DataRails

SSAE 18 (SOC 1) Type II Report
For the period from March 1, 2021 to February 28, 2022

Description of the DataRails Platform
Relevant to Security, Availability and Confidentiality
With the Independent Service Auditor's report
Including Tests Performed and Results thereof.

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations

TM

TABLE OF CONTENTS

DataRails

Section I – DataRails Ltd.'s Management Assertion

April 1, 2022

We have prepared the description of DataRails Ltd.'s Platform system entitled, "DataRails Ltd.'s Description of Its DataRails Platform System" (Description) for processing user entities' transactions throughout the period March 1, 2021 to February 28, 2022 for user entities of the system during some or all of the period March 1, 2021 to February 28, 2022, 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 the Description, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

DataRails Ltd. uses Microsoft Azure to provide infrastructure management services. The Description includes only the control objectives and related controls of DataRails Ltd. and excludes the control objectives and related controls of the subservice organization. The Description also indicates that certain control objectives specified in the Description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The Description does not extend to controls of the subservice organization.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of DataRails Ltd.'s controls are suitably designed and operating effectively, along with related controls at the service organization. The Description does not extend to controls of the user entities.

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

a. The Description fairly presents the *DataRails Platform* system (System) made available to user entities of the System during some or all of the period March 1, 2021 to February 28, 2022 for processing their transactions as it relates to controls that are likely relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description:

(1) Presents how the System made available to user entities of the system was designed and implemented to process relevant transactions, including, if applicable:

- The types of services provided, including, as appropriate, the classes of transactions processed.
- The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the System.
- 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 prepared for user entities.
- How the System captures and addresses significant events and conditions, other than transactions.
- The process used to prepare reports and other information for user entities.
- Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
- The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls.

- Other aspects of our control environment, risk assessment process, information, and communication systems (including the related business processes), control activities, and monitoring activities that are relevant to the services provided, including processing and reporting transactions of user entities.

(2) Includes relevant details of changes to the System during the period covered by the Description.

(3) Does not omit or distort information relevant to the System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the System and their user auditors, and may not, therefore, include every aspect of the DataRails Platform System that each individual user entity of the System and its user auditor may consider important in the user entity's own particular environment.

b. The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period March 1, 2021 to February 28, 2022 to achieve those control objectives, if subservice organizations applied the complementary subservice organization controls and user entities applied the complementary user entity controls assumed in the design of DataRails Ltd.'s controls throughout the period March 1, 2021 to February 28, 2022. The criteria we used in making this assertion were that

(1) The risks that threaten the achievement of the control objectives stated in the Description have been identified by management of the service organization.
(2) The controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and
(3) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

DocuSigned by:
Zviki Shimon
652707D8D20C4C9...
Zviki Shimon

CFO

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

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

Section II - Independent Service Auditor's Report

To the management of DataRails Ltd.

Scope

We have examined DataRails Ltd.'s description entitled "Description of DataRails Ltd.'s DataRails Platform system" (Description) throughout the period March 1, 2021 to February 28, 2022 of its DataRails Platform system (System) for processing user entities' transactions and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description (Control Objectives), based on the criteria identified in DataRails Ltd. assertion (Assertion). The Control Objectives and controls included in the Description are those that management of DataRails Ltd. 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 Description indicates that certain Control Objectives can be achieved only if complementary user entity controls assumed in the design of DataRails Ltd.'s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

DataRails Ltd. uses Microsoft Azure to provide infrastructure management services. The Description includes only the Control Objectives and related controls of DataRails Ltd. and excludes the control objectives and related controls of Microsoft Azure. The description also indicates that certain Control Objectives specified by DataRails Ltd. can be achieved only if complementary subservice organization controls assumed in the design of DataRails Ltd.'s controls are suitably designed and operating effectively, along with the related controls at DataRails Ltd. Our examination did not extend to such complementary controls of Microsoft Azure, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

DataRails Ltd.'s responsibilities

DataRails Ltd. has provided the accompanying assertion titled, DataRails Ltd. management assertion (Assertion) about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives. DataRails Ltd. 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.

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 described therein to achieve the related Control Objectives, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our 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 operating effectively to achieve the related Control Objectives throughout the period March 1, 2021 to February 28, 2022. We believe that the evidence we have 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:

- 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, 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.
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related Control Objectives were achieved.
- Evaluating the overall presentation of the Description, the suitability of the Control Objectives, and the suitability of the criteria specified by the service organization in the Assertion.

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 a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the 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 the nature, timing, and results of those tests are listed in the accompanying Section IV - DataRails Ltd.'s control objectives, controls and service auditor's tests of controls and results of tests (Description of Tests and Results).

Opinion

In our opinion, in all material respects, based on the criteria described in DataRails Ltd.'s Assertion:

a. The Description fairly presents the System that was designed and implemented throughout the period March 1, 2021 to February 28, 2022.

b. The controls related to the Control Objectives were suitably designed to provide reasonable assurance that the Control Objectives would be achieved if the controls operated effectively throughout the period March 1, 2021 to February 28, 2022 and if subservice organizations and user entities applied the complementary controls assumed in the design of DataRails Ltd.'s controls throughout the period March 1, 2021 to February 28, 2022.

c. The controls operated effectively to provide reasonable assurance that the Control Objectives were achieved throughout the period March 1, 2021 to February 28, 2022 if complementary subservice organization and user entity controls assumed in the design of DataRails Ltd.'s controls operated effectively throughout the period March 1, 2021 to February 28, 2022.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of management of DataRails Ltd., user entities of DataRails Ltd.'s System during some or all of the period March 1, 2021 to February 28, 2022, 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 misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Kost Forer Gabbay and Kasierer
A member firm of Ernst & Young Global

April 1, 2022
Tel-Aviv, Israel

DataRails

Section III - Description of the DataRails platform for the Period March 1, 2021 to February 28, 2022.

Company Overview and Background

DataRails is a technology solution that tracks, controls, and manages spreadsheets at the enterprise and business level, with no change to the end-user Excel experience. DataRails is a platform that tackles the problem of the Single Version of Truth, by verifying your version, and your team's version of excel spreadsheets, promoting financial integrity in companies and providing better control.

Products and services

- *DataRails platform introduces a technology that databases Excel in real-time transforming it into an enterprise solution. DataRails allows companies to take control and automate Excel based business processing without changing the way their users work.*
- *DataRails' patented technology reads the metadata in Excel (e.g., the formulas, the formatting) and then automatically processes the information to turn it into a structured database. There is no need for the corporation to change its processes; DataRails' flexibility allows companies to keep using the same processes.*

Purpose and Scope of the Report

The scope of this report is limited to the controls supporting DataRails and does not extend to other products and services or the controls at third-party service providers.

Note: Parenthetical references have been included in the following narrative as a cross-reference to the applicable control procedures included in the Description of Criteria, Controls, Tests and Results of Tests section of this report.

Entity Level Controls (ELC's)

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. DataRails executive management recognizes its responsibility for directing and controlling operations and for establishing, communicating and monitoring control policies and procedures. Policy and procedures documents for significant processes that address system requirements and relevant updates are available to DataRails employees on the internal intranet. Policies and procedures are documented, reviewed, and approved on an annual basis by the Management Team.

Authority and Responsibility: Lines of authority and responsibility are clearly established throughout the organization and are communicated through DataRails:

(1) Management operating style;
(2) Organizational structure;
(3) Employee job descriptions; and
(4) Organizational policies and procedures.

Board of Directors: The Board of Directors (BOD) of DataRails is comprised of both external directors and directors who are executive officers of the Company. The external directors are both: (1) Industry experts; (2) Investor representatives. The Board of Directors is actively engaged in the governance of the Company and its strategic direction. The Board of Directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations. It has sufficient members who are independent from management and objective in evaluations and decision making. Members of the Board meet on at least a quarterly basis to discuss matters pertinent to the Company and to review financial information. Part of the Board's mission is to define, maintain and periodically evaluate the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action. The Board's responsibilities include but are not limited to (1) monitoring the actual performance of the Company through its financial results; (2) monitoring the Company's compliance with legal and regulatory requirements; (3) analysis of the budget vs actual results; (4) guiding the Company in the way it funds its operation; (5) approving arrangements with executive officers relating to their employment relationships with the Company, including, without limitation, employment agreements, severance agreements, change in control agreements and restrictive covenants, and (6) approving equity-based compensation plans in which directors, officers or employees may participate. The Board of Directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control. The expectations of the Board of Directors and senior management concerning integrity and ethical values are defined in the standards of conduct. There is a Company Board that meets on a semi-annual basis. The board meeting has a fixed agenda covering (1) financial aspect details, (2) HR, (3) Pipeline of clients, (4) Support issues review, and (5) a discussion on new product features.

Management Philosophy and Operating Style – The Management Team, chaired by the Chief Executive Officer ("CEO"), has been delegated by the Board the responsibility to manage DataRails and its business on a daily basis. DataRails is led by a team with proven ability in managing media and online customer solutions to the global market. In its role, the Management Team assigns authority and responsibility for operating activities and establishes reporting relationships and authorization hierarchies. The Management Team designs policies and communications so that personnel understand DataRails objectives, know how their individual actions interrelate and contribute to those objectives and recognize how and for what they will be held accountable. The Management Team convenes on a weekly basis or more frequently if necessary.

Integrity and Ethical values – Integrity and ethical values are essential elements of the control environment, affecting the design, administration and monitoring of key processes. Integrity and ethical behavior are the products of DataRails ethical and behavioral standards, how they are communicated and how they are monitored and enforced in its business activities. They include management's actions to remove or reduce inappropriate incentives or extraneous pressures, and opportunities that might prompt personnel to engage in dishonest, illegal or unethical acts. They also include the communication of the organization's values and behavioral standards to personnel through policy statements and from the executives. The Board of Directors and Management Team recognize their responsibility to foster a strong ethical environment within DataRails to determine that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct.

Integrity and Ethical values: Integrity and ethical values are essential elements of the control environment, affecting the design, administration and monitoring of key processes. Integrity and ethical behavior are the products of DataRails ethical and behavioral standards, how they are communicated and how they are monitored and enforced in its business activities. They include management's actions to remove or reduce inappropriate incentives or extraneous pressures, and opportunities that might prompt personnel to engage in dishonest, illegal or unethical acts. They also include the communication of the organization's values and behavioral standards to personnel through policy statements and from the executives. The Board of Directors and Management Team recognize their responsibility to foster a strong ethical environment within DataRails to determine that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct.

Human Resources Policy and Practices – Human resource policies and practices relate to hiring, orienting, training, evaluating, promoting and compensating personnel. The competence and integrity of DataRails personnel are essential elements of its control environment. The organization's ability to recruit and retain highly trained, competent and responsible personnel is dependent to a great extent on its human resource policies and practices. Teams are expected to adhere to the DataRails policies that define how services should be delivered and products need to be developed. These are located on DataRails platform and can be accessed by relevant DataRails team members while communicated by emails or other messaging applications, such as Slack, on an as-needed basis. Internal employees sign on a non-disclosure agreement (NDA) as part of their employment contract with the Company while clients and third parties sign on an NDA within the business contract.

Commitment to Competence: Competence at DataRails is designed to (1) identify and hire competent personnel, (2) provide employees with the training and information they need to perform their jobs, (3) evaluate the performance of employees to determine their ability to perform job assignments, and (4) through the performance evaluation process, identify opportunities for growth and job performance improvement. Job descriptions are documented and maintained. Job candidates go through a screening process and appropriate background checks are conducted.

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.

DataRails 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 Microsoft Azure and regulations.

The controls activities are designed to address specific risks associated with DataRails operations and are reviewed as part of the risk assessment process. DataRails has developed formal policies and procedures covering various operational matters to document the requirements for performance of many control activities. New employees (e.g., R&D) go through an onboarding process during which, among others, they are communicated their responsibilities and the different DataRails policies. Based on appropriate development or operational needs, on-going training is performed in an ad hoc manner (**2.7**).

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. DataRails 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 the DataRails's objectives during response, mitigation, and recovery efforts.

Information and Communication

Information and communication are an integral component of DataRails 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 DataRails, information is identified, captured, processed and reported by various information systems, as well as through conversations with clients, vendors, regulators and employees. Weekly management meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls and other strategic initiatives. A management meeting is performed on a weekly basis in order to go through day to day issues.

Senior executives who lead the meetings use information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to organization-wide security policies and procedures are usually communicated to the appropriate DataRails personnel via Slack and/or Shout-Out function in DataRails platform. An internal portal is available for DataRails employees. The portal includes among others: business updates and major activities that occurred within the past month. A description of the DataRails system and its boundaries is documented and communicated to DataRails employees within the internal portal and to external users through the DataRails customer through the support portal.

Monitoring

DataRails uses a suite of monitoring tools in order to monitor its service. Alerts are sent to relevant stakeholders based on pre-defined rules (**3.2**). 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 particular process. Alerts are sent to authorized personnel upon the occurrence of an event related to the system availability, security or confidentiality of data based on pre-defined rules configured within the monitoring systems. Managers are given the responsibility to inform the individuals who report to them about these items at the appropriate time. The DataRails Management Team monitors the progress with respect to DataRails 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 emails, meetings, and a project portal tool in order to prevent future occurrences. Changes impacting customers are communicated to clients through release notes within the DataRails support portal or by email. While internal employees receive notifications at the DataRails internal portal (**2.8**). A security policy is documented by DataRails's management, reviewed and approved on an annual basis. The security policy is available to DataRails employees within the shared folders and to the customer through the support portal.

Asset Management

Company assets are tracked and managed throughout the asset lifecycle. Assets are assigned owners to ensure there is an individual responsible for securing the asset. The tracked assets include production components as well as employee devices that may contain personal data. When assets reach end of life, they are securely destroyed to ensure that data is not recoverable.

Confidentiality Procedures

Customer confidentiality is key factor in DataRails. As such, DataRails has implemented security measures to ensure the confidentiality of its customer's sensitive personal information. Customer passwords are encrypted within the database**.** The security measures aim to prevent unauthorized access, disclosure, alteration or destruction of sensitive personal information. Each access request to the database includes a tenant ID, to ensure that customers are restricted to their own data. In the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive, impacted customers are notified as defined within their Service Level Agreements (SLAs). A confidentiality agreement is disclaimed as it relates to contracts with third-party service providers in accordance with DataRails security policy. Encryption between DataRails customers and the DataRails application is enabled using an authenticated TLS tunnel. Customer's files are encrypted and stored to a secure Microsoft Azure location (**1.6**).

Business Controls

Control Objectives: Controls provide reasonable assurance that:

DataRails retains control in order to track and manage customers' file version uploaded within customer workspace.

Version Control

DataRails software retains a unique and complete copy of each version of each excel file in selected folders. When a new document version is created (saved from the open application or override the file in the folder) or there was a change in the version "review status" (see "Approval Flow"), DataRails automatically creates a new complete unadulterated version in the repository, with the following Meta data:

- The name of the person who saved it (from Active Directory / DataRails users)
- Version date and time
- Version number: When document is added to the library, it starts as version 1. Document versions are simply numbered as 1,2,3,4, and so on.

Version's meta-data can't be modified or edited. No version can be deleted or removed unless specifically requested to support. Older versions can be searched, viewed and retrieved (download). Version Control is implemented and retains a unique and complete copy of each version of each excel file in selected folders (**4.1**).

Change Management

DataRails software identifies, logs, saves and enables monitoring and viewing of change in the content of two versions of the Excel document (**4.2**).

Those changes include:

- Cell values
- Cell formula
- Visual Basic for Applications (VBA)
- Format
    - Whole number
    - Decimal number
    - Currency (Specifically $ or € or £…)
    - Percent
    - Date

Approval Flow

DataRails software enables to set the review status each version, the status field can be one of the following:

- File Status
    - Draft / Final / Signed.
- Approval Flow
    - In Progress/ Pending/Approved/Rejected (**4.3**).

Access Control

DataRails software enables automatic protection of Excel files. In this mode, every file is protected by default upon connection to DataRails. The user who connects the file, becomes the "owner" of the file, and he is the only user who can access the file (open for view or edit). All other users should get the password from the owner in order to access the file.

The owner can retrieve the password from DataRails software and share it with other users (**4.4**).

IT General Controls

Information system Security

Control Objectives: Controls provide reasonable assurance that:

- Logical security tools and techniques are implemented and configured to restrict access to programs, data, and other information resources to authorized personnel.
- Physical access DataRails facilities, computer hardware, software and data are restricted to authorized personnel.

Logical Access

DataRails 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 services where information is stored, the systems that process it, as well as infrastructure components that facilitate its transmission.

Access Control, User and Permissions Management

DataRails builds its production environment system architecture using Microsoft Azure's services. DataRails are using both IP based firewall managed by Microsoft Azure as well firewall Web Application Firewall.

Access to system resources is protected through a combination of firewalls, VPNs, native operating system access controls, database management system security, application controls and intrusion detection monitoring software (**1.10**). Customer's files are encrypted and stored to a secure Microsoft Azure location (**1.6**). The access to the change management application tool is restricted to authorized personnel and based on job needs (**1.5**). The database servers reside within the production environment. The access to the production environment servers is restricted to authorized personnel and to specific set of IP addresses (refer to section 'Production Environment Logical Access'). DataRails uses a dedicated database for data analysis. The access to the database is restricted to authorized personnel (**1.8**).

Recertification of Access Permissions

DataRails has implemented a recertification process to help ensure that only authorized personnel have access to the production environment 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

In order to assist in the prevention of unauthorized access to data, user accounts within the DataRails production environment and supporting tools are disabled promptly upon termination of employment. Terminated employees who had access to the production environment have their permissions removed timely (**1.7**). Terminated employees complete a termination clearance process on their last day at DataRails while the termination notification is documented and accessible within the DataRails platform. 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

The access to the production server is performed using SSH key and is restricted to authorized personnel (**1.1**). The access within the production environment is performed using a two-factor authentication method (**1.2**). Developers do not have access to the production environment (**1.3**). The access to the Azure management console is restricted to authorized personnel (**1.4**).

Physical Access

DataRails recognizes the significance of physical security controls as a key component in its overall security program Physical access to the DataRails office is restricted to authorized personnel using personal electronic identification cards (**1.9**).

Data centers

Production environment physical security is managed by Microsoft Azure. In fact, DataRails employees do not have access to the production environment data center. Microsoft is responsible for implementing an appropriate set of controls in order to address physical security issues. The access to the Azure management console is restricted to authorized personnel (**1.4**).

Monitoring the Change Management Processes

A risk assessment meeting of the Management Team is performed every six months, in order to assess the risks identified and review changes performed to the application. Action items are updated within the DataRails management tool. In addition, metric reports are regularly issued to the Management Team in order to provide them with key indicators regarding the change management process. Risk assessment issues relevant to each member of the Management Team are included in the monthly report submitted to the management forum.

Penetration Testing

A penetration test is performed on an annual basis and high issues are resolved in a timely manner through the SDLC process (**1.11**). 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 a semi-annual basis. The penetration tests and security scans are performed by a reputable third-party vendor. Vulnerabilities of system components to security, availability or confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated as part of the weekly management meetings.

Antivirus

An antivirus/malware solution is installed on employees' laptops in order to detect and prevent infection from unauthorized or malicious software. Antivirus reports are sent to relevant stakeholders on a regular basis (**1.12**). Antivirus definition updates are performed and monitored on a regular basis by the CPO.

System Systems Development and Maintenance

Control Objectives: Controls provide reasonable assurance that:
Only tested and approved software changes are implemented into the live production environment.

Software development and Change Management at DataRails include the development and production changes to the DataRails platform. The processes are performed in a manner that helps ensure applications are properly designed, tested, approved and aligned with DataRails as well as with DataRails clients' business objectives and security standards. Several groups are involved in the SDLC and Change Management processes. They are part of the products and R&D groups, which defines the change roadmap.
Changes are documented and prioritized using tickets within the change management application (**2.2**). In addition, personnel responsible for the design, development, deployment, and operation of systems affecting security, availability and confidentiality are trained on an ad hoc basis (**2.7**).

Change Initiation: Change requests are opened in the change management tool and are reviewed in Product meetings. The requests are reviewed from various angles (e.g. business needs, security, etc.). Changes are documented in Bit Bucket and actions are marked there as well. Changes performed in the source control are automatically connected to a task within the change management application (**2.4**). Every bug is assigned to a developer until it is resolved. Once the bug is fixed, the developer updates the bug status within the change management application and the fix is tested by the QA

team. Automation tests are performed and documented per version in order to identify issues within the application. These tests include reviewing security aspects of the change (**2.3**). New features are communicated to customers, if relevant, through emails, the website or directly through the account manager (**2.1**). A code review process is implemented in order to review the security aspects of the code (**2.5**). The access to the deploy code to the production environment is restricted to authorized personnel (**2.6**).

DataRails Production Environment

The processes described below are executed within the DataRails production environment, hosted in cloud-based data centers by Microsoft Azure.

Communication

All communication regarding new features, bug fixes and customers' issues are shared by using communication and change management platforms. Meetings are scheduled on weekly basis between R&D and Product. In addition, daily sync meetings are performed with the relevant shareholders. Quarterly sync meetings are held with Product and Development, where pull requests status, open bugs and other product issues are discussed.

Computer operations

Control Objectives: Controls provide reasonable assurance that:

- Controls are in place over processing, error monitoring and system availability.
- In the event of significant disruption to normal computer operations at DataRails, critical information systems processing functions can be resumed.

Production Monitoring

DataRails production network encompasses numerous components including web services, application and data server types, database, monitoring tools, and redundant network equipment provided as part of Microsoft Azure services.

Support

DataRails 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. Client issues are documented. Cases are prioritized and processed based on the internal support policy (**3.9**). Client issues are addressed based on the internal DataRails SLA (**3.10**).

Ticketing and Management

DataRails opens a ticket when an issue is raised by a client or when an issue is proactively identified. DataRails uses a third-party CRM 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. In addition, client issues are documented. Cases are prioritized and processed based on the internal support policy (**3.9**).

Database Backup and restoration

Twice a day, the meta data retained in the database is dumped and stored into a bucket enabling geo redundancy (**3.5**). The backup system automatically generates a backup log. In case of failure, a notification is sent to the R&D team. Restore tests are performed on an annual basis. The test includes a full restore to a separate database server and bringing up the database to verify data integrity and accessibility. In addition, a backup restoration is preformed (**3.7**). DataRails performs backups in order to maintain full redundancy in six different locations (**3.4**).

Data Protection Procedures

Data loss prevention processes and technologies are used to restrict the ability to authorize and execute transmission, movement and removal of information. The transmission of data is a key aspect of DataRails's internal controls.

Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points. The transmission of data can be performed through removable media as well as through mobile device. Processes are in place to protect mobile devices (e.g., laptops, smart phones, and tablets) that serve as information assets. When an unauthorized use or disclosure of personal information has occurred, the affected information is identified.

Data center availability procedures

Microsoft Azure provide DataRails with a secured location implementing security measures to protect against environmental risks or disaster.

Risk Assessment

The process of identifying, assessing and managing risks is a critical component of DataRails internal control system. The purpose of DataRails risk assessment process is to identify, assess and manage risks that affect the organization's ability to achieve its objectives. Ongoing monitoring and risks assessment procedures are built into the normal recurring activities of DataRails and include regular management and supervisory activities. 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. Minutes of risk assessment meetings and actions items are documented into emails. On a quarterly basis, as part of the management meeting, risks are reviewed and updated in order to, among others, re-assess risks, review operational aspects of the control environment and monitor the control environment (**3.1**). An awareness meeting is performed on an annual basis during which security, availability and confidentiality issues are discussed and relevant updates are communicated to DataRails employees.

Monitoring

The Management Team is updated on a weekly basis on security, confidentiality and availability non-compliance issues that may come up, and address them as needed. Such issues are documented as part of a Root Cause Analysis (RCA) report created by the Support team, the Operations team or the CTO. Change reports from the Change Management Tool, 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. DataRails uses a suite of monitoring tools in order to monitor its service. Alerts are sent to relevant stakeholders based on pre-defined rules (**3.2**). Alerts are sent to authorized personnel upon the occurrence of an event related to the system availability, security or confidentiality of data based on pre-defined rules configured within the monitoring systems (**3.3**).

Disaster Recovery Plan (DRP)

DataRails has developed a Disaster Recovery Plan to enable the company to continue to provide critical services in case of a disaster. DataRails maintains a backup at a separated location within the Microsoft Azure environments.
The backup file has been designed to allow full functionality of the DataRails platform in case of a disaster in the main data center. DataRails documents and approves on an annual basis a restore document describing the required steps in order to perform a restore (**3.8**).

Availability Procedures

The DataRails production environment is fully managed as part of Microsoft Azure services and monitored by DataRails R&D and Success teams using the tools provided by the third-party vendors as well as internal tools. The application level is fully managed by the DataRails R&D and Success teams. DataRails has implemented the operations management controls described below to manage and execute production operations. Database is replicated in two different datacenters (**3.6**).

Subservice Organization carved-out controls: Microsoft Azure

Microsoft Azure provides infrastructure services. The subservice organization is expected to:

- Implement controls to enable security and monitoring tools within the production environment.
- Implement logical access security measures to infrastructure components including native security or security software and appropriate configuration settings.
- Restrict the access to the virtual and physical servers, software, firewalls and physical storage to authorized individuals and to review the list of users and permissions on a regular basis.
- Implement controls to:
    - Provision access only to authorized persons
    - Remove access when no longer appropriate
    - Secure the facilities to permit access only to authorized persons
    - Monitor access to the facilities
- Be consistent with defined system security, processing integrity availability and security as it relates to the design, acquisition, implementation, configuration modification, and management of infrastructure and software.
- Maintain system components, including configurations consistent with the defined system security, availability, processing integrity and confidentiality related policies.
- Provide that only authorized tested and documented changes are made to the system.
- Implement and maintain procedures consistent with the risk assessment to protect the system against potential risks (for example, environmental risks, natural disasters, and routine operational errors and omissions) that might impair system processing integrity.

Section IV - Description of Criteria, Controls, Tests and Results of Tests

Testing Performed and Results of Tests of Entity-Level Controls

In planning the nature, timing and extent of its testing of the controls specified by DataRails, Kost Forer Gabbay and Kasierer (KFGK) considered the aspects of DataRails' control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE, including Electronic Audit Evidence (EAE) (e.g., controls requiring system-generated populations for sample-based testing), we performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspect the source of the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) tie data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity. In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), we inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Overview of Entity-Level Controls

Internal control is a process designed to provide reasonable assurance that business objectives related to: (1) the reliability of financial reporting, (2) the effectiveness and efficiency of operations, and (3) compliance with applicable laws and regulations, are met. In addition to the tests of operating effectiveness of specific control activities and information and communication systems described below, KFGK's procedures included an examination of the following entity-level controls of DataRails:

- Inspected the Code of Conduct and Code of Ethics provided to DataRails employees and management, noting that it addressed business practices, conflicts of interest, confidentiality, compliance with laws and regulations.
- For a sample of new hires, inspected evidence noting that new hires have read and signed the Code of Conduct.
- For a sample of new hires, inspected documentation noting that new hires attended a training course to provide
- Inspected a sample of formal job descriptions containing employee responsibilities and determined that responsibilities were assigned to employees throughout the Company in order to meet the goals and objectives, operating functions and regulatory requirements.
- Inspected evidence of the personnel training program and noted that training was appropriate for the technical skills and functional responsibilities of the employees.
- Obtained and inspected evidence of periodic management meetings, noting that management actively communicated among themselves and the Board of Directors

Criteria and controls

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by and are the responsibility of DataRails.

The testing performed by Kost Forer Gabbay and Kasierer (KFGK) and the results of the tests are the responsibility of the service auditor. Refer to the Trust Services criteria mapping section for the mapping of these controls to the Trust Services criteria.

Information Technologies General Controls

Control Objectives: Controls provide reasonable assurance that:

- Logical security tools and techniques are implemented and configured to restrict access to programs, data, and other information resources to authorized personnel.
- Physical access DataRails facilities, computer hardware, software and data are restricted to authorized personnel.

Control ID	Control description	Testing Performed by the auditors and Results of Testing
1.1	The access to the production server is performed using SSH key and is restricted to authorized personnel.	Inspected the production server configuration and determined that access was performed using SSH key. Inspected the list of users with access permissions to the production server and determined that it was restricted to authorized. No deviations noted.
1.2	The access within the production environment is performed using a two-factor authentication method.	Inspected the production environment configurations and determined that the access was performed using a two-factor authentication method. No deviations noted.
1.3	Developers do not have access to the production environment.	Inspected list of users with access to the production environment and determined that developers did not have access to the production environment. No deviations noted.
1.4	The access to the Azure management console is restricted to authorized personnel.	Inspected the list of users with access to the Microsoft Azure console and their permissions and determined that it was restricted to authorized personnel.

Control ID	Control description	Testing Performed by the auditors and Results of Testing
		No deviations noted.
1.5	The access to the change management application tool is restricted to authorized personnel and based on job needs.	Inspected the list of users with access to the change management application and determined that it was restricted to authorized personnel based on their job positions. No deviations noted.
1.6	Customer's files are encrypted and stored to a secure Microsoft Azure location.	Inspected the DataRails application database configuration and determined that Customers' Excel files were encrypted. No deviation noted.
1.7	Terminated employees who had access to the production environment have their permissions removed timely.	For a sample of leaving employees, inspected their termination tickets, and determined that user accounts were disabled or deleted on the production, application and database and the Company’s assets were returned timely upon notification of job termination. No deviations noted.
1.8	DataRails uses a dedicated database for data analysis. The access to the database is restricted to authorized personnel.	Inspected list of users with access to the database and determined it was restricted to authorized personnel. No deviations noted.
1.9	Physical access to the DataRails office is restricted to authorized personnel using personal electronic identification cards.	Performed a walkthrough of the DataRails office and determined that access was restricted to authorized personnel using personal electronic identification cards. No deviations noted.
1.10	Access to system resources is protected through a combination of firewalls, VPNs, native operating system access controls, database management system security, application controls and intrusion detection monitoring software.	Inspected inventory of information resources and the security systems protecting each resource. For a sample of resources, observed that the systems were implemented and functioning. No deviations noted.
1.11	A penetration test is performed on a semi- annual basis and high issues are resolved in a timely manner through the SDLC process.	Inspected the penetration Test report and determined it was performed on at least semi-annual basis. High issues were investigated and taken care of as part of the SDLC process or by any necessary means. No deviations noted.

Control ID	Control description	Testing Performed by the auditors and Results of Testing
1.12	An antivirus/malware solution is installed on employees' laptops in order to detect and prevent infection from unauthorized or malicious software. Antivirus reports are sent to relevant stakeholders on a regular basis	Inspected antivirus solution configuration and noted that it was installed on employees' laptops. No deviations noted.

Systems Development and Maintenance

Control Objectives: Controls provide reasonable assurance that:

- Only tested and approved software changes are implemented into the live production environment.

Control ID	Control description	Testing Performed by the auditors and Results of Testing
2.1	New features are communicated to customers, if relevant, through emails, the website or directly through the account manager.	Inspected notifications for a sample of new features and determined that they were communicated to customers, if relevant, through emails, the website or directly through the account manager. No deviations noted.
2.2	Changes are documented and prioritized using tickets within the change management application.	Inspected the change management application workflow and determined that changes were documented and prioritized using tasks within the change management application. No deviations noted.
2.3	Automation tests are performed and documented per version in order to identify issues within the application. These tests include reviewing security aspects of the change.	Inspected screenshots of the automated tests results and determined that the tests were performed and documented per version in order to identify issues within the application and that the tests included reviewing security aspects of the change. No deviations noted.
2.4	Changes performed in the source control are automatically connected to a task within the change management application.	Inspected the change management configuration and determined that changes performed in the source control are automatically connected to a task within the change management application. No deviations noted.
2.5	A code review process is implemented in order to review the security aspects of the code.	Inspected the change management configuration and determined that a code review is implanted in order to review the security aspects of the code. No deviations noted.

Control ID	Control description	Testing Performed by the auditors and Results of Testing
2.6	The access to the deploy code to the production environment is restricted to authorized personnel.	Inspected the list of users with permission to deploy code to the production environment and determined that permissions were restricted to authorized personnel. No deviations noted.
2.7	Based on appropriate development or operational needs, on-going training is performed in an ad hoc manner.	Inspected the training agenda and documentation and determined that R&D and DevOps departments performed regular trainings. No deviations noted.
2.8	Changes impacting customers are communicated to clients through release notes within the DataRails support portal or by email. While internal employees receive notifications at the DataRails internal portal.	For a sample of change, inspected release notes, emails and notifications and determined that changes impacting customers were communicated to clients through release notes within the DataRails support portal or by email. While internal employees received notifications at the DataRails internal portal. No deviations noted.

Computer Operations

Control Objectives: Controls provide reasonable assurance that:

- Controls are in place over processing, error monitoring and system availability.
- In the event of significant disruption to normal computer operations at DataRails, critical information systems processing functions can be resumed.

Control ID	Control description	Testing Performed by the auditors and Results of Testing
3.1	On a quarterly basis, as part of the management meeting, risks are reviewed and updated in order to, among others, re-assess risks, review operational aspects of the control environment and monitor the control environment.	Inspected a sample of management meeting minutes and determined risks were reviewed and updated in order to among others, re-assess risks, review operational aspects of the control environment and monitor the control environment. No deviations noted.
3.2	DataRails uses a suite of monitoring tools in order to monitor its service. Alerts are sent to relevant stakeholders based on pre-defined rules.	Inspected DataRails' monitoring dashboards and configuration and determined that DataRails used a suite of monitoring tools in order to monitor its

Control ID	Control description	Testing Performed by the auditors and Results of Testing
		services. Alerts were sent to relevant stakeholders based on pre-defined rules. No deviations noted.
3.3	Alerts are sent to authorized personnel upon the occurrence of an event related to the system availability, security or confidentiality of data based on pre-defined rules configured within the monitoring systems.	Inspected uptime report of DataRails system and determined that alerts were sent in case of deviations to authorize employees. No deviations noted.
3.4	Backups are performed by DataRails in order to maintain full redundancy in six different locations for files.	Inspected the backup configuration and determined that backups were performed according to the policy in order to maintain full redundancy in six different locations. No deviations noted.
3.5	Twice a day, the meta data retained in the database is dumped and stored into a bucket enabling geo redundancy.	Inspected screenshots of the meta data retention in the database and noted that meta data was dumped and stored into a bucket enabling geo redundancy. No deviations noted.
3.6	The Database is replicated in two different datacenters.	Inspected the Database server's configuration and determined that the databases were replicated to two availability zones. No deviations noted.
3.7	Backup restoration is performed on at least annual basis.	Inspected the backup configuration and determined that backup was restored. No deviations noted.
3.8	DataRails documents and approves on an annual basis a restore document describing the required steps in order to perform a restore.	Inspected the restoration test result and determined that the restore process was performed successfully and documented on an annual basis.

Control ID	Control description	Testing Performed by the auditors and Results of Testing
		No deviations noted.
3.9	Client issues are documented. Cases are prioritized and processed based on the internal support policy.	Inspected a sample of clients' issues and determined that issues raised to the support team were documented within the CRM tool. Cases were prioritized and processed based on the internal support policy. No deviations noted.
3.10	Client issues are addressed based on the internal DataRails SLA.	Inspected a sample of client issues resolution and determined that they were handled based on the internal DataRails SLA. No deviations noted.

Business Control

Control Objectives: Controls provide reasonable assurance that:

DataRails retains control in order to track and manage customers' file version uploaded within customer workspace.

Control ID	Control description	Testing Performed by the auditors and Results of Testing
4.1	Version Control is implemented and retains a unique and complete copy of each version of each excel file in selected folders.	Inspected the version control implementation and noted that unique copy version was retained for each file in selected folders. No deviations noted.
4.2	DataRails software identifies, logs, saves and enables monitoring and viewing of change in the content of two versions of the Excel document.	Inspected DataRails software configurations for identifying, logging and saving of information from the spreadsheet used by DataRails platform and determined that DataRails software had configured and enabled monitoring and viewing of change in the content of two versions of Excel document.

Control ID	Control description	Testing Performed by the auditors and Results of Testing
		No deviations noted.
4.3	Each version cannot have more than one review status and once review status is set – it cannot be modified or removed.	Inspected DataRails platform version control status configuration and determined that only one review was set that could not be modified or removed. No deviations noted.
4.4	Access to the file is defined by the file owner.	Inspected the file configuration and determined that the access to the files was defined by the file owner. No deviations noted.
4.5	Customers go through onboarding process in order to get training on how to use DataRails platform	Inspected Customers onboarding playbook and determined that customers get it in order to understand how to use the DataRails platform. No deviations noted.

****