payouts.com

SOC 1 Type II Report

For the Period of October 1, 2023 to September 30, 2024

DESCRIPTION OF MRKTER TECHNOLOGIES L.B.O. LTD'S PLATFORM SYSTEM
FOR THE PERIOD OCTOBER 1, 2023 TO SEPTEMBER 31, 2024
WITH THE INDEPENDENT SERVICE AUDITOR'S REPORT
INCLUDING TESTS PERFORMED AND RESULTS THEREOF

Table of Contents

payouts.com

Section I - Mrkter Technologies L.B.O Ltd's Management Assertion

March 31,2025

We have prepared the description of Mrkter Technologies L.B.O Ltd's Payouts Platform system entitled, "Mrkter Technologies L.B.O Ltd's Description of Its Payouts Platform System" (Description) for processing user entities' transactions throughout the period October 1, 2023 to September 30, 2024 for user entities of the system during some or all of the period October 1, 2023 to September 30, 2024, 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.

[Carved-out Unaffiliated Subservice Organization: Mrkter Technologies L.B.O Ltd uses a subservice organization to provide infrastructure management services**.** The Description includes only the control objectives and related controls of Mrkter Technologies L.B.O 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**.**

Complementary user entity controls: 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 Mrkter Technologies L.B.O 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 *Payouts Platform* system (System) made available to user entities of the System during some or all of the period October 1, 2023 to September 30, 2024, 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 communications (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 Payouts 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 October 1, 2023 to September 30, 2024, 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 Mrkter Technologies L.B.O Ltd's controls throughout the period October 1, 2023 to September 30, 2024. 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 effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved.

(3) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Leor Ceder
CEO

Shape the future with confidence

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 Mrkter Technologies L.B.O Ltd

Scope

We have examined Mrkter Technologies L.B.O Ltd's description entitled "Description of the Payouts.com Platform throughout the period October 1, 2023 to September 30, 2024" of its Payouts 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 Mrkter Technologies L.B.O Ltd management assertion (Assertion). The Control Objectives and controls included in the Description are those that management of Mrkter Technologies L.B.O 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.

Complementary user entity controls: The Description indicates that certain Control Objectives can be achieved only if complementary user entity controls assumed in the design of Mrkter Technologies L.B.O 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.

Carved-out Unaffiliated Subservice Organization: Mrkter Technologies L.B.O Ltd uses Amazon Web Services (AWS) to provide infrastructure management services. The Description includes only the Control Objectives and related controls of Mrkter Technologies L.B.O Ltd and excludes the control objectives and related controls of Amazon Web Services (AWS). The description also indicates that certain Control Objectives specified by Mrkter Technologies L.B.O Ltd can be achieved only if complementary subservice organization controls assumed in the design of Mrkter Technologies L.B.O Ltd's controls are suitably designed and operating effectively, along with the related controls at Mrkter Technologies L.B.O Ltd. Our examination did not extend to such complementary controls of Amazon Web Services (AWS), and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Mrkter Technologies L.B.O Ltd's responsabilités

Mrkter Technologies L.B.O Ltd has provided the accompanying assertion titled, Mrkter Technologies L.B.O 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. Mrkter Technologies L.B.O 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.

Shape the future with confidence

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 ("AICPA"). 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 October 1, 2023 to September 30, 2024. 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.

We are required to be independent of Mrkter Technologies L.B.O Ltd and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements related to our examination engagement 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

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 - Mrkter Technologies L.B.O Ltd's Control Objectives, controls and service auditor's tests of controls and results of tests (Description of Tests and Results).

Shape the future
with confidence

Opinion

In our opinion, in all material respects, based on the criteria described in Mrkter Technologies L.B.O Ltd's Assertion:

a. The Description fairly presents the System that was designed and implemented throughout the period October 1, 2023 to September 30, 2024.
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 October 1, 2023 to September 30, 2024, and the subservice organization and user entities applied the complementary controls assumed in the design of Mrkter Technologies L.B.O Ltd's controls throughout the period October 1, 2023 to September 30, 2024.
c. The controls operated effectively to provide reasonable assurance that the Control Objectives were achieved throughout the period October 1, 2023 to September 30, 2024, if complementary subservice organization and user entity controls assumed in the design of Mrkter Technologies L.B.O Ltd's controls operated effectively throughout the period October 1, 2023 to September 30, 2024.

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 Mrkter Technologies L.B.O Ltd, user entities of Mrkter Technologies L.B.O Ltd's System during some or all of the period October 1, 2023 to September 30, 2024, 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
March 31, 2025
Tel-Aviv, Israel

payouts.com

Section III – Description of the Payouts.com Platform throughout the period October 1, 2023 to September 30, 2024

Company Overview and Background

Mrkter Technologies L.B.O. Ltd., headquartered at 10 Hasadanot St. Hertzeliya, Israel, is specializing in automated payout solutions specifically engineered for the dynamic marketing industry. Mrkter's mission is to streamline and enhance financial operations through automation, simplifying the payout process for marketing vendors and addressing the intricate financial challenges inherent in the marketing sector. Leveraging a comprehensive global operational network, Mrkter delivers not only seamless integration with clients' existing systems—ensuring real-time data flow and financial accuracy—but also offers advanced payment services tailored to the needs of the industry.

Purpose and scope of the report

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

Types of Services Provided

Mrkter Technologies L.B.O. Ltd. offers the "Payouts.com Platform," an advanced Finance Operations solution aimed at streamlining marketing and financial operations. This platform is the primary service and the subject of the SOC 2 report.

Payouts.com Platform is designed to consolidate all the financial operations of a marketing team into a single, unified system. This includes budget management, vendor payments, cash flow projections, real-time financing, and more. Additionally, the platform also includes advanced banking capabilities.

One of the features is the advanced payment feature, which is facilitated by real-time data accessible through 600 connectors, allowing marketers to scale their operations without cash flow disruptions. Payouts.com MVP, developed in collaboration with leading, publicly listed companies, is an integral part of this service."

The scope of SOC 1 report covers all these services provided by the Payouts.com Platform adhering to the control objectives related to Logical Access, Change Management, Backup and DRP, Security and ELC.

The core features and services of the Mrkter Payouts.com Platform, are as follows:

Marketing Dashboard - provides a consolidated and comprehensive view of all marketing data, segmented by teams like Affiliation, PPC, Social, etc. It allows customers to understand their marketing activities and spending in real-time.

Payment Automation: The platform automates payments to all marketing vendors, including larger ones like Google and Facebook, and smaller affiliates. This streamlines cash flow and ensures consistent monthly payments.

Budget Management: The platform provides a dedicated tool for marketing teams, allowing both Finance and Marketing departments to maintain control over the budget. It includes alerts for potential overspending per team or source.

Advanced Payment Feature: The feature, facilitated by real-time data accessible through 600 connectors, allows affiliates to receive instant financing, enabling them to increase traffic without the constraint of Net 45/60 payment terms.

Banking Capabilities: Mrkter' s platform offers global accounts in 15 countries and 130 currencies, the ability to issue cards per employee or company purpose and acquiring services.

Data Integration and Management: With 600 connectors, payouts.com platform integrates with various data sources, providing valuable insights and enabling data-driven decision making.

Cash Flow Projections: The platform provides projections of the company's cash flow based on current marketing spend and budget, enabling better financial planning.

All these features are designed to work in a seamless, integrated manner, providing an all-in-one FinOps solution for customers' marketing needs.

Principal Service Commitments and System Requirements

Service commitments are declarations made by management to customers regarding the performance of the Platform. Commitments are communicated in Subscription and Services Agreements, Data Protection Agreements and the Terms of Service and Privacy Policy that are made available to customers, prospects and business partners on the Company's website.

System requirements are specifications regarding how the Platform should function to meet the Company's principal commitments to user entities. System requirements are specified in Mrkter's policies and procedures, which are available to all employees.

The Components of the System Used to Provide the Services

Mrkter Technologies L.B.O Ltd. designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Mrkter Technologies L.B.O Ltd makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Mrkter Technologies L.B.O Ltd. has established for the services. The system services are subject to the Security commitments established internally for its services.
At Mrkter, we are dedicated to maintaining clear, open, and consistent communication with customers. We communicate system and service commitments to customers in the following ways:

User Agreement and Policies: When a customer signs up for the platform, they are provided with a user agreement and Mrkter’ s policies which clearly outline the services customers will receive, company’s commitments to them, and their responsibilities as a user.

Onboarding and Training: During the customer onboarding process, Mrkter conduct training sessions which detail the use of the platform and commitments regarding each feature and service. The company also address any queries or concerns they might have about services.

Regular Updates and Notifications: Mrkter continuously keep customers informed about any changes or updates to the system or services through emails, in-app notifications, and newsletters. This includes updates on new features, maintenance schedules, and system improvements.

Customer Support: Mrkter’ s dedicated customer support team is available to assist with any questions or issues regarding the system or services. Customer support team provides timely, clear, and accurate information to customers to ensure their satisfaction and success with the platform.

Website and Marketing Material: Detailed information about the system, services, and commitments to users are also communicated through the website and marketing material. Mrkter makes sure that all the information is accurate and up to date to provide a clear understanding of what customers can expect. By consistently communicating system and service commitments, Mrkter aims to build trust with customers and provide them with a reliable, high-quality service.

BOUNDARIES OF THE SYSTEM

The boundaries of the primary offering of Mrkter Technologies L.B.O. Ltd. is a Finance Operations Platform, a comprehensive solution that aligns marketing and financial operations. This platform is the focal point of customer interaction and the core of product suite. Designed with an emphasis on efficiency and transparency, it incorporates different functionalities such as real-time budget management, streamlined payments to vendors, cash flow forecasting, and instant financing. These features are tailored to facilitate smooth financial operations for marketing teams. The Finance Operations Platform adheres strictly to SOC 2 standards, demonstrating commitment to data security and integrity. This platform is the cornerstone of Mrkter services and the embodiment of the mission to revolutionize financial operations within the marketing realm.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

Security commitments

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Up time availability of production systems

Components of the system

The System description is comprised of the following components:

- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

Mrkter Technologies L.B.O Ltd. maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description and owner. To outline the topology of its network, the organization maintains the following network diagram(s).

Hardware	Type	
AWS Elastic Compute Cloud (EC2)	AWS	Running application and infrastructure workloads
AWS Elastic Load Balancers	AWS	Load balance internal and external traffic
Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access
S3 Buckets	AWS	Storage, upload and download

Software: Mrkter Technologies L.B.O. Ltd is responsible for managing the development and operation of the primary offering of Mrkter Technologies L.B.O. Ltd. is advanced Finance Operations Platform, a comprehensive solution that aligns marketing and financial operations. The platform is the focal point of customer interaction and the core of product suite. Designed with an emphasis on efficiency and transparency, it incorporates sophisticated functionalities such as real-time budget management, streamlined payments to vendors, cash flow forecasting, and instant financing. These features are specifically tailored to facilitate smooth financial operations for marketing teams. The Payouts.com Platform adheres strictly to SOC 2 standards, demonstrating Mrkter commitment to data security and integrity. The platform is the cornerstone of services and the embodiment of Mrkter' s mission to revolutionize financial operations within the marketing realm. system including infrastructure components such as servers, databases, and storage systems. The in-scope Mrkter Technologies L.B.O Ltd. infrastructure and software components are shown in the table provided below:

System/Application	Operating System	Purpose
GuardDuty	AWS	Security application used for automated intrusion detection (IDS)
Amazon Web Services	AWS	Cloud provider user to host k8s cluster, LBs, build machines, etc.
GitHub	GitHub	Storing source code and code history, build pipelines
Google Workspace	Google Workspace	Used for emails communication
Vanta	Vanta	The organization compliance and security monitoring platform

Human Resources and Recruiting: The company employ dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Mrkter Technologies L.B.O Ltd has a staff of approximately 1 organized in the following functional areas:

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.
This includes:

- CEO
- CFO
- CTO
- CRO

Operations: Responsible for maintaining the availability of production infrastructure and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

Information Technology: Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

Data: Data as defined by Mrkter Technologies L.B.O Ltd, constitutes the following:

User and account data - includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Mrkter Technologies L.B.O Ltd has policies and procedures in place to proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

Control Environment

Integrity and Ethical Values - The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Mrkter Technologies L.B.O Ltd 's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Mrkter Technologies L.B.O Ltd 's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Board of Directors - The Board of Directors is composed of 3 members, which includes 1 director that is independent of management, who serve on behalf of the investors and provide organizational oversight to the Company. The role of the Board of Directors is to establish short-term and long-term strategic goals and objectives for the Company, as outlined in the Board of Directors' Charter, and is ultimately responsible for corporate governance. The Board of Directors holds annual meetings to review operating results, discuss business initiatives and oversee corporate governance and risks.

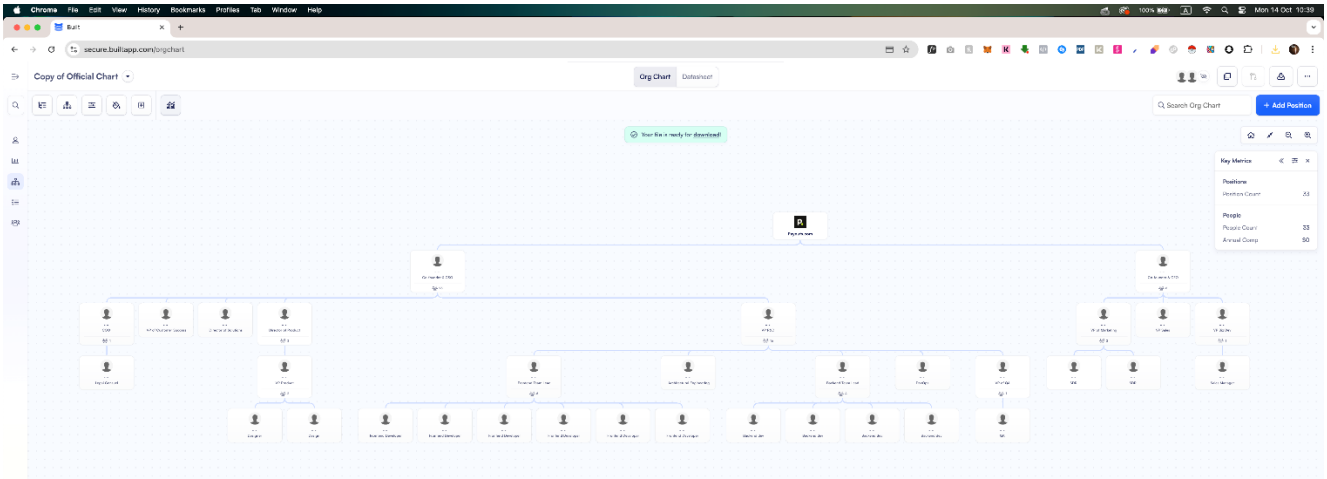
Organizational Structure

Mrkter Technologies L.B.O Ltd 's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Mrkter Technologies L.B.O Ltd 's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.



Commitment to competence - Mrkter Technologies L.B.O Ltd 's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style - The Mrkter Technologies L.B.O Ltd management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows customers entrust to us.

Authority and Responsibility - The management team meets frequently to be briefed on technology changes that impact the way Mrkter Technologies L.B.O Ltd. can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Mrkter Technologies L.B.O Ltd. to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the

management team to ensure they can be conducted in a way that is compatible with Mrkter's core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Human Resources Policy and Practices - Mrkter Technologies L.B.O Ltd 's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Mrkter Technologies L.B.O Ltd 's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

Control Activities

Mrkter's control activities are defined through its established policies and procedures. Policies are dictated through management of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Risk Assessment

Risk identification: Mrkter Technologies L.B.O Ltd.'s risk assessment process identifies and manages risks that could potentially affect Mrkter Technologies L.B.O Ltd.'s ability to provide reliable and secure services to customers. As part of this process Mrkter Technologies L.B.O Ltd maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Mrkter Technologies L.B.O Ltd. product development process so they can be dealt with predictably and iteratively.

***Risk assessment*:** The environment in which the system operates; the commitments, agreements, and responsibilities of Mrkter Technologies L.B.O Ltd.'s system; as well as the nature of the components of the system result in risks that the criteria will not be met. Mrkter Technologies L.B.O Ltd. addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Mrkter Technologies L.B.O Ltd.'s management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Risk Mitigation: Management identifies and assesses changes that could significantly impact the system of internal control. The risk identification process considers changes to the regulatory, economic, and physical environment in which the Company operates. The Company considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations, rapid growth, and new technologies on the system of internal control. Identified risks are analyzed through a process that includes estimating the potential significance of the risk. Mrkter' s risk assessment process includes considering how the risk should be managed and whether to accept, avoid, mitigate, or share the risk. Management determines mitigation strategies for the risks that have been identified and designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy. Security risks related to external parties (such as contractors and vendors) are identified and addressed based on the Company's vendor review process.

Mrkter considers the inherent risk of working with vendors and business partners as part of the annual risk assessment performed by the engineering team. Internal and external cyber threats and vulnerabilities are identified and assessed based on the likelihood that they could prevent the Company from achieving its objectives. Consideration is given to cyber threats and the vulnerabilities such relationships may present and whether the Company's controls reduce such risks to a level consistent with objectives and risk acceptance.

Communication and Information

Information and communication are an integral component of Mrkter Technologies L.B.O. Ltd.'s internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Mrkter Technologies L.B.O Ltd. uses several information and communication channels internally to share information with management, employees, contractors, and customers. Mrkter Technologies L.B.O. Ltd uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Mrkter Technologies L.B.O Ltd. uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

Monitoring

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Mrkter Technologies L.B.O Ltd.'s management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-going monitoring

Mrkter Technologies L.B.O Ltd.'s management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Mrkter Technologies L.B.O Ltd. 's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Mrkter Technologies L.B.O Ltd.'s personnel.

Reporting deficiencies

Mrkter's internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

- Changes to the system (Type 1) - No significant changes have occurred.
- Changes to the system (Type 2) - No significant changes have occurred.
- Incidents (Type 1) - No Incidents, not live yet.
- Incidents (Type 2) - No Incidents, not live yet.

Logical and Physical Access

A security policy is documented by Mrkter management, reviewed and approved on an annual basis by the management team. The security policy is available to Mrkter employees and reviewed annually within the compliance management platform, versioned documentation platform, and shared folders.

Access Control, User and Permissions Management

The System Access Control Policy establishes the access control requirements for requesting and provisioning user access to the system. The policy requires that access be denied by default, follow a least privilege principle, and be granted only upon business need. Each user account is unique and is identifiable to an individual user. Segregation of duties is established for critical functions within the environment to minimize the risk of unauthorized changes to production systems.

Mrkter Technologies L.B.O Ltd employs a structured access provisioning process to ensure secure and appropriate access to its systems. Domain account management requests are routed to designated asset owners or associated employees for approval, following established provisioning and de-provisioning procedures. Access is managed through individual user accounts added to domain security groups, with explicit approval required from security group owners for any access requests. Mrkter Technologies L.B.O Ltd. provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and reportable user provisioning and deprovisioning processes. Access to these systems is split into admin roles, user roles, and no access roles. User access and roles are reviewed on an annual basis to ensure least privilege access. Management is responsible for provision access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Mrkter Technologies L.B.O Ltd, completing security training. These steps must be completed within 14 days of hire.

Recertification of Access Permissions

Periodic reviews have been implemented to manage the appropriateness of access granted to information systems. Manual periodic reviews of individual accounts and security group memberships on assets are performed by authorized individuals, as appropriate, to evaluate whether access is still required. Remediation action is taken, as necessary, based on the review.

Policies and standards have been established and implemented to enforce appropriate user account password length and complexity. Personnel are required to follow the password standards established in the Information Security Program for all domains, as well as local user accounts for all assets.

Revocation Process

Employee status data is used to facilitate the provisioning and removal of user accounts in the System. Account management processes prevent the creation of an account for individuals that do not have valid HR records. Select users can request the removal of user accounts from the System. In addition, system owners can directly remove users from security groups. Upon termination, employees are required to return their keys and devices to Mrkter. When an employee is terminated, management is responsible for deprovisioning access to all in scope systems within 3 days for that employee's termination.

Production Environment Logical Access

Access to the production environment is controlled through a designated set of access points and restricted to authorized individuals. Users are authenticated to access points using domain credentials depending on where the production assets are located. Passwords, along with two factor authentication used to access network devices, are restricted to authorized individuals and system processes based on job responsibilities.

Information System's Inventory

The Company maintains an inventory of information systems. All such assets are assigned ownership by a designated department or team within Mrkter Technologies L.B.O Ltd. and prioritized based on the asset's business value and criticality to the Company. The classification process is owned by the engineering team. Information and data assets are subject to the Data Management Policy that defines parameters for the ownership, classification, security, storage, and retention of data. Software and hardware assets are subject to the Asset Management Policy and Third-Party Management Policy that defines parameters for the acquisition, development, maintenance, security, and disposal of information system assets.

Physical security

Mrkter Technologies L.B.O Ltd.'s production servers are maintained by AWS. The physical and environmental security protections are the responsibility of AWS. Mrkter Technologies L.B.O Ltd. reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

Software Development Lifecycle (SDLC) Overview

Mrkter Technologies L.B.O Ltd. maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is

logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Production Monitoring

At Mrkter, a comprehensive vulnerability management process is in place to ensure the security and reliability of systems. Vulnerability process is divided into next steps:

Regular Vulnerability Scans: Mrkter conducts automated vulnerability scans of systems on a weekly basis. These scans help to identify potential security weaknesses in networks, applications, and systems.

External Assessments: In addition to internal scans, we also engage third-party cybersecurity firms to conduct an annual penetration test. This independent assessment provides with an unbiased review of security posture and helps uncover potential vulnerabilities that could be missed in internal scans.

Patch Management: After vulnerabilities are identified, they are prioritized based on the risk they pose. Critical vulnerabilities are patched immediately, while other less severe vulnerabilities are scheduled for patching in accordance with their risk level. All patches are tested in a controlled environment before deployment to ensure they do not disrupt services.

Security Incident and Event Management (SIEM): Mrkter utilizes SIEM tools to monitor and analyze activity across the network in real-time. This helps in the early detection of potential security incidents and suspicious activities.

Threat Intelligence: Mrkter subscribe to industry-leading threat intelligence feeds to stay informed about the latest vulnerabilities and threats in the cybersecurity landscape. This information is used to enhance security measures and preemptively protect against emerging threats.

This rigorous approach ensures that we identify and address vulnerabilities in a timely and efficient manner, thereby reducing the risk of security incidents.

Security

Incident Management

Mrkter Technologies L.B.O Ltd. maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting and acting upon breaches or other incidents.

Mrkter Technologies L.B.O Ltd. internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Mrkter Technologies L.B.O Ltd. utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

Data Encryption

Data in transit:
Mrkter utilizes an ALB to manage incoming traffic, which acts as a termination point for TLS connections. This ensures that all data exchanged between clients and services is encrypted during transmission.

The TLS configuration on load balancer adheres to best practices and industry standards to ensure the security and integrity of data in transit. This includes the use of strong cryptographic algorithms and key lengths, as well as regular updates and patching to mitigate any vulnerabilities.

The communication to RDS also employs TLS for encryption. This ensures that all data transmitted between the application servers and the RDS instance is encrypted, further enhancing the security of data in transit. The TLS configuration for RDS is configured to meet best practices and industry standards, including the use of strong cryptographic algorithms and regular updates to maintain security.

Data at rest:
Mrkter' s data is stored in Amazon S3 and Amazon RDS and encrypted using industry-standard encryption algorithms. In Amazon S3, data is encrypted using the AES-256 algorithm. This ensures that all objects stored in S3 are encrypted at rest, providing an additional layer of security for our data.

Similarly, in Amazon RDS, data is encrypted using the same AES-256 algorithm. This means that all data stored in RDS instances, including databases and backups, is encrypted at rest. This encryption helps protect the data from unauthorized access and ensures its confidentiality and integrity.

To manage the encryption keys securely, Mrkter uses AWS KMS They. KMS allows to create and control encryption keys used to encrypt data in S3 and RDS. By using KMS, Mrkter can enforce access controls, audit encryption key usage, and rotate encryption keys regularly, further enhancing the security of Mrkter's data.

Backup and DRP

Database Backup

Backup infrastructure is maintained in AWS with physical access restricted according to the policies. Backups are fully backed up daily, encrypted, with access restricted to key personnel. The backup system automatically generates a backup log. In case of failure, a notification is sent to the Engineering team. Replicas are used to achieve high availability in case of a disaster.

Amazon RDS instance is configured with automatic daily snapshots to ensure the availability and durability of Mrkter' s data. These snapshots are taken automatically and can be used to restore database to a specific point in time. Additionally, RDS instance is deployed in a multi-AZ configuration for high availability. This means that database is replicated synchronously across multiple AZs within the same AWS Region. In the event of a hardware failure or AZ outage, RDS instance can failover to a standby instance in another AZ, minimizing downtime and ensuring continuous availability of the database.

Business Continuity Plan (BCP)

Mrkter Technologies L.B.O Ltd. maintains a Business Continuity and Disaster Recovery (BC/DR) Plan designed to support the continuity of critical business functions and minimize downtime in the event of a disruption. The plan outlines procedures for maintaining operations during incidents and restoring services in a timely manner.

Mrkter maintains infrastructure and platform-level backups that support system recovery and data restoration capabilities. These backups are taken regularly and retained in accordance with internal data retention policies. Restoration procedures are documented and designed to enable recovery of essential systems and services.

While formal disaster recovery testing is not currently conducted, the organization has the capability to restore critical systems and data based on predefined recovery steps. This capability is supported by cloud-based infrastructure, automated backup processes, and role-based access to restoration tools.

Mrkter continuously reviews and updates its BC/DR documentation to reflect changes in systems, personnel, and business needs, ensuring preparedness and alignment with evolving risks and operational priorities.

Report Use

The Description does not omit or distort information relevant to the Platform while acknowledging that the Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

Subservice organizations

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

Subservice description of services

The Cloud Hosting Services provided by AWS support the physical infrastructure of the entities services.

Complementary Subservice Organization Controls

Mrkter Technologies L.B.O Ltd.'s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the control objectives related to Mrkter Technologies L.B.O Ltd.'s services to be solely achieved by Mrkter Technologies L.B.O Ltd control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Mrkter Technologies L.B.O Ltd.

The following subservice organization controls have been implemented by AWS and included in this report to provide additional assurance that the control objectives are met.

Category	Applicable Control Objective	Complementary Subservice Organization Controls
Logical Access	4.2	Physical access to data centers is approved by an authorized individual.
Logical Access	4.4	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.

Category	Applicable Control Objective	Complementary Subservice Organization Controls
Logical Access	4.3	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
Logical Access	4.11	Closed circuit television camera (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
Logical Access	4.6	Access to server locations is managed by electronic access control devices.
Security	5.9	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.
ELC	3.10	AWS has a process in place to review environmental and geo-political risks before launching a new region.
Logical Access	4.6	Amazon-owned data centers are protected by fire detection and suppression systems.
Logical Access	4.6	Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
Logical Access	4.6	Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon owned data centers
Logical Access	4.6	Amazon-owned data centers have generators to provide backup power in case of electrical failure.
Logical Access	4.6	Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.

The Company also utilizes other, less significant, third-party service organizations to support its services. These organizations are generally referred to as vendors.

Mrkter Technologies L.B.O Ltd management, along with the subservice provider, define the scope and responsibility of the controls necessary to meet all the relevant control objectives through written contracts, such as service level agreements. In addition, Mrkter Technologies L.B.O Ltd performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- Making regular site visits to vendor and subservice organization(s') facilities
- Testing controls performed by vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)

- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Complementary User Entity Controls (CUECs)

Mrkter Technologies L.B.O Ltd.'s services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the control objectives related to Mrkter Technologies L.B.O Ltd's services to be solely achieved by Mrkter Technologies L.B.O Ltd control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Mrkter Technologies L.B.O Ltd.'s.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the control objectives described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

Number	Control Objective	User Entities Control Description
1	ELC	User entities are responsible for understanding and complying with their contractual obligations to Mrkter Technologies L.B.O Ltd.
2	ELC	User entities are responsible for notifying Mrkter Technologies L.B.O Ltd. of changes made to technical or administrative contact information.
3	ELC	User entities are responsible for maintaining their own system(s) of record.
4	Change Management	User entities are responsible for ensuring the supervision, management, and control of the use of Mrkter Technologies L.B.O Ltd. services by their personnel.
5	Backup and DRP	User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Mrkter Technologies L.B.O Ltd. services.
6	Logical Access	User entities are responsible for providing Mrkter Technologies L.B.O Ltd. with a list of approvers for security and system configuration changes for data transmission.
7	Security	User entities are responsible for immediately notifying Mrkter Technologies L.B.O Ltd. of any actual or suspected information security breaches, including compromised

		user accounts, including those used for integrations and secure file transfers.

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 Mrkter, KFGK considered the aspects of the Mrkter 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.

Control Objective #1 - Backup and DRP

Controls provide reasonable assurance that data is backed up regularly and available for restoration in the event of processing errors and/or unexpected processing interruptions.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1.1	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the operations security policy and determined that Company's data backup policy had documented requirements for backup and recovery of customer data.	No deviations noted.
1.2	The company has Business Continuity and Disaster Recovery Plan in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the business continuity and disaster recovery plan and determined that company had Business Continuity and Disaster Recovery Plan in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	No deviations noted.
1.3	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected load balancers test from monitoring compliance tool and determined that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met.	No deviations noted.
1.4	The company performs periodic backups for production data. Data is backed up to a different location than the production system.	Inspected RDS backup configuration from AWS and determined that Mrkter performed periodic backups for production data. Data was backed up to a different location than the production system.	No deviations noted.
1.5	The company has a multi-location strategy for production environments employed to permit the resumption of operations at other company data centers in the event of loss of a facility.	Inspected the configuration from cloud provider and determined that Mrkter had a multi-location strategy for production environments employed to permit the resumption of operations at other company data centers in the event of loss of a facility.	No deviations noted.

Control Objective #2 – Change Management

Controls provide reasonable assurance that the organization has established and maintains a change management process that effectively identifies, manages, and controls changes to IT systems, applications, infrastructure, and procedures.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2.1	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. The company use a tool to manage and prioritize changes.	Inspected the change management tickets for a sample of commits and determined that changes to the software and infrastructure were authorized and formally documented before implemented in the production environment. Inspected the test pipeline for a sample of commits and determined that changes to the software were tested prior to being implemented in the production environment. Inspected the merge request for a sample of commits and determined that changes to the software and infrastructure were reviewed and approved before implemented in the production environment.	**Deviations noted:** Inspected a sample of changes during the audit period. 8 of 25 sample commits did not have documented test evidence and 1 of 25 of sample commits did not have code review or approval. **Management Response:** The company recognizes the importance of maintaining a robust change management process. We are reinforcing our change control framework by implementing stricter validation checks within our change management tool to ensure test evidence and approvals are documented before deployment. Additionally, we are increasing training efforts for development teams to emphasize compliance with change management policies. Regular audits will be conducted to ensure adherence, and non-compliance trends will be escalated for corrective action.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2.2	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the System development life cycle (SDLC) policy document and determined that Company had a formal systems development life cycle (SDLC) methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No deviations noted.

Control Objective #3 – ELC

Mrkter implements controls to support the overall control environment, including governance, risk management and communication processes.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
3.1	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the Board Charter official documentation and determined that Company had documented charter that outlined its oversight responsibilities for internal control.	No deviations noted.
3.2	The company's board of directors meets at least annually and maintains formal meeting minutes.	Inspected the board meeting minutes and determined that Mrkter's board of directors met at least annually and maintained formal meeting minutes.	No deviations noted.
3.3	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected the code of conduct acknowledgement evidence for a sample of new contractors and determined that Mrkter required contractors to acknowledge a code of conduct at the time of hire.	**Deviations noted:** 2 of 5 sample employees showed that policies were not accepted or acknowledge by contractors on the compliance platform **Management Response:** The company is committed to ensuring that all contractors acknowledge and adhere to our Code of Conduct. We are enhancing our onboarding procedures by enforcing automated tracking within our compliance platform to verify acknowledgment before contractors can commence work. Additionally, reminders and escalations will be implemented for pending acknowledgments to ensure full compliance.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
3.4	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the code of conduct acknowledgement evidence for a sample new employees and determined that Mrkter required employees to acknowledge a code of conduct at the time of hire. Inspected the Mrkter's code of conduct and determined that policy was established where employees who violate the code of conduct were subject to disciplinary actions in accordance with a disciplinary policy. No violation occurred during the audit period.	**Deviations noted:** 5 of 5 sample employees showed that policies were not accepted or acknowledge by employees on the compliance platform **Management Response:** The company is committed to ensuring that all employees acknowledge and adhere to our Code of Conduct. We are enhancing our onboarding procedures by enforcing automated tracking within our compliance platform to verify acknowledgment before employees can commence work. Additionally, reminders and escalations will be implemented for pending acknowledgments to ensure full compliance.
3.5	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected the confidentiality agreement for a sample of contractors and determined that contractors needed to sign a confidentiality agreement during onboarding.	**Deviations noted:** 1 of 5 sample contractor did not have a signed NDA or confidentiality agreement. **Management Response:** The company takes confidentiality obligations seriously and is enhancing its contractor onboarding process to ensure NDAs/confidentiality

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
			agreements are signed without exception. Going forward, we will implement a system-driven control that prevents engagement until the agreement is signed. Additionally, periodic compliance audits will be conducted to validate adherence, and any gaps identified will be promptly remediated.
3.6	The company requires employees to sign a confidentiality agreement during onboarding.	Inspected the confidentiality agreement of an employee and determined that employees signed a confidentiality agreement during onboarding.	No deviations noted.
3.7	The company performs reference checks on new employees.	Inspected the reference check evidence of new employees and determined that Mrkter performed reference checks on new employees.	No deviations noted.
3.8	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the risk assessment objectives and determined that Company specified its objectives in order to identify and assess risk associated with the objectives.	No deviations noted.
3.9	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy and determined that Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No deviations noted.
3.10	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified	Inspected the risk assessment exercise and determined that Mrkter's risk assessments were performed at least annually.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment exercise and determined that the risk assessment process, threats and changes (environmental, regulatory, and technological) to service commitments were identified and the risks were formally assessed. Inspected the risk assessment exercise and determined that the risk assessment included a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	
3.11	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the third-party management policy and determined that Company had a vendor management program in place. Components of the program included: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	No deviations noted.

Control Objective #4 – Logical Access

Logical access to programs, data, and computer resources relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4.1	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the access control policy document and determine that Mrkter's the policy documented the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	No deviations noted.
4.2	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the access request evidence for a sample of new employees and determined that user access to in-scope system components was based on job role and function or required a documented access request form and manager approval prior to access being provisioned.	**Deviations noted:** Inspected 4 samples of access requests of new users during the audit period. 1 of 4 new users samples access did not have evidence of access request and approvals **Management Response:** Mrkter acknowledges the exception noted during the audit related to missing documentation for one new user's access request and approval. This deviation was the result of a process oversight during a period of organizational growth and onboarding volume.
4.3	The company conducts access reviews at least semi-annually for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the user access review documentation and determined that company conducted access review at least semi-annually for the in-scope system components to ensure that access was restricted appropriately.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4.4	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the information security policy and determined that the company had a process to ensure that access was revoked for terminated employees within SLAs.	**Deviations noted:** Inspected 5 samples of terminated employees during the audit period. 4 of 5 terminated samples access deactivation were not done timely over the span of months. **Management Response:** The company acknowledges the identified gaps in timely access deactivation for terminated employees. We are enhancing our termination checklist process by automating access revocation through our identity and access management (IAM) system. Additionally, we are reinforcing monitoring controls to ensure compliance with service-level agreements (SLAs) and conducting periodic reviews to validate timely execution. Training sessions will also be provided to relevant teams to reinforce best practices and accountability
4.5	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the password policy and determined that passwords were required for in-scope system components to be configured. Inspected the authentication configuration test from	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		monitoring compliance tool and determined that passwords were required for in-scope system components to be configured according to Company's policy.	
4.6	The company has processes in place for granting, changing, and terminating physical access to company offices based on an authorization from control owners.	Inspected the physical security policy and determined that company had processes in place for granting, changing, and terminating physical access to Mrkter's offices based on an authorization from control owners.	No deviations noted.
4.7	The company restricts privileged access to databases to authorized users with a business need.	Inspected the list of users with privileged access to databases and their job titles and determined that Mrkter restricted privileged access to the application to authorized users with a business need.	No deviations noted.
4.8	The company restricts access to migrate changes to production to authorized personnel.	Inspected the list of users with access to migrate changes to production and their job titles and determined that Company restricted access to migrate changes to authorized personnel.	No deviations noted.
4.9	The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to system and determined that Mrkter required authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	No deviations noted.
4.10.	The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.	Inspected the company's authentication to the production datastores and determined that Mrkter required authentication to production datastores to use authorized secure authentication mechanisms using unique SSH key.	No deviations noted.
4.11	The company requires visitors to sign-in, wear a visitor badge, and be escorted by an authorized employee when accessing the data center or secure areas.	Inspected the physical access policy and determined that visitors were required to sign-in, wear a visitor badge, and be escorted by an authorized employee when accessing the data center or secure areas.	No deviations noted.

Control Objective #5 – Security

The entity has processes in place to establish and monitor the different security operations to protect information security assets and environment

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
5.1	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected SSL/TLS encryption configuration test from monitoring compliance tool and determined that Mrkter used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No deviations noted.
5.2	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the cryptography policy document and determined that Mrkter restricted privileged access to encryption keys to authorized users with a business need. Inspected the list of users and their job titles and determined that Mrkter reviewed and restricted privileged access to encryption keys to authorized users with a business need.	No deviations noted.
5.3	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the incident response policy and determined that Mrkter's security and privacy incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. No security incidents occurred during the audit period.	No deviations noted.
5.4	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the incident response policy and determined that Mrkter had security and privacy incident response policies and procedures that were documented and communicated to authorized users.	No deviations noted.
5.5	The company utilizes a log management tool to identify events that may have a potential impact on	Inspected the logs from the compliance monitoring tool and determined that log management tool was utilized	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	the company's ability to achieve its security objectives.	to identify events that may have a potential impact on Mrkter's ability to achieve its security objectives.	
5.6	The company use security groups and configures them to prevent unauthorized access.	Inspected the security groups test from monitoring compliance tool and determined that Mrkter used security groups and configured them to prevent unauthorized access.	No deviations noted.
5.7	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration test report and determined that the company's penetration testing was performed at least annually. A remediation plan was developed and changes were implemented to remediate vulnerabilities in accordance with SLAs. Inspected the results of the penetration test and determined that high issues were remediated in accordance with SLA's.	No deviations noted.
5.8	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the roles and responsibilities policy.	Inspected information security roles and responsibilities policy and an example of job description and determined that roles and responsibilities of the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions or the roles and responsibilities policy.	No deviations noted.
5.9	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the information security policy and determined that Mrkter's information security policies and procedures were documented and reviewed at least annually.	No deviations noted.
5.10	Host-based vulnerability scans are performed continuously on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the integration with GitHub in the compliance monitoring tool and GuardDuty dashboard for vulnerability scanning and determined that host-based	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		vulnerability scans were performed continuously on external-facing systems. Inspected the outstanding vulnerabilities based on the scanning performed and determined that high and critical vulnerabilities were tracked to remediation.	

****