Service Organization Controls 3 Report

For the period February 1, 2023, to January 31, 2024

REPORT ON CONTROLS PLACED IN OPERATION AT INVESTOR TECHNOLOGY GROUP, INC. (MOSAIC PLATFORM)
RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY

Management's Report of its Assertions on the Effectiveness of its Controls over the Mosaic Platform Based on the Trust Services Criteria for Security, Availability, and Confidentiality for the Period February 1, 2023, to January 31, 2024.

February 25, 2024

We, as management of Investor Technology Group, Inc. ("Mosaic") are responsible for:

- Identifying the Mosaic Platform ("System") and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of our principal service commitments and service requirements that are the objectives of our System, which are presented in Attachment A
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories and associated criteria that are the basis of our assertions

Carved-out Unaffiliated Subservice Organizations: Mosaic uses Amazon Web Services ("AWS") to provide infrastructure management services and OpenAI for artificial intelligence ("AI")-enabled services. The description of the boundaries of the System presented in Attachment A indicates that complementary controls at AWS and OpenAI that are suitably designed and operating effectively are necessary, along with controls at Mosaic to achieve the service commitments and system requirements. The description of the boundaries of the System presents the types of complementary subservice organization controls assumed in the design of Mosaic's controls. It does not disclose the actual controls at the carved-out AWS or OpenAI.

We confirm to the best of our knowledge and belief that the controls over the System were effective for the period February 1, 2023, to January 31, 2024, to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus – 2022*).

Very truly yours,

Ian Gutwinski
Chief Executive Officer

Building a better
working world

Kost Forer Gabbay & Kasierer
144 Menachem Begin Road, Building A
Tel-Aviv 6492102, Israel

Tel: +972-3-6232525
Fax: +972-3-5622555
ey.com

Independent Service Auditor's Report

The Board of Directors
Investor Technology Group Inc. ("Mosaic")

Scope

We have examined Investor Technology Group Inc. ("Mosaic") management's assertion, contained within the accompanying "Management's Report of its Assertions on the Effectiveness of its Controls over the Mosaic Platform Based on the Trust Services Criteria for Security, Availability, and Confidentiality for the Period February 1, 2023 to January 31, 2024" (the "Assertion"), that Mosaic's controls over the Mosaic Platform (the "System") were effective for the period February 1, 2023 to January 31, 2024, to provide reasonable assurance that Mosaic's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022).

Carved-out Unaffiliated Subservice Organizations: Mosaic uses Amazon Web Services ("AWS") (subservice organizations) to provide infrastructure management services and OpenAI for artificial intelligence ("AI")-enabled services. The description of the boundaries of the system presented at Appendix A indicates that complementary subservice organizations' controls that are suitably designed and operating effectively are necessary, along with related controls at Mosaic, to provide reasonable assurance that Mosaic's service commitments and system requirements are achieved based on the applicable trust service criteria. The description of the boundaries of the system presents the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS and OpenAI. Our procedures did not extend to the services provided by AWS or OpenAI and we have not evaluated whether the controls management assumes have been implemented at AWS or OpenAI have been implemented or whether such controls were suitably designed and operating effectively for the period February 1, 2023 to January 31, 2024.

Management's responsibilities

Mosaic's management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that Mosaic's service commitments and system requirements were achieved. Mosaic management is also responsible for providing the accompanying assertion about the effectiveness of controls within the system, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of the System

Our responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects.

An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Mosaic's relevant to security, availability and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we consider necessary in the circumstances.

The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Mosaic's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

We are required to be independent of Mosaic and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Inherent limitations:

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Mosaic's service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the System or controls, or the failure to make needed changes to the System or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion:

In our opinion, Mosaic's controls over the System were effective for the period February 1, 2023 to January 31, 2024, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Very truly yours,

Kost Forer Gabbay and Kasierer

Kost Forer Gabbay and Kasierer
A member firm of Ernst & Young Global
February 25, 2024
Tel Aviv, Israel

Attachment A: Description of the Mosaic platform

Company Overview and Background

Investor Technology Group, Inc. (the “Company”), the creator of the Mosaic Digital Deal Modeling platform (“Mosaic” or the “Platform”), helps investment professionals at private equity firms, investment banks, and corporate development teams to rapidly build and check financial models used in the underwriting and due diligence of business acquisitions. Mosaic’s software enables these players to conduct financial analysis on new acquisition opportunities, collaborate within deal teams on critical model assumptions, and analyze trends in their proprietary financial modeling over time.

Since its founding, Mosaic has deployed its financial modeling software within some of the largest private equity firms in the world – the existing customer base collectively manages over $500 billion in assets, and Mosaic has been used to analyze company acquisitions worth billions of dollars.

Products and Services

The Company’s core offering is the financial model automation and collaboration platform branded “Mosaic”. The Company’s marketing website can be accessed at www.mosaic.pe. The Digital Deal Modeling platform can also be augmented by an Artificial Intelligence (“AI”)-enabled module branded Mosaic Vision™ which allows users to upload a screenshot of a financial model table for automatic ingestion and interpretation – saving end users the manual data entry required in the past to achieve the same functionality. Mosaic Vision™ is powered in part by OpenAI – access via API calls and thus governed by OpenAI's API privacy policy. Neither OpenAI nor Mosaic train their models on customer data uploaded into Mosaic Vision.

Overview of Mosaic’s Internal Control

A company’s internal control is a process – affected by the entity's boards of directors, management, and other personnel – designed to enable the achievement of objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations. The following section is a description of the five components of internal control for the Company.

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its employees. It reflects the overall attitude, awareness, and actions of management, the Board of Directors, and others concerning the importance of controls and the emphasis given to controls in the entity’s policies, procedures, methods, and organizational structure. Mosaic’s executive management recognizes its responsibility for directing and controlling operations and for establishing, communicating, and monitoring control policies and procedures.

Control Activities

Control activities are the policies and procedures that enable management directives to be carried out to address risks to the achievement of the entity’s objectives. Mosaic’s operating and functional units are required to implement control activities that help achieve business objectives associated with:

(1) The reliability of financial reporting,
(2) The effectiveness and efficiency of operations, and
(3) Compliance with applicable laws and regulations.

The controls activities are designed to address specific risks associated with Mosaic operations and are reviewed as part of the risk assessment process. Mosaic has developed formal policies and procedures covering various operational matters to document the requirements for performance of many control activities.

Risk Assessment

Risk identification: The process of identifying, assessing, and managing risks is a critical component of Mosaic's internal control system. The purpose of Mosaic's risk assessment process is to identify, assess and manage risks that affect the organization's ability to achieve its objectives. Risk analysis embodies identification of key business processes in which potential exposures of some consequence exist. Exposures defined by Mosaic consider both internal and external influences that may harm the entity's ability to provide reliable services. They include (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets. It also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and service, business partners, customers, and others with access to Mosaic's information systems.

Risk assessment: Ongoing monitoring and risks assessment procedures are built into the normal recurring activities of Mosaic and include regular management and supervisory activities. Identified risks are analyzed through a process that includes estimating the potential significance of the risk. The assessment includes how the risk should be managed and whether to accept, avoid, reduce, or share the risk. Managers of each department are regularly in touch with personnel and may question the accuracy of information that differs significantly from their knowledge of operations. The Management Team considers the significance of the identified risks by determining the criticality and impact of the risks.

Risk Mitigation: Once the severity and likelihood of a potential risk has been assessed, management considers how the risk should be mitigated. The mitigation process involves making inferences based on assumptions about the risk and carrying out a cost-benefit analysis. Necessary actions are taken to reduce the level of severity or the likelihood of the risk occurring, and the control activities necessary to mitigate the risk are identified. Mosaic selects and develops control activities that contribute to the mitigation of risks to the achievement of the company's objectives to acceptable levels. The risk mitigation process is integrated with the company's risk assessment. Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet Mosaic's objectives during response, mitigation, and recovery efforts.

Risk responses that address and mitigate risks are carried out. The Management Team considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities. The relevant business processes are thoroughly controlled using a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls. Financial impacts of the risks are also taken into consideration during the process. Mosaic assesses the risks associated to their vendors and business partners on a periodic basis.

Fraud assessment: Controls are in place at Mosaic to evaluate and monitor the risks of fraud. The assessment of fraud considers:

- Fraudulent reporting
- Possible loss of assets
- Incentives and pressures
- Corruption resulting from the various ways that fraud and misconduct can occur
- How management and other personnel might engage in or justify inappropriate actions

Information and Communication

Information and communication are an integral component of Mosaic's internal control system. It is the process of identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage, and control the organization's operations. At Mosaic, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

General Company Policies

Formal written policies for the principles and processes within the organization are developed and communicated so that personnel understand Mosaic's objectives. The assigned policy owner updates the policy annually and the policy is reviewed and approved by designated members of management. In addition, responsibility and accountability for developing and maintaining the policies are assigned to the Mosaic relevant teams and are reviewed and approved on an annual basis by the Management Team.

Monitoring

Managers at Mosaic are responsible for monitoring the quality and effectiveness of the various operations and internal controls as a routine part of their activities. Performance reports and statistics are generated on a regular basis and presented to Executive management for evaluation. Management uses automated reports created through various applications and processes to monitor the efficiency of specific processes and the effectiveness of specific key controls. Metrics produced from these systems are used to identify the strengths and achievements, as well as the weaknesses, inefficiencies or potential performance issues with respect to a specific process. Managers have responsibility for informing their direct reports about these items at the appropriate time. The Executive Management Team monitors the progress with respect to Mosaic service processes on a regular basis.

Analysis of root cause is performed through various tools and meetings, and corrective measures are communicated to relevant groups through e-mails, meetings, and a project portal tool to prevent future occurrences.

Support

Mosaic's customer support procedures are designed to handle and resolve issues and requests in a timely manner. This includes issues that are internally identified, or issues submitted by clients. Mosaic provides its clients with one level of support comprising an email support address available 24/7/365 or a phone support line available during regular business hours.

Ticketing and Management

Mosaic opens a ticket when an issue is raised by a client or when an issue is proactively identified. Mosaic uses a third-party application to manage, classify and ticket the client support-related issues. Tickets are classified by the level of urgency and assigned to the appropriate support tier for resolution. Security-related issues are classified as the highest priority.

Incident Management Process

Mosaic employees are instructed to use email to report breaches in system security, availability, and confidentiality to the CEO or CTO. The Company has a procedure and process in place to raise and manage Information Security Incidents. Incidents are classified according to the level of urgency and importance. Incidents can be submitted by email following a customer-identified issue, through both manual and automated proactive checks. Resources are allocated to investigate the incident and resolve the issue. The CEO and CTO are responsible for escalating critical incidents. By procedure, incident notifications are sent to customers in the case that their data has been impacted.

Escalation Process

Mosaic's goal is to resolve issues in an efficient manner. The issue is tracked and updated in the support ticketing system. Tickets are escalated as deemed necessary to the CEO. Service interruptions are communicated to clients using e-mail and the company's status website (https://status.mosaic.pe/).

Logical and Physical Access

Mosaic has established an organization-wide information security policy designed to protect information at a level commensurate with its value. The policy dictates security controls for media where information is stored, the systems that process it, as well as infrastructure components that facilitate its transmission. A security policy is documented by Mosaic management and reviewed and approved on an annual basis.

Access Control, User and Permissions Management

Mosaic builds its production environment system architecture using the AWS services. Firewall detailed configuration is defined and performed by the Mosaic Development team. In addition, the global management of the Mosaic infrastructure is performed by Mosaic using the AWS console and software development kit ("SDK"). This interface allows Mosaic to, among others, (1) add, modify, and manage servers, (2) create security policies as they relate to these servers, (3) configure a few network and firewall parameters, (4) manage the databases and (5) manage the AWS users. Firewalls separate the internal network from the internet. Firewall settings have been configured to allow only authorized traffic, as defined in Mosaic's Security Policy.

Mosaic manages and delivers its services using a variety of systems and environments. As previously described, information security controls and procedures are implemented throughout these systems, to help prevent unauthorized access to data. Authorized access to the AWS' hosting environment is performed by authorized Mosaic employees using two-factor authentication. The database servers reside within the production environment. The access to the production environment servers is restricted to authorized personnel (refer to section 'Production Environment Logical Access').

Principle of Least Privilege

Mosaic applies the "Principle of Least Privilege" to access controls within the organization – meaning that only those employees with a bona fide business reason to access certain types of confidential data are authorized and able to do so. This is best exemplified in the Company's approach to Customer confidential data contained in the production environment – where only the Company's CEO and CTO have access for the purpose of assisting customers with task execution or troubleshooting issues that arise.

Recertification of Access Permissions

Mosaic has implemented a recertification process to help ensure that only authorized personnel have access to the production interface, servers, environments, and databases. Employees whose job functions have changed and therefore no longer require access to a group of user permissions will have their access disabled or modified as needed.

Revocation Process

Terminated employees complete a termination clearance process on their last day at Mosaic while the termination notification is documented and accessible within the Mosaic Internal IT management ticket system. This process includes revocation of access permissions to the systems and premises, as well as the return of the property, data, and equipment.

Production Environment Logical Access

Access to the customer environment web application interface is performed using SSO credentials governed by the Mosaic Azure Active Directory. Access to the Production databases is limited to VPN access with SSO credentials, with only the CEO and CTO having access as governed by the Mosaic Azure Active Directory.

Remote Access

Mosaic's production environment servers are protected by the AWS tools and controls configured by Mosaic. Mosaic employees are granted remote access to the AWS environment based on the need-to-work principle.

Physical Access and Visitors

Mosaic recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures and controls have been implemented to help prevent unauthorized access to data, assets and restricted areas. Office access cards are issued to Mosaic's employees by the administrative manager. Permissions to issue cards and grant access are restricted to the administrative manager and the authorized designees.

Description of the Production Environment

The processes described below are executed within Mosaic's production environment, hosted in data centers by a third-party vendor, Amazon Web Services in the United States.

Production Environment

The processes described below are executed within Mosaic's production environment, which is hosted in Amazon Web Services (AWS) Virtual Private Cloud located globally. The facilities comply with standards of quality, security, and reliability that enable Mosaic to provide its services in an efficient and stable manner.

Software Development Lifecycle (SDLC) Overview

The software development lifecycle consists of the following phases:

- Determine system need phase
- Determine system requirements phase
- Design system component phase
- Build system component phase
- Evaluate system readiness phase
- System deployment phase

Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved by the Management Team within the Change Management application. Each change goes through a life cycle. Product requirements are constantly being collected from customers and from market research by Mosaic's CEO. These requirements combined with additional engineering improvement requirements are discussed by the CEO and CTO and are converted to Epics, Stories and Tasks that contains more specific description of required features and changes.

The Engineering team reviews the Epics, Stories and Tasks and provide a high-level effort estimation for every feature. The CEO works with the Engineering team to create a prioritized features list based on the effort estimation and required timeline of the release. The CTO collects the features list, validates the total effort vs teams foreseen progress and creates a release plan specifying integration dates, Feature Freeze and Code Freeze dates as well as the release date of first release candidate to production.

Engineers are engaged with ongoing enhancements of the product functionality. Engineers' check-in their respective code to a common source control system that provides extensive version tracking functionality and other software building abilities. All changes which are added to the Source Control contain information linking them to the relevant features and bugs. Code changes are reviewed along with the Pull Request ("PR") performed by the engineer.

Software Testing and QA Process: The Mosaic engineering team tests each feature using a mix of manual and automated tests. Upon each PR creation, Mosaic's automated code scanners review the newly created code for bugs or other issues. Reviewers assigned to a PR are responsible for running the new feature locally and manually testing the application for errors or bugs. During this stage, any bugs are reported in the PR comments and resolved before the PR is approved and merged.

Software Release: It is mandatory that all automation tests pass and that scans are free of Critical and High findings prior to a release. Mosaic also conducts a yearly pen testing of which findings are fixed in the following release. The released version is verified by the CEO and CTO prior to releasing to customers. Bugs or functional requests that are made by customers are reported in the development workflow tool employed by Mosaic's development team and marked High Priority. Faults reported during this stage are analyzed by the CEO and CTO and fixed as soon as practicable. Requests for functional enhancements are added to Mosaic's product development backlog for future releases.

Monitoring the Change Management Processes

A change management meeting is performed as needed, to assess the risks identified and review changes required to the production environment. Action items are updated within as part of the process and change is approved only after review and assessment. In addition, metric reports are regularly issued to the Management Team to provide them with key indicators regarding the change management process.

Infrastructure Change Management Overview

Mosaic regularly makes changes within its production environment in response to the evolving client and market needs. These changes include adding/removing/changing the configuration policies of the existing servers or performing routine maintenance activities, software updates, and other infrastructure-related changes accordingly to available possibilities provides by the third-party vendors. Infrastructure changes are documented within the Change Management process. The request is reviewed and approved by the CTO and CEO. Emergency changes are performed and updated as part of hot fixes, which follow the same process as described above though the timeframe may be shortened, and approvals may be provided after the change was already performed.

Network Infrastructure

Robust network infrastructure is essential for reliable and secure real-time data communication between the Mosaic cloud service components. To provide sufficient capacity, the Mosaic network infrastructure relies on platforms provided by Amazon Web Services (AWS). To ensure appropriate network security levels, Mosaic security standards and practices are backed by a multi-layered approach that incorporates practices for preventing security breaches, ensuring confidentiality, integrity, and availability.

Web, Application and Service Supporting Infrastructure Environment

Mosaic utilizes AWS's clustered infrastructure design to provide redundancy and high availability. In addition, the infrastructure is configured in a way that enables auto scaling capabilities. This allows supporting high performance during demand spikes to the services.

Production Monitoring

Mosaic uses a suite of monitoring tools to monitor its service. Alerts are sent to relevant stakeholders based on pre-defined rules. Mosaic's production network encompasses numerous components including web services, application and data server types, database, monitoring tools, and redundant network equipment provided as part of the AWS services. Key Mosaic staff members are notified of events related to the security, availability, or confidentiality of service to clients.

Security and Architecture

Mosaic provides a secure, reliable, and resilient Software-as-a-Service platform that has been designed from the ground up based on industry best practices. The below addresses the network and hardware infrastructure, software and information security elements that Mosaic delivers as part of this platform, database management system security, application controls and intrusion detection monitoring software.

Data Center Security

Mosaic relies on Amazon Web Services' global infrastructure, including the facilities, network, hardware, and operational software (e.g., host OS, virtualization software, etc.) that support the provisioning and use of basic computing resources and storage. This infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards: FedRAMP, HIPAA, ISO 27001:2015, AICPA SOC 1, SOC 2, SOC 3 and PCI-DSS and more.

Infrastructure Security

End-to-End Network Isolation – The Virtual Private Cloud is designed to be logically separated from other cloud customers and to prevent data within the cloud being intercepted.

External & Internal Enforcement Points – All servers are protected by restricted AWS firewall rules. The configuration of AWS firewall rules is restricted to authorized personnel.

Server Hardening – All servers are hardened according to industry best practices.

Segregation Between Office and Production Networks – There is a complete separation between the Mosaic corporate network and the production network. Access to the production environment is granted to authorized personnel only, and traffic between the networks is sent over an encrypted tunnel.

Application Security

Penetration Testing - The penetration tests include, among others, procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own. In addition, security scans are performed on an annual basis. The penetration tests and security scans are performed by a reputable third-party vendor.

Vulnerabilities Management – Web application architecture and implementation follow OWASP guidelines. The application is regularly tested for common vulnerabilities (such as CSRF, XSS, SQL Injection).

Segregation of Customer Data – Mosaic employs a login system and authorization mechanism based on industry best practices. During each user request, a validation process is performed through encrypted identifiers to ensure that only authorized users gain access to the specific data.

Operational Security

Configuration and Patch Management – Mosaic employs a centrally managed configuration management system, including infrastructure-as-code systems through which predefined configurations are enforced on its servers, as well as the desired patch levels of the various software components.

Security Incident Response Management – Whenever a security incident of a physical or electronic nature is suspected or confirmed, Mosaic's engineers are instructed to follow appropriate procedures. Customers and legal authorities will be notified as required by Privacy regulations.

Antivirus – Antivirus definition updates are performed and monitored on a regular basis by the IT and Operations teams. The employees' laptops are encrypted with the use of a 256-bit AES encryption.

Availability Procedures

Mosaic's production environment is fully managed as part of the AWS services and monitored by Mosaic's Development team using the tools provided by AWS as well as internal tools. The application level is fully managed by the Mosaic Development team. Mosaic has implemented the operations management controls described below to manage and execute production operations.

Database Backup

Mosaic's databases are hosted at AWS and fully backed up on a daily basis. The backup system automatically generates a backup log. In case of failure, a notification is sent to the CEO and CTO. The Company can deploy these backup replicas to alternative data centers for high-availability standards in case of a disaster.

Restoration

Backup data captured as part of the daily backup procedures is restored automatically into a separate environment in order to determine the integrity of data and potential data recovery issues.

Data center availability procedures

AWS provides Mosaic with a secured location implementing security measures to protect against environmental risks or disaster.

Business Continuity Plan (BCP)

Mosaic has developed a Business Continuity Plan to enable the company to continue to provide critical services in case of a disaster. Mosaic maintains a backup server's infrastructure at a separate location within the AWS environments. The backup server's infrastructure has been designed to provide clients with business-critical services until the disaster has been resolved and the primary system is fully restored. The alternative processing environment is wholly managed by appropriate Mosaic personnel, as is the case with the primary production environment.

Monitoring Usage

The Management Team is updated on an annual basis on security, confidentiality, and availability non-compliance issues that may come up and addresses them as needed. Such issues are documented as part of a support process and if necessary, notifications are sent to the Development team or the CEO. Change reports, vulnerability reports from production and monitoring tools as well as support metrics are reviewed and discussed in relation to organization's system security, availability, and confidentiality policies. In addition, environmental, regulatory, and technological changes are monitored. Their effects are assessed, and their policies are updated accordingly. A summarized protocol is made available to relevant managers and team members.

Confidentiality Procedures

Customer confidentiality is key factor in Mosaic. As such, Mosaic has implemented security measures to ensure the confidentiality of its customer's sensitive personal and commercial information. The security measures aim to prevent unauthorized access, disclosure, alteration, or destruction of sensitive personal information. Encryption between Mosaic customers and the Mosaic application as well as between Mosaic sites is enabled using an authenticated TLS tunnel. Encrypted based on AWS's data at rest encryption policies which impose several layers of encryption to protect customer data at rest in Amazon Web Services products

****