT were performed and the bugs identified during UAT were closed and "Signed-off".</p>	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 8			
Controls provide reasonable assurance that application changes to KFin business applications are recorded, analyzed, tested, approved and implemented.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
8.5	Upon UAT sign-off, the developed code is uploaded within the dev/prod site to the IT Team for deployment. The IT team deploys the change in to the production and changes the status of the ticket as complete.	<p>Inspection</p> <p>For selected sample of application change request within the specified period in Enhancement tracker, inspected the ticket and verified that IT team deployed the code within production upon UAT sign-off and released the change request within the Enhancement Tracker.</p>	No exception noted.
8.6	Test and Production environments of in-house applications are segregated	<p>Observation</p> <p>Observed during the application walkthrough it was noted that in-house applications were segregated (Test and Production environments).</p> <p>.</p>	No exception noted.

This space has been intentionally left blank

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

4.9. Operations Management

<p>Control Objective 10</p> <p><i>Controls provide reasonable assurance that batch jobs are appropriately scheduled, monitored, and batch job failures are identified and resolved in a timely manner.</i></p> <p><i>Controls provide reasonable assurance that access to create, modify and delete batch jobs is restricted to authorized individuals.</i></p>			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
9.1	KFintech has defined and documented the job schedule / batch process within their policies and procedure documents	<p>Inspection</p> <p>Inspected database administration and services document and verified that the procedures to be followed for job schedule/ batch process were established and documented.</p>	No exception noted.
9.2	Authorized personnel raises the batch job creation, modification and deletion request through e-mail to the DB team. Upon receiving the request, the jobs are scheduled by designated team.	<p>Inquiry</p> <p>Confirmed via corroborative inquiry with Database Administrator Manager that authorized Unit Managers raises the batch job creation, modification and deletion request through e-mail to the DB team. Upon receiving the request, the jobs were scheduled by the DBAs. However, the service auditor noted that this control did not operate during the specified period, as there were no occurrences of batch jobs created during the specified period. Therefore, this control activity could not be tested for operating effectiveness.</p>	No occurrence during the specified period.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 10
Controls provide reasonable assurance that batch jobs are appropriately scheduled, monitored, and batch job failures are identified and resolved in a timely manner.
Controls provide reasonable assurance that access to create, modify and delete batch jobs is restricted to authorized individuals.

Control Activity		Tests Performed by the Service Auditor	Results of Testing
9.3	Access to create, modify, delete, and configure Scheduler jobs is restricted to authorized personnel within DB team.	Inspection Inspected Scheduler job tool and verified that the access to create, modify, delete and configure scheduler job were restricted to authorized personal.	No Exception noted.

This space has been intentionally left blank

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

4.10. Physical Security

Control Objective 11			
Controls provide reasonable assurance that KFinTech's facilities are physically secured and monitored.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
10.1	KFinTech has defined and documented the Physical security policy and procedures. The policy and procedure documents are made available to the employees.	Inspection Inspected the physical security policy & procedures and verified that the procedures for monitoring, authorizing, and approving physical access to the KFinTech's facilities were defined and documented. Further, inspected that the policies and procedures were available to KFinTech intranet portal.	No exception noted.
10.2	Security guards are deployed at entry and exits of all KFinTech facilities on a 24*7 basis.	Inspection For selected sample dates, inspected the security guards' attendance register and verified that the guards were deployed on a 24*7shift basis.	No exception noted.
10.3	Proximity card / biometric equipment installed at the entry and exit of information processing across KFinTech.	Observation Observed during the facility walkthrough that proximity card/ biometric equipment were installed at the entry and exit points in accordance to the floor plan.	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 11			
Controls provide reasonable assurance that KFinTech's facilities are physically secured and monitored.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
10.4	KFinTech facilities are monitored through Closed Circuit Television (CCTV) cameras. CCTV recordings are retained for a period of one month.	<p>Observation</p> <p>Observed during the facility walkthrough that Closed Circuit Television (CCTV) were placed.</p> <p>Inspection</p> <p>Inspected selected sample dates of CCTV footage within the specified period when facilities were operational and verified that logs were retained for a minimum period of one month.</p>	No exception noted.
10.5	KFinTech employees are provided with photo based Identity cards. Personnel are instructed to display their identification cards prominently while inside the facility.	<p>Observation</p> <p>Observed during the facility walkthrough and verified that the employees were instructed by security guards to display their identification cards.</p>	No exception noted.
10.6	Visitors / vendors visiting KFinTech facilities are issued visitor /vendor ID cards by security guards at the security point. Visitor obtains sign off from the respective user department on the visitor pass issued to him / her.	<p>Inspection</p> <p>Inspected selected sample of dates in visitor register and verified that visitors / vendors visiting KFinTech facilities were issued visitor / vendor ID cards by security guards at the security point</p> <p>Additionally, inspected visitor authentication slip and verified that visitor obtained sign off from the respective user department on the visitor pass issued to him / her.</p>	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 11 Controls provide reasonable assurance that KFinTech's facilities are physically secured and monitored.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
10.7	An employee enters in the exit tracker during his/her resignation and submits their ID and access cards to respective team. HR revokes the proximity/biometric access for the respective employee.	Inspection For selected sample of separation of on roll employees, inspected the access control system and verified that physical access to the facility were revoked. Additionally, inspected the logs from the access control system and the date of separation of the employee to verify that the employee had accessed the facility after the date of separation.	No exception noted.
10.8	In case of any loss of access card, employee informs the same to physical security/admin team and access card is deactivated within one business day of intimation, temporary identity/ access card having access to common area would be provided.	Inquiry Inquired with the KFinTech team to determine whether in case of any loss of access card, employee informed the same to physical security/admin team and access card were deactivated within one business day of intimation.	No exception noted.

This space has been intentionally left blank

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

4.11. Environmental Safeguards and Backup

Control Objective 12			
Controls provide reasonable assurance that data and applications are protected against environmental threats.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
11.1	KFintech has defined and documented the Environmental Safeguards and backup related policies and procedures.	Inspection Inspected the physical security policy & procedures and verified that aspect related to environmental safeguard and backup were defined.	No exception noted.
11.2	On a periodic basis, maintenance activities for fire extinguishers are performed as agreed with the vendor.	Inspection For selected sample of quarter, within the specified period, inspected the fire extinguisher maintenance reports and verified that preventive maintenance activity were performed.	No exception noted.
11.3	On a periodic basis, authorized personnels perform the Fire drill activity and the results are documented.	Inspection Inspected the fire drill report and verified that fire drills were conducted on a periodic basis.	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 12			
Controls provide reasonable assurance that data and applications are protected against environmental threats.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
11.4	Uninterruptible Power Supply (UPS) and backup generators are installed at KFinTech facilities. UPS and generators are covered under annual maintenance contracts and are serviced as per the service maintenance schedule agreed with the vendor.	<p>Observation</p> <p>Observed during the physical walkthrough to determine whether Uninterruptible Power Supply and backup generators were installed at the facility.</p> <p>Inspection</p> <p>Further, inspected the Annual maintenance contract to verify UPS and backup generators are included.</p> <p>Additionally, inspected the PM report and verified that preventive maintenance were performed quarterly.</p>	No exception noted.
11.5	Fire and emergency instructions are displayed at prominent locations.	<p>Inspection</p> <p>Observed KFinTech facilities to determine whether the Fire and emergency instructions were displayed in prominent locations such as entry-exit point, server room and office space</p>	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 12			
Controls provide reasonable assurance that data and applications are protected against environmental threats.			
Control Activity	Tests Performed by the Service Auditor	Results of Testing	
11.6	<p>System state backup and data backup from servers (operating system) and network devices are taken at predetermined time intervals (daily incremental/differential backup, weekly full backup and monthly full backup) as per the documented backup policy and recorded on backup plan.</p>	<p>Inspection</p> <p>Inspected the backup plan and verified that predefined time intervals and schedules were defined as per policy.</p> <p>Additionally, inspected the the backup tools and verified that the backup type and schedule were as per the backup plan..</p>	No Exception noted.
11.7	<p>Backups of identified IT systems are performed as per the documented backup policy and schedule. Backup data is stored at offsite location on periodic basis for restoration whenever required</p>	<p>Inspection</p> <p>Inspected the configuration for the scheduled job and verified that backup process runs every 5 mins daily between 00:00:00 to 23:59:59. Further, verified that restoration testing were performed for backups of identified IT systems as per the documented backup policy and schedule.</p> <p>Additionally, Inspected the database(DB) replication settings and verified that DBs were configured for synchronous replication at Disaster recovery(DR) site.</p>	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 12			
Controls provide reasonable assurance that data and applications are protected against environmental threats.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
11.8	Restoration testing is performed for backups of identified IT systems are performed as per the documented backup policy and schedule.	Inspection For selected sample of restoration testing performed, during the specified period ,inspected the restoration records and verified that backup data were tested by KFintech if it can be restored as per the original state.	No Exception noted.

This space has been intentionally left blank

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

4.12. Logical Security

Control Objective 13			
Controls provide reasonable assurance that logical access to programs, data, workstations, network, and network infrastructure is restricted to authorized and appropriate users.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
12.1	KFINTECH has defined and documented the policy and procedures related to logical security.	<p>Inspection</p> <p>Inspected the Information Security Management System Manual document and verified that the logical security related policies and procedures were defined by the ISMS team.</p>	No exception noted.
12.2	For newly joined employees, (On-Roll/Off-Roll) HR team raises request for domain and e-mail ID creation and concerned team creates domain and e-mail ID.	<p>Inspection</p> <p>For selected sample of Domain and e-mail ID creation requests during the specified period, inspected the tickets raised in user track and verified that concerned team created the domain and e-mail ID.</p>	No exception noted.
12.3	When an employee separates from KFin, a ticket is raised by the concerned team for approval from authorized personnel basis which concerned Team revokes the employee's access to system and e-mail.	<p>Inspection</p> <p>For selected sample of separated employees, inspected the corresponding User Track ticket raised for requesting domain and e-mail ID access revocation and verified that the access revocation was raised in a timely manner.</p> <p>Additionally, inspected the domain user listing and verified that the access of sample separated employees were revoked.</p>	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin's Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 13			
Controls provide reasonable assurance that logical access to programs, data, workstations, network, and network infrastructure is restricted to authorized and appropriate users.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
12.4	On a periodic basis, HR Team generates a list of absconding employees those who are continuously absent for more than 2 weeks and uploads the same in HR System and relevant team disables the system, email, door access.	<p>Inspection</p> <p>Inspected the list of separated employees, during the specified period and verified that there were no cases of employees absconding.</p>	No occurrence during the specified period
12.5	The list of active system access IDs are reviewed by concerned team at least on quarterly basis and accesses are revoked in case of any issues identified.	<p>Inspection</p> <p>For selected sample of quarter, during the specified period, inspected the access review reports and verified that system access was reviewed and corrective actions were taken for identified deviations.</p> <p>Additionally, inspected the system user listing and verified that the access of identified deviation during quarterly review were revoked.</p>	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 13			
Controls provide reasonable assurance that logical access to programs, data, workstations, network, and network infrastructure is restricted to authorized and appropriate users.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
12.6	KFintech has defined and documented password policy stipulating minimum length, password history, password expiry, minimum password age, complexity and account lockout threshold. The password policy is enforced within KFintech system including Databases, Servers and workstations.	<p>Inspection</p> <p>Inspected the KFintech Password usage and management policy document to verify that password settings stipulating minimum length, password history, password expiry, minimum password age, complexity and account lockout settings were defined and documented.</p> <p>Additionally, inspected the group policy defined on Kfintech and verified that password parameters are enforced align with password policy document.</p>	No exception noted.
12.7	Password protected screensavers are enabled onworkstations including desktops and laptops. Servers are also configured with Idle session timeout capability.	<p>Inspection</p> <p>Inspected the group policy defined on KFintech domain and verified that password protected screensavers were enabled on workstations. Also verified that idle system timeout were defined on servers.</p>	No exception noted.
12.8	Antivirus is installed on workstations and Servers along with Latest signatures are automatically downloaded and pushed from KFintech centralized antivirus Server.	<p>Inspection</p> <p>For sample of workstations and Servers, inspected the Antivirus settings and verified that Antivirus client were installed and configured to receive updates from the Antivirus Server.</p>	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 13			
Controls provide reasonable assurance that logical access to programs, data, workstations, network, and network infrastructure is restricted to authorized and appropriate users.			
Control Activity		Tests Performed by the Service Auditor	Results of Testing
12.9	All incoming and outgoing e-mails are scanned for virus and spam through the installed e-Mail scanner.	Inspection Inspected configuration of email scanner and verified that all incoming and outgoing e-mail were configured to scan for virus, malware and blacklisted file types.	No exception noted.
12.10	Employee requiring specific product/ fund access in applications raises request for the same which requires approval from Authorized personnel basis which concerned team creates the access within those application.	Inspection For selected sample of users created within the applications, during the specified period, inspected the corresponding User Track ticket or the hard copy access request form and verified that the request were approved by the USC/UH. Also, for selected sample of users, inspected the application user listing and verified that the user were created post approval.	No exception noted.
12.11	When an employee separates from KFinTech, concerned team revokes access to application/ applications based on the access revocation requests raised.	Inspection For selected sample of separated employees, inspected the corresponding User Track ticket raised for requesting application access revocation and verified that the access revocation was raised in a timely manner. Additionally, inspected the application user listing and verified that the access of sample separated employees were revoked.	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

4.13. Third Party Management

<p>Control Objective 14</p> <p>Controls provide reasonable assurance that Kfin assesses and manages risks associated with vendors and business partners.</p>			
<p>Control Activity</p>		<p>Tests Performed by the Service Auditor</p>	<p>Results of Testing</p>
<p>13.1</p>	<p>Company enters a contract with Vendor / Business partners which includes scope of services or product specifications, roles and responsibilities, compliance requirements, service levels, communication Protocols and termination clause permitting the company to terminate any services from Vendor/ Business Partners. Contracts are reviewed by Business and Legal team before sign-off.</p>	<p>Inspection</p> <p>For selected sample of vendors/,usiness partners inspected the contract/ agreements to verified that contracts included scope of services or product specifications, roles and responsibilities, compliance requirements, service levels, communication Protocols and termination clause permitting the company to terminate any services from Vendor/ Business Partners.Also, verified that contracts/agreements were reviewed and approved from Business and Legal team before sign-off.</p>	<p>No exception noted.</p>

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.

Control Objective 14		
Controls provide reasonable assurance that Kfin assesses and manages risks associated with vendors and business partners.		
Control Activity	Tests Performed by the Service Auditor	Results of Testing
13.2 Vendor / Business Partner assessment is performed during vendor on boarding and company annually assesses the performance of critical vendors and business partners	<p>Inspection</p> <p>For selected sample of vendors/business partners onboarded during the specified period, inspected the vendor risk assessment records and verified that vendors/business partner were onboarded post clearance of assessment only.</p> <p>Additionally, for selected samples of critical vendors/business partners, inspected the annual vendor risk assessment records and verified that assessment was performed in accordance to Kfin’s vendor risk management policies and procedures.</p>	No exception noted.
13.3 Service Level Agreements (SLAs) are defined for vendors and any deviations from SLAs are reviewed and approved by the Authorized Personnel	<p>Inspection</p> <p>For selected samples of vendors, inspected the contracts/agreements and verified that Service Level Agreements (SLAs) were defined for vendors and reviewed & approved by the Authorized Personnel.</p>	No exception noted.

Privileged and Confidential

This report, including the description and test of controls in Section 4 of this report, is intended solely for the information and use of the Company, user entities of the KFin’s Business Process and general IT controls related to inscope infrastructure system during some or all of the Specified Period, and the independent auditors of such user entities. This report is not intended to be and should not be used by anyone other than those specified parties.



© GRANT THORNTON BHARAT LLP
All rights reserved.
India member firm of Grant Thornton International Ltd.

This report is confidential. Unauthorized use of this report in whole or in part is strictly prohibited.