System and Organization Controls Report (SOC 1® Type 2)

Report on Deal Engine, Inc.'s Description of Its Automated Refunds and Changes Platform and on the Suitability of the Design and Operating Effectiveness of Its Controls Throughout the Period January 1, 2025, to September 30, 2025
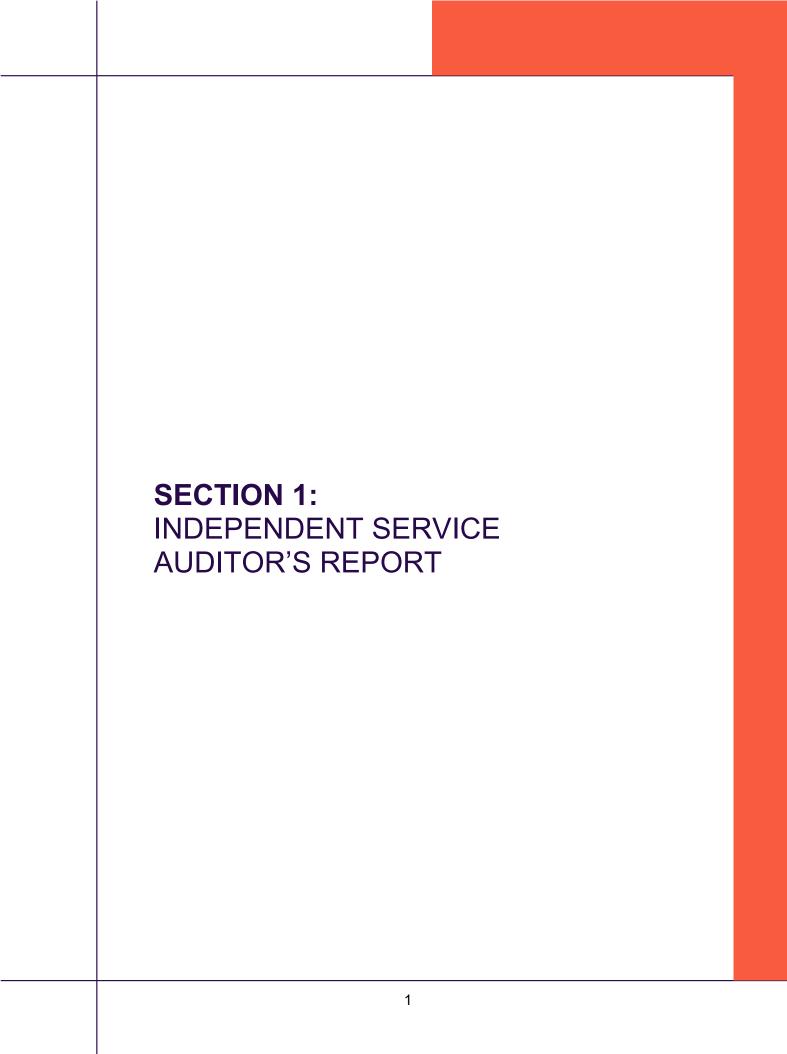

+1 877.607.7727

www.InsightAssurance.com

TABLE OF CONTENTS

SECTION 1:
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Deal Engine, Inc.

Scope

We have examined Deal Engine, Inc.'s ('Deal Engine' or 'the Service Organization') accompanying description of its Automated Refunds and Changes Platform found in Section 3 titled "Deal Engine, Inc.'s Description of Its Automated Refunds and Changes Platform" (description) for processing user entity transactions throughout the period January 1, 2025, to September 30, 2025 and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Deal Engine, Inc.'s Management Assertion" (assertion). The controls and control objectives included in the description are those that management of Deal Engine believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Automated Refunds and Changes Platform for processing user entity transactions that are not likely to be relevant to user entities' internal control over financial reporting.

Deal Engine uses Amazon Web Services (AWS) and Google Cloud Platform (GCP) to provide hosting services and management of Deal Engine's network and IT-managed services. The description includes only the control objectives and related controls of Deal Engine and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by Deal Engine can be achieved only if complementary subservice organization controls assumed in the design of Deal Engine's controls are suitably designed and operating effectively, along with the related controls at Deal Engine. Our examination did not extend to controls of the subservice organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Deal Engine's controls are suitably designed and operating effectively, along with related controls at Deal Engine. 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.

The information included in Section 5, "Other Information Provided by Deal Engine, Inc." is presented by management of Deal Engine to provide additional information and is not a part of Deal Engine's description of its Automated Refunds and Changes Platform made available to user entities during the period January 1, 2025, to September 30, 2025. Information about Deal Engine's responses to identified exceptions has not been subjected to the procedures applied in the examination of the description of the Automated Refunds and Changes Platform and of the suitability of the design and operating effectiveness of controls to achieve the related control

objectives stated in the description of the Automated Refunds and Changes Platform and, accordingly, we express no opinion on it.

Service Organization's Responsibilities

In Section 2 of this report, Deal Engine has provided an assertion about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Deal Engine is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; selecting the criteria stated in the assertion; and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

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

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period January 1, 2025, to September 30, 2025. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.

- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.

- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.

- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 Section 4.

Opinion

In our opinion, in all material respects, based on the criteria described in management of Deal Engine's assertion:

- The description fairly presents the Automated Refunds and Changes Platform that was designed and implemented throughout the period January 1, 2025, to September 30, 2025.

- The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 2025, to September 30, 2025 and the subservice organizations and user entities applied the complementary controls assumed in the design of Deal Engine's controls throughout the period January 1, 2025, to September 30, 2025.

- The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period January 1, 2025, to September 30, 2025 if complementary subservice organization and user entities controls assumed in the design of Deal Engine's controls operated effectively throughout the period January 1, 2025, to September 30, 2025.
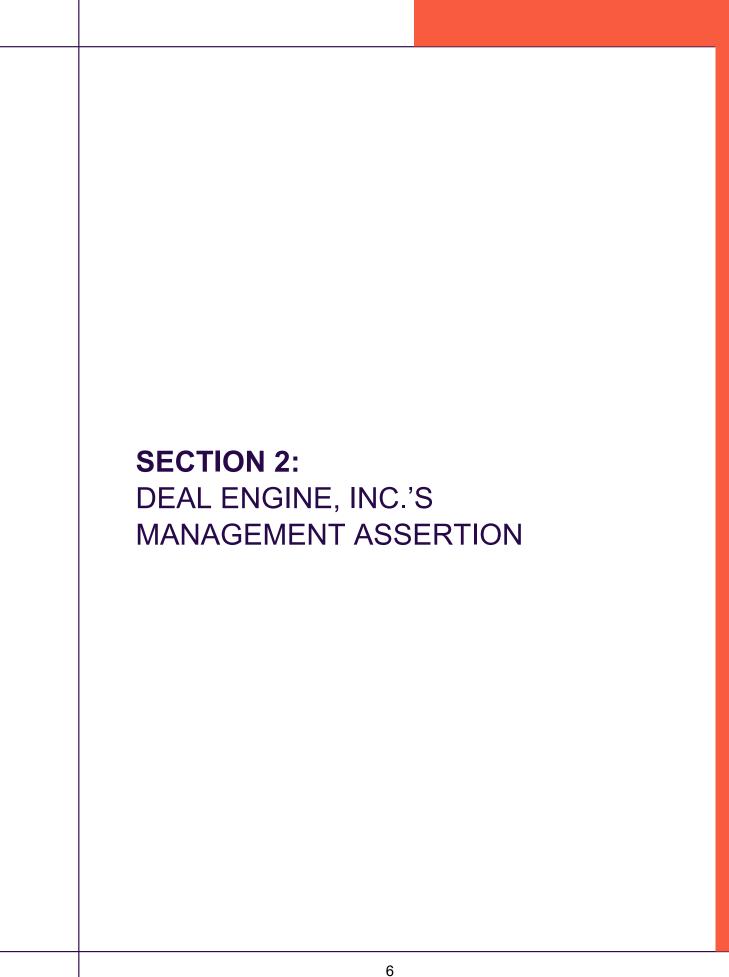
Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Deal Engine; user entities of Deal Engine's system during some or all of the period January 1, 2025, to September 30, 2025; and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Insight Compliance LLC

dba Insight Assurance
Tampa, Florida
December 10, 2025

SECTION 2:
DEAL ENGINE, INC.'S
MANAGEMENT ASSERTION

Deal Engine

DEAL ENGINE, INC.'S MANAGEMENT ASSERTION

We have prepared the description of Deal Engine, Inc.'s ('Deal Engine') Automated Refunds and Changes Platform for processing user entities' transactions throughout the period January 1, 2025, to September 30, 2025 (description), for user entities of the Automated Refunds and Changes Platform during some or all of the period January 1, 2025, to September 30, 2025, 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 the subservice organizations and user entities of the Automated Refunds and Changes Platform themselves when assessing the risks of material misstatement of the user entities' financial statements.

Deal Engine uses Amazon Web Services (AWS) and Google Cloud Platform (GCP) to provide hosting services and management of Deal Engine's network and IT-managed services. The description includes only the control objectives and related controls of Deal Engine and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by Deal Engine can be achieved only if the complementary subservice organization controls assumed in the design of Deal Engine are suitably designed and operating effectively, along with the related controls at Deal Engine. The description does not extend to controls of the subservice organizations.
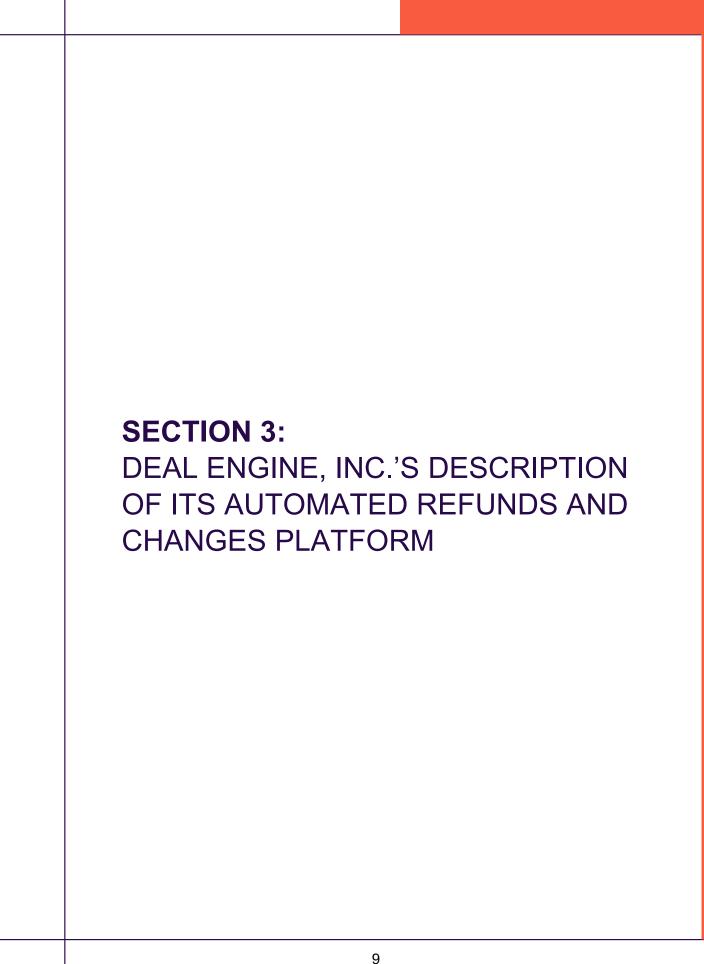
The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Deal Engine's controls are suitably designed and operating effectively, along with related controls at Deal Engine. The description does not extend to the controls of the user entities.

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

1) The description fairly presents Deal Engine's Automated Refunds and Changes Platform made available to user entities of the system during some or all of the period January 1, 2025, to September 30, 2025 for processing user entities' transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

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

        i)   The types of services provided including, as appropriate, the classes of transactions processed.

        ii) 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.

        iii) The information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

iv) How the system captures and addresses significant events and conditions other than transactions.

v) The process used to prepare reports and other information for user entities.

vi) Services performed by subservice organizations, if any, including whether the inclusive or the carve out method has been used in relation to them.

vii) 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 controls.

viii) Other aspects of our control environment, risk assessment process, information and communications, control activities, and monitoring activities that are relevant to the services provided.

b) Includes relevant details of changes to Deal Engine's Automated Refunds and Changes Platform during the period covered by the description.

c) 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 and their user auditors and may not, therefore, include every aspect of Deal Engine's Automated Refunds and Changes Platform that each individual user entity of the Automated Refunds and Changes Platform and its user auditor may consider important in its own particular environment.

2) The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period January 1, 2025, to September 30, 2025, to achieve those control objectives if the subservice organizations and user entities applied the complementary controls assumed in the design of Deal Engine's controls throughout the period January 1, 2025, to September 30, 2025. The criteria we used in making this assertion were that:

a) The risks that threaten the achievement of the control objectives stated in the description have been identified by management of Deal Engine.

b) 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.

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

Deal Engine, Inc.
December 10, 2025

SECTION 3:
DEAL ENGINE, INC.'S DESCRIPTION OF ITS AUTOMATED REFUNDS AND CHANGES PLATFORM

DEAL ENGINE, INC.'S DESCRIPTION OF ITS AUTOMATED REFUNDS AND CHANGES PLATFORM

Company Background

Deal Engine, Inc. ("Deal Engine," "the Service Organization," or "the Company") was founded on March 30, 2017, by Alexandro Jara ex-McKinsey to provide Software-as-a-Service in the airline refund industry. The organization is based out of Miami, Florida, with additional sites in Mexico City.

Description of Services Provided

Automated Refunds and Changes Platform is an online platform (or API) that enables automatic quoting, processing, and tracking of large quantities of refunds from one place in real time. The Automated Refunds and Changes Platform reduces costs and improves travelers' experience by improving operational efficiency immediately. The platform provides reporting via API and digital dashboards. The platform receives all refund requests in three ways:

- Refund quote generation: our A.I. algorithms calculate the exact refund amount, reading and interpreting the ticket's fare and tax rules.

- Refund request validation: refund requests are validated by an agent or traveler before being automatically processed through BSP, ARC, or GDS.

- Refund confirmation: refund request is processed and informed on the client user interface.

Boundaries of the System

This description details the Automated Refunds and Changes Platform and the related control objectives, policies, procedures, and control activities for the Automated Refunds and Changes Platform. This description does not include any other services and does not include the control objectives, policies, procedures, and control activities at any subservice organizations.

CONTRACT MANAGEMENT CONTROL

The Company's system provides services through a combination of automated and manual procedures. Transactions are initiated when the Legal Manager prepares and submits a draft contract to the client for review, and are authorized once contract terms are reviewed, negotiated, and approved by the Legal Manager in accordance with the Company's established liability thresholds and approval guidelines.

Once authorized, transactions are recorded by generating the final contract document and uploading it into the Company's document-management environment, and are processed through issuance of the finalized contract to all required parties via DocuSign for electronic signature in accordance with established procedures.

If exceptions or errors are identified, they are corrected through contract adjustment procedures, including documented negotiation updates, Legal Manager review, and supervisory approval where required before final processing. Processed transactions and relevant information are then

transferred into the client's designated contract folder, ensuring accuracy, completeness, and consistency with contractual requirements.

Transaction Flow

1. **Contract Initiation –** Legal Manager drafts and sends the contract to the client.
2. **Client Review & Negotiation –** Client provides feedback; Legal Manager negotiates within predefined liability and contractual boundaries.
3. **Internal Authorization –** Legal Manager confirms alignment with company liability standards and approves the final version.
4. **Contract Execution –** Final contract is issued to all signatories through DocuSign for electronic signature.
5. **Recording & Storage –** Fully executed contract is automatically returned from DocuSign and stored in the client's designated folder.
6. **Completion –** Legal phase is marked as complete once the contract is stored and all required parties have signed.

CLIENT CREDENTIAL INTEGRATION

The Company relies on information from both internal and external sources to perform its processing procedures. This information includes client-provided credentials, API keys, SFTP access details, airline/agency portal credentials, and supporting configuration documentation shared by user entities, which may be maintained in either automatic or manual formats.

The information is used to support the full transaction cycle, including initiation, authorization, recording, processing, and reporting. Data is captured and stored in the Firestore Database, secure credential vaults, integrations microservices, and internal workflow platforms and is subject to established validation checks to ensure accuracy and completeness.

When incorrect or incomplete information is identified, it is addressed through integration review procedures, and supervisory validation performed by the Integrations and Operations teams. Additionally, a gradual credential-management update process is followed to ensure that all client credentials remain current and accurate. Once corrected, the updated information is reprocessed and incorporated into the alerts, systems, credential-validation processes, and other deliverables prepared for user entities. This process helps ensure that the information provided to user entities is reliable and consistent with contractual requirements.

INVOICING SETUP

In addition to routine transaction processing, the Company's system captures and addresses significant events and conditions that may affect reporting and services. Such events may include the establishment of client-specific billing rules, reimbursement and refund conditions, eligible fare types, route-based fee structures, PNR-level requirements, and any operational specifications defined during the initial invoicing configuration.

These events are identified through the client onboarding process, the review of contract documents (e.g., Master Service Agreements (MSAs), Service Level Agreements (SLAs), pricing schedules), validation of ticket-processing requirements, and coordination between the Finance

and Operations teams to ensure that all invoicing parameters are correctly captured at setup. Once identified, they are addressed by configuring billing rules in the invoicing module, enabling reimbursement logic, defining applicable routes and fare conditions, setting up PNR-based processing rules, and documenting all parameters for future reference.

Corrections and adjustments arising from these events are documented and incorporated into the reporting process to ensure that reports and information provided to user entities remain accurate, complete, and consistent with service commitments.

INVOICING MONITORING

Reports and other information for user entities are prepared using data collected from multiple sources, including transaction-processing systems, industry system data, client invoicing configurations, internal Deal Engine databases, and operational billing databases. This information is compiled and formatted through a combination of automated report-generation tools, data extraction from the billing platform, and review performed by the Finance and Operations teams.

Prior to delivery, reports are subject to reconciliations between invoicing setups and contractual terms, exception reporting from system-generated alerts, and supervisory review performed during the monthly dry-run validation. to confirm completeness and accuracy. Once validated, reports are distributed to user entities through secure channels, including encrypted email or shared client portals.

These procedures are designed to ensure that user entities receive information that is accurate, complete, and consistent with the service organization's contractual and operational commitments.

CLIENT DATA

Client data used for billing and operational processes is collected from industry systems, the Deal Engine platform, internal databases, and operational billing repositories. This information includes billing contacts, incorporation data, credential information, and configuration details. The Finance team validates client billing data quarterly by comparing information stored in the internal database with client-provided documentation or formal change requests.

Prior to use in invoicing or reporting, client data is subject to system-enforced data quality checks, monthly sanity validations, and supervisory review to confirm accuracy and completeness. Once validated, updated client records are maintained in Deal Engine's internal systems to support downstream billing, reporting, and operational processes.

OPERATIONS MONITORING

Operational monitoring activities use data from system logs, automated industry integrations, processing systems, and internal operational databases. The Operations team performs monthly system health checks, reviews performance metrics, and evaluates alerting signals generated by automated monitoring tools.

Identified issues—such as service delays, ticket-processing anomalies, or availability degradations—are escalated through established workflows and validated by supervisory

personnel to ensure appropriate resolution. Monitoring outputs are documented and retained to support operational stability and service-level commitments.

These procedures ensure continuous oversight of system availability, performance, and service quality.

MONTHLY INVOICING

Monthly invoicing activities rely on data sourced from transaction-processing systems, client invoicing configurations, internal Deal Engine databases, operational billing data, and Finance reconciliation records. These inputs are consolidated using automated report-generation tools, billing-platform extractions, and manual checks performed by the Finance team.

Before invoice issuance, data undergoes monthly validation procedures, including reconciliation of invoicing data across systems, supervisory verification of client adjustments, and automated validation controls within the billing platform. Once validated, invoices are generated according to established billing cycles and sent to customers via email.

These procedures help ensure that invoices are accurate, complete, and aligned with contractual billing terms.

ACCOUNTS RECEIVABLE COLLECTION

Accounts receivable information is compiled from the financial system, bank statements, Deal Engine internal records, and operational billing databases. The Finance team uses this information to assess collection performance, measure key metrics, and identify overdue balances.

Prior to reporting, the Finance team performs monthly reconciliations between payments recorded in financial software and corresponding bank transactions to confirm accuracy. Delinquent accounts follow an established escalation protocol, with reviews conducted at least monthly.

These procedures ensure that collection activities are timely, accurate, and fully documented.

FINANCE PROCESS

Finance-related issues and adjustments are tracked using Deal Engine's standardized workflow tools, internal financial records, and operational databases. Upon receiving a client claim or update, the Finance team logs the issue, documents the required actions, and monitors completion through formal resolution workflows.

The Finance Manager conducts monthly review meetings to evaluate outstanding issues, remove blockers, and validate accuracy of financial insights shared with the business. Documentation is retained to ensure traceability and completeness.

These procedures support the timely resolution of finance-related matters and maintain the integrity of financial data.

CLIENT CANCELLATION

Client cancellation activities use information from Deal Engine systems, operational ticket-processing logs, and client termination requests submitted through email or formal channels. The Operations team promptly disables ticket-processing operations upon termination and documents the deactivation.

Supervisory personnel validate that no further processing occurs after cancellation, confirming system safeguards and operational compliance. Any required financial adjustments or refunds are processed based on contract terms and client request data.

These procedures ensure that cancellations are executed completely, accurately, and in accordance with client instructions.

INVOICE DEACTIVATION

Invoice deactivation relies on information from client communications, financial records, internal databases, and accounts-receivable systems. Upon receiving a deactivation request, the Finance team follows a formal approval workflow to validate and record the change.

Monthly reconciliations are performed for deactivated customers to verify outstanding balances and confirm completion of required payments. Results are documented to ensure that deactivation activities are accurate, consistent, and auditable.

These procedures help ensure that invoice deactivation is executed securely and in line with financial controls.

CLIENT ACCESS DEACTIVATION

Client access deactivation activities rely on information collected from client termination requests, internal Deal Engine databases, credential-management systems, and operational product-configuration records. Once a client notifies Deal Engine of service termination, the Integrations team reviews the request and validates the client's identity and associated products to ensure accuracy before proceeding.

Upon validation, integration managers disable client credentials within Deal Engine's system infrastructure and deactivate all active products associated with the customer, typically within 24 hours of receiving the notification. These actions are logged and verified through supervisory checks to confirm that no additional access remains and that the client can no longer trigger credential-based processing (e.g., refund quotes, ticket fulfillment, or system-to-system communication).

These procedures ensure that client access is removed completely, accurately, and in a timely manner, preventing unauthorized use of Deal Engine's systems after termination.

Controls Designed to Achieve the Objectives

The specified controls are presented in Section 4, "Description of Control Objectives, Controls, Tests of Controls, and Results of Tests" and are integral components of the system.

OTHER ASPECTS OF THE SERVICE ORGANIZATION'S INTERNAL CONTROL COMPONENTS

Other aspects of the service organization's system that support the services provided include elements of the control environment, risk assessment processes, control activities, information and communication systems, and monitoring activities. These aspects collectively support the achievement of the service organization's objectives and the reliable delivery of services to user entities.

Control Environment

Demonstrating Commitment to Integrity and Ethical Values

The entity promotes a culture of integrity and ethical behavior through established policies, procedures, and leadership practices. Management sets the tone at the top by communicating expectations regarding ethical conduct and compliance with applicable laws and regulations. Employees are provided with training and resources to understand and adhere to these standards. Mechanisms such as whistleblower programs, confidential reporting channels, and disciplinary policies are in place to encourage ethical behavior and address instances of noncompliance. The entity regularly monitors and reinforces its commitment to integrity and ethical values as a foundational aspect of its control environment.

Exercising Oversight Responsibility

The entity's governing body and management actively oversee the design, implementation, and operation of the internal control system. Oversight responsibilities include monitoring management's performance, evaluating compliance with policies and procedures, and reviewing the effectiveness of internal controls over financial reporting. The governing body receives regular reports on key control activities, significant risks, and remediation efforts. This oversight helps ensure that internal controls are appropriately maintained and that deficiencies are addressed in a timely manner, supporting the reliability of financial reporting.

Establishing Structure, Authority, and Responsibility

The entity has established an organizational structure that clearly defines roles, responsibilities, and lines of authority. Management assigns accountability for achieving operational and financial reporting objectives and ensures that employees understand their responsibilities. Authority levels are communicated and documented to support effective decision-making and control execution. The structure is periodically reviewed to ensure it remains appropriate for the entity's size, complexity, and business objectives, supporting the overall effectiveness of the internal control system.

Demonstrating Commitment to Competence

The entity emphasizes the importance of employee competence in achieving operational and financial reporting objectives. Management identifies the knowledge, skills, and experience required for each role and provides appropriate training, guidance, and resources. Performance is monitored to ensure employees can effectively execute their responsibilities, and actions are taken to address gaps in knowledge or skills. This commitment helps maintain the effectiveness of internal controls and supports reliable financial reporting.

Enforcing Accountability

The entity promotes accountability by clearly defining roles and responsibilities and by establishing performance expectations for employees. Management monitors adherence to policies, procedures, and internal controls, and takes appropriate action to address deviations or noncompliance. Mechanisms are in place to recognize performance and address deficiencies in a timely manner. This enforcement of accountability supports the consistent operation of internal controls and the reliability of financial reporting.

Risk Assessment Process

Establishing Suitable Objectives

The entity establishes objectives that are aligned with its mission, strategy, and risk appetite. These objectives provide a framework for identifying and assessing risks that may affect the achievement of operational, financial reporting, and compliance goals. Management ensures that objectives are specific, measurable, and relevant, and periodically reviews them to respond to changes in business conditions, regulatory requirements, and industry practices. This process supports effective risk assessment and the implementation of controls to mitigate potential threats.

Risk Identification and Analysis

The entity identifies and analyzes risks that could affect the achievement of its operational, financial reporting, and compliance objectives. Management considers both internal and external factors, including changes in the business environment, technology, and regulatory requirements. Risks are assessed in terms of their likelihood and potential impact, and prioritized to focus on those that could have the greatest effect on the entity's objectives. This process supports informed decision-making and the design of controls to mitigate significant risks.

Fraud Risk Assessment

The entity considers the risk of fraud in its risk assessment process. Management evaluates potential fraud schemes, including misappropriation of assets and fraudulent financial reporting, and assesses the likelihood and potential impact of such risks. Employees are provided guidance on recognizing and reporting suspected fraud. The assessment results inform the design and implementation of controls intended to prevent, detect, and respond to fraudulent activities, supporting the reliability of financial reporting and operational integrity.

Identification and Analysis of Significant Changes

The entity identifies and evaluates significant changes that could affect the achievement of its objectives, including changes in operations, technology, regulatory requirements, or industry conditions. Management analyzes the potential impact of these changes on existing risks and controls, and determines whether adjustments to controls are necessary. This process helps ensure that the entity's risk assessment remains current and that internal controls continue to operate effectively in a changing environment.

Control Activities

Selection and Development of Control Activities

The entity selects and develops control activities that are designed to mitigate identified risks and support the achievement of objectives. This includes developing both entity-level controls and process-level controls, as well as implementing general controls over technology. Management ensures that control activities are integrated into policies and procedures, consistently applied across the organization, and periodically reviewed to maintain their effectiveness in addressing evolving risks.

Selection and Development of General IT Controls

The entity selects and develops general IT controls to support the reliability, integrity, and security of its information systems. These controls include access management, change management, system development, and backup and recovery processes. Management ensures that IT controls are designed to mitigate technology-related risks, are integrated into relevant processes, and are periodically reviewed and updated to address evolving threats and business needs.

Deployment of Control Activities Through Policies and Procedures

The entity deploys control activities through established policies and procedures to ensure consistent and effective operation. Management communicates expectations to employees, integrates controls into business processes, and monitors adherence to policies. Procedures are documented and periodically reviewed to ensure they remain relevant and effective in mitigating risks and supporting the achievement of operational and financial reporting objectives.

Information and Communication

Use of Relevant Quality Information

The entity obtains and uses information that is relevant, reliable, and timely to support the achievement of its objectives. Management ensures that information is accurate, complete, and appropriately documented to enable effective decision-making, risk assessment, and internal control monitoring. Processes are in place to collect, process, and disseminate information from both internal and external sources, ensuring that stakeholders have access to the information needed to carry out their responsibilities.

Internal Communication

The entity communicates relevant information internally to support the achievement of objectives and the effective functioning of internal controls. Management ensures that employees understand their roles and responsibilities and are informed about policies, procedures, and expectations. Mechanisms such as meetings, reports, and internal messaging systems are used to facilitate timely and accurate communication across all levels of the organization, enabling employees to perform their duties effectively and support reliable financial reporting.

External Communication

The entity communicates relevant information to external parties, including regulators, service recipients, and other stakeholders, as necessary to support transparency and compliance with

applicable requirements. Management ensures that communications are accurate, complete, and timely, and that they convey the necessary information for external parties to understand the entity's processes, risks, and controls. This external communication supports accountability, informed decision-making, and the reliability of information provided outside the organization.

Monitoring Activities

Ongoing and/or Separate Evaluations

The entity performs ongoing and/or separate evaluations to assess the effectiveness of internal controls. Ongoing evaluations occur as part of regular operations, while separate evaluations are conducted periodically or in response to specific events. Management monitors control performance, identifies deficiencies, and takes timely corrective actions. The results of these evaluations are documented and communicated to relevant personnel, supporting the continuous improvement and reliability of the internal control system.

Evaluation and Communication of Deficiencies

The entity evaluates identified control deficiencies to determine their significance and potential impact on achieving objectives. Management communicates significant deficiencies to appropriate personnel, including those responsible for corrective actions and oversight. Timely remediation efforts are initiated to address deficiencies, and follow-up activities are conducted to ensure that corrective actions are effective. This process supports the ongoing reliability and effectiveness of the internal control system.

CHANGES TO THE SYSTEM DURING THE PERIOD

No significant changes have occurred to the services provided to user entities during the examination period.

SYSTEM INCIDENTS DURING THE PERIOD

No significant incidents have occurred to the services provided to user entities during the examination period.

COMPLEMENTARY SUBSERVICE ORGANIZATIONS CONTROLS (CSOCS)

Deal Engine's controls related to the Automated Refunds and Changes Platform cover only a portion of overall internal control for each user entity of Deal Engine. It is not feasible for the control objectives related to the Automated Refunds and Changes Platform to be achieved solely by Deal Engine. Therefore, each user entity's internal controls should be evaluated in conjunction with Deal Engine's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

Deal Engine relies on AWS and GCP as the subservice organizations to provide Cloud Hosting Services and controls, which form the foundation of the company's IT infrastructure.

The core financial processes that rely on AWS and GCP are those performed by Deal Engine's refunds management platform, which include:

- **Transaction Initiation and Authorization:** Financial transactions (e.g., customer payments, billing records, adjustments) are created by authorized personnel or system integrations. Controls ensure transactions are properly approved before processing.

- **Transaction Processing:** The underlying servers, databases, and network components that support the real-time processing, authorization, and routing of payment transactions. Once authorized, transactions are validated for completeness and accuracy and processed in real time within the company's financial platform. System logic enforces business rules, prevents duplicate entries, and ensures that only valid transactions move forward.

- **Recording and Classification:** Processed transactions are stored in the company's financial database, where they are automatically categorized and recorded to support accurate financial reporting.

- **Data Integrity and Reconciliation:** System controls, automated checks, and periodic reconciliations ensure that financial data remains accurate, consistent, and free from unauthorized modification.

- **Reporting:** The financial information generated by the system (e.g., transaction summaries, account balances, revenue reports) is used by management for operational and financial reporting purposes.

- **Data Integrity and Availability:** Infrastructure, backup procedures, and monitoring controls ensure financial systems remain available to support timely processing and reporting requirements.

The design of Deal Engine's controls assumes that AWS and GCP are responsible for maintaining physical and environmental protection controls over the data centers hosting Deal Engine's infrastructure and assumes that those controls were suitably designed and operating effectively between January 1, 2025, to September 30, 2025.

| #	Complementary Subservice Organizations Controls (CSOC)	Control Objectives
1	Controls provide reasonable assurance that all newly onboarded client contracts are accurately created, maintained, and updated in accordance with organizational policies and regulatory requirements.	Control Objective 1
2	Controls provide reasonable assurance that client credential integrations are executed safely, completely, and in a timely manner, and that required operations are enabled properly (e.g., fetch ticket information, quoting, refunds).	Control Objective 2
3	Controls provide reasonable assurance that invoicing configurations are set up accurately and correctly.	Control Objective 3
4	Controls provide reasonable assurance that invoicing monitoring configurations are accurate and appropriate.	Control Objective 4
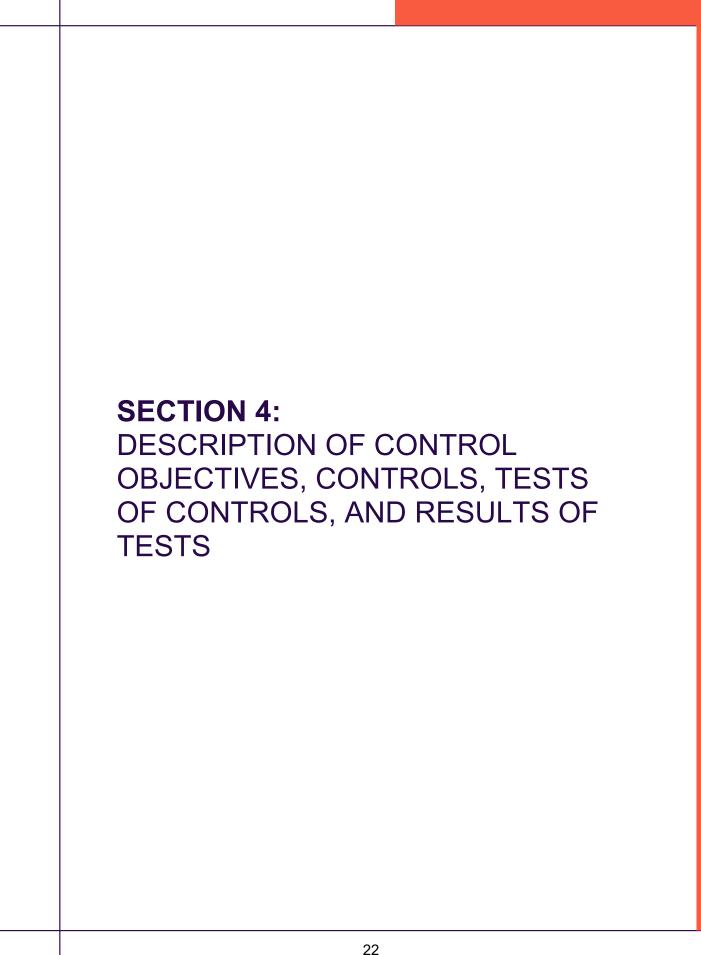
#	Complementary Subservice Organizations Controls (CSOC)	Control Objectives
5	Controls provide reasonable assurance that client billing information is periodically validated and that the system enforces monthly data-quality checks to prevent incomplete or inaccurate entries.	Control Objective 5
6	Controls provide reasonable assurance that operational systems are continuously monitored to maintain service quality, availability, and performance standards.	Control Objective 6
7	Controls provide reasonable assurance that monthly invoicing processes are executed accurately, on schedule, and on time.	Control Objective 7
8	Controls provide reasonable assurance that accounts receivable collection processes are effective, timely, and properly documented.	Control Objective 8
9	Controls provide reasonable assurance that finance-related issues are properly tracked and resolved.	Control Objective 9
10	Controls provide reasonable assurance that client cancellations are processed accurately, completely, and in a timely manner, and that any associated financial impacts (e.g., refunds, adjustments) are properly recorded and reported.	Control Objective 10
11	Controls provide reasonable assurance that invoice deactivation processes are managed securely and on schedule.	Control Objective 11
12	Controls provide reasonable assurance that client cancellations are processed accurately, completely, in a timely manner and that all credentials and services are disconnected from our infrastructure to avoid their misuse (e.g., refund quote and fulfillment).	Control Objective 12
13	Controls provide reasonable assurance that oversight, standards of conduct, and a structure for carrying out internal controls and identifying and assesses risks are implemented.	Control Objective 13
14	Controls provide reasonable assurance that security measures are in place around sensitive data and logical access to programs, data, and computer resources is restricted to authorized and appropriate users.	Control Objective 14
15	Controls provide reasonable assurance that systems are monitored and deviations, problems and errors are identified, tracked, and recorded in a complete, accurate and timely manner.	Control Objective 15
16	Controls provide reasonable assurance that changes to systems, applications, databases, and infrastructure are authorized, tested, documented, approved and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.	Control Objective 16
17	Controls provide reasonable assurance that critical applications and data are backed up regularly and are available for restoration in the event of processing errors or unexpected processing interruptions.	Control Objective 17

COMPLEMENTARY USER ENTITY CONTROLS (CUECS)

Deal Engine's controls were designed with the assumption that certain controls will be implemented by user entities. It is not feasible for control objectives relating to transaction processing to be achieved completely by Deal Engine's management or the user entities acting alone. It is necessary for user entities to implement controls to achieve some of the control objectives identified in this report, as applicable.

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 achieved. 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.

#	Complementary User Entity Control	Related Control Objective
1	User entity must provide an authorized signature or executed agreement to establish a commercial relationship and initiate service provisioning.	Control Objective 1
2	User entity must submit credentials, sensitive information, or system access details only through secure, encrypted communication channels.	Control Objective 2
3	User entity must provide complete and accurate billing information (e.g., legal entity name, tax details, billing contact, PO requirements) to ensure proper setup and ongoing accuracy of the Deal Engine financial and billing processes.	Control Objectives 3 & 7
4	If the user entity requires purchase orders, financial approvals, or internal authorization documents, such approvals must be issued to the Company in a timely manner before billing or invoicing can proceed.	Control Objective 7
5	User entity must ensure that all invoices issued by the Company are internally reviewed, approved, and paid in accordance with the user entity's internal financial authorization and payment processes.	Control Objective 8

SECTION 4:
DESCRIPTION OF CONTROL OBJECTIVES, CONTROLS, TESTS OF CONTROLS, AND RESULTS OF TESTS

DESCRIPTION OF CONTROL OBJECTIVES, RELATED CONTROLS, TESTS OF CONTROLS, AND RESULTS OF TESTS

INFORMATION PROVIDED BY INSIGHT ASSURANCE

This SOC 1 Type 2 report was prepared in accordance with American Institute of Certified Public Accountants (AICPA) Statements on Standards for Attestation Engagements. Insight Assurance's examination of the controls of Deal Engine was limited to the control objectives and related controls specified by Deal Engine's management and did not encompass all aspects of Deal Engine's operations or operations at user entities.

In determining whether this report meets the user entities' auditors' objectives, the user auditor should perform the following procedures:

- Understand the aspects of Deal Engine's controls that may affect the processing of the user entities' transactions;
- Understand the flow of significant transactions through Deal Engine;
- Determine whether the control objectives are relevant to the user entities' financial statement assertions;
- Determine whether Deal Engine's controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the user entities' financial statements and determine whether they have been implemented.

FOOTNOTES FOR TEST RESULTS WHEN NO TESTS OF OPERATING EFFECTIVENESS WERE PERFORMED

1. The control was performed on an annual basis; however, its execution occurred outside the examination period. Therefore, no tests of operating effectiveness were performed.

CONTROL OBJECTIVES, RELATED CONTROLS, TESTS OF CONTROLS, AND RESULTS OF TESTS

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 1 - CONTRACT MANAGEMENT CONTROL			
CO 1 - Controls provide reasonable assurance that all newly onboarded client contracts are accurately created, maintained, and updated in accordance with organizational policies and regulatory requirements.			
CO 1.1	Clients are required to review and execute Deal Engine's Master Service Agreement (MSA), Non-Disclosure Agreement (NDA), Order Form and Service Level Agreement (SLA) prior to onboarding with the Deal Engine service.	Inspected the executed agreements and Order Form for a sample of new clients to determine that clients were required to review and execute the company's MSA, NDA, Order Form and SLA prior to onboarding with the company's service.	No exceptions noted.
CO 1.2	The legal manager requires the signature of the contract in order to confirm the consent of the client regarding Deal Engine services.	Inspected the signed contracts for a sample of new clients to determine that the legal manager required the signature of the contract in order to confirm the consent of the client regarding the company's services.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 2 - CLIENT CREDENTIAL INTEGRATION			
CO 2 - Controls provide reasonable assurance that client credential integrations are executed safely, completely, and that required operations are enabled properly (e.g., fetch ticket information, quoting, refunds).			
CO 2.1	The client shares credentials via an encrypted channel and the integration engineer adds the credentials to the Firestore Database as agreed upon with the client.	Inspected the credential-sharing documentation for a sample of client integrations to determine that the client shared credentials via an encrypted channel.	No exceptions noted.
		Inspected the system configuration and database records for a sample of client integrations to determine that the integration engineer added the credentials to the Firestore Database as agreed upon with the client.	No exceptions noted.
CO 2.2	An integrations engineer makes a request to the Deal Engine application to use the credentials for communication with an external service provider to extract client data as agreed upon with the client.	Inspected the supporting documentation for credential use requests to the application for a sample of client integrations to determine that an integrations engineer made a request to the company's application to use the credentials for communication with an external service provider to extract client data as agreed upon with the client.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 3 - INVOICING SETUP			
CO 3 - Controls provide reasonable assurance that invoicing configurations are set up accurately and correctly.			
CO 3.1	Set up invoice rules: The finance team and the IT team maintain a formal approval process for all billing initial configuration every time a client is registered.	Inspected the product billing rules, the invoice matching documentation, and the Dry Run meeting records for a sample of new clients to determine that the finance team and the IT team maintained a formal approval process for all billing initial configuration every time a client was registered.	Exceptions noted: For five of five (100%) samples of new clients, the company did not maintain formal approval documentation for all billing initial configurations.
CO 3.2	Generation of the invoices: The finance manager, once the client integration is completed, ensures all invoicing setups match Deal Engine's customers' contract terms.	Inspected the invoicing setup for a sample of new clients to determine that the finance manager, once the client integration was completed, ensured all invoicing setups match the Deal Engine's customers' contract terms.	Exceptions noted: For five of five (100%) samples of new clients, the company did not maintain formal documentation demonstrating that the finance manager reviewed and confirmed that the invoicing setups aligned with the customers' contract terms.
CO 3.3	Validate authorized users in invoice application: The IT team implements system controls to prevent unauthorized users from changing billing configurations.	Inspected the user administrator listing to determine that the IT team implemented system controls to prevent unauthorized users from changing billing configurations.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 4 - INVOICING MONITORING			
CO 4 - Controls provide reasonable assurance that invoicing configurations are accurate and appropriate.			
CO 4.1	Monitoring rules control: The finance manager ensures all invoicing setups match Deal Engine's customers' contract terms quarterly.	Inspected the invoicing setup for a sample of quarters to determine that the finance manager ensured all invoicing setups match the company's customers' contract terms quarterly.	No exceptions noted.
CO 4.2	Approval process for changes in invoicing configuration: The finance and IT teams validate billing rate updates through a formal change management process (requests, approvals, testing, and verification) twice a year.	Inspected the invoice configuration change ticket to determine that the finance and IT teams validated billing rate updates through a formal change management process (requests, approvals, testing, and verification) twice a year.	No exceptions noted.
CO 4.3	On a monthly basis, the Offline and Online Travel Agencies (OOTAs) operations team monitors system performance, transaction processing, and service availability through automated alerting tools, ensuring timely identification of operational anomalies.	Inspected system performance monitoring, transaction processing, and automated alerting tool to determine that on a monthly basis, the OOTAs operations team monitored system performance, transaction processing, and service availability through automated alerting tools, ensuring timely identification of operational anomalies.	No exceptions noted.
CO 4.4	Credentials validation for authorized users: The IT team verifies system controls semi-annually to prevent unauthorized users from changing billing configurations.	Inspected the credential validation to determine that the IT team verified system controls semi-annually to prevent unauthorized users from changing billing configurations.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 5 - CLIENT DATA			
CO 5 - Controls provide reasonable assurance that client billing information is periodically validated and that the system enforces monthly data-quality checks to prevent incomplete or inaccurate entries.			
CO 5.1	Validate registered information: The finance manager validates customers' billing information recorded in the database and compares it with the official incorporation forms or subsequent requests for changes in billing information on a quarterly basis.	Inspected the client database documentation and the Dry Run meeting records for a sample of quarters to determine that the finance manager validated customers' billing information recorded in the database and compared it with the official incorporation forms or subsequent requests for changes in billing information on a quarterly basis.	No exceptions noted.
CO 5.2	Data validation - Sanity check for invoicing data: The Deal Engine system enforces data quality controls to prevent incomplete or invalid contact information entries every month.	Inspected the system's data validation rules and test data results to determine that the company's system enforced data quality controls preventing incomplete or invalid contact information entries every month.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 6 - OPERATIONS MONITORING			
CO 6 - Controls provide reasonable assurance that operational systems are continuously monitored to maintain service quality, availability, and performance standards.			
CO 6.1	The operations team conducts monthly system health checks and performance reviews to proactively identify potential issues before they impact service delivery.	Inspected the documented results of system performance checks for a sample of months to determine that the operations team conducted monthly system health checks and performance reviews to proactively identify potential issues before they impacted service delivery.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 7 - MONTHLY INVOICING			
CO 7 - Controls provide reasonable assurance that monthly invoicing processes are executed accurately, on schedule, and on time.			
CO 7.1	Data Validation: The finance team ensure all invoicing data is accurate and complete across databases on a monthly basis.	Inspected the invoice data validation documentation for a sample of months to determine that the finance team ensured all invoicing data was accurate and complete across databases on a monthly basis.	No exceptions noted.
CO 7.2	Approve client adjustments: The finance team reviews and approves all customer adjustments through a formal verification process on a monthly basis.	Inspected the verification process for a sample of client adjustments to determine that the finance team reviewed and approved all customer adjustments through a formal verification process on a monthly basis.	No exceptions noted.
CO 7.3	Generation of invoices: The Deal Engine system generates invoices according to established billing cycles and contractual terms with automated validation controls on a monthly basis.	Inspected the automated backend validation control and the generated invoices for a sample of months to determine that the company's system generated invoices according to established billing cycles and contractual terms with automated validation controls on a monthly basis.	No exceptions noted.
CO 7.4	Invoices classification: The finance team maintains and archives all invoices in designated repository with appropriate access controls on a monthly basis.	Inspected the company's invoice repository for the sampled months and its authorized list of users to determine that the finance team maintained and archived all invoices in the designated repository with appropriate access controls on a monthly basis.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 7 - MONTHLY INVOICING			
CO 7 - Controls provide reasonable assurance that monthly invoicing processes are executed accurately, on schedule, and on time.			
CO 7.5	Sending Invoices: The finance team distributes invoices to customers through established channels on a monthly basis.	Inspected the customer invoice distribution channel for a sample of months to determine that the finance team distributed invoices to customers through established channels on a monthly basis.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 8 - ACCOUNTS RECEIVABLE COLLECTION			
CO 8 - Controls provide reasonable assurance that accounts receivable collection processes are effective, timely, and properly documented.			
CO 8.1	Analysis of accounts receivable: The finance manager evaluates collection effectiveness through key metrics (i.e., collection rate) and implements corrective measures for underperforming segments.	Inspected the analysis of accounts receivable documentation to determine that the finance manager evaluated collection effectiveness through key metrics (i.e., collection rate) and implemented corrective measures for underperforming segments.	No exceptions noted.
CO 8.2	Escalation process in accounts receivable: The finance team applies a clearly defined escalation protocol based on the level of client delinquencies at least monthly.	Inspected the escalation protocol documentation for a sample of months to determine that the finance team applied a clearly defined escalation protocol based on the level of client delinquencies at least monthly.	No exceptions noted.
CO 8.3	Matching between financial software and bank statements: The finance team ensures all customers' payments are reconciled at least monthly against cashflow entries and ensure in-full payment.	Inspected the payment reconciliation documentation for a sample of months to determine that the finance team ensured all customers' payments were reconciled at least monthly against cashflow entries and ensured full payment.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 9 - FINANCE PROCESS			
CO 9 - Controls provide reasonable assurance that finance-related issues are properly tracked and resolved.			
CO 9.1	Finance related adjustments: The finance team implements a standardized workflow system for tracking all finance-related issues from identification through resolution upon receipt of client claims.	Inspected the standardized workflow for a sample of client claims to determine that the finance team implemented a standardized workflow system for tracking all finance-related issues from identification through resolution upon receipt of client claims.	No exceptions noted.
CO 9.2	Finance results and insights with each line of business: The finance manager conducts monthly issue review meetings to assess the status of outstanding items and remove resolution barriers.	Inspected the issue review meeting invitations, attendee listing, and the supporting meeting summaries for a sample of months to determine that the finance manager conducted monthly issue review meetings to assess the status of outstanding items and remove resolution barriers.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 10 - CLIENT CANCELLATION			
CO 10 - Controls provide reasonable assurance that client cancellations are processed accurately, completely, and in a timely manner, and that any associated financial impacts (e.g., refunds, adjustments) are properly recorded and reported.			
CO 10.1	Deactivation of the operations: The OOTAs team promptly deactivates ticket operations upon client termination as per client request.	Inspected the deactivation of operations for a sample of terminated clients to determine that the OOTAs team promptly deactivated ticket operations upon client termination as per client request.	No exceptions noted.
CO 10.2	Verification of the deactivation: The OOTAs manager ensures operational safeguards to prevent further ticket processing after client termination.	Inspected the deactivation verification process for a sample of terminated clients to determine that the OOTAs manager ensured operational safeguards to prevent further ticket processing after client termination.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 11 - INVOICE DEACTIVATION			
CO 11 - Controls provide reasonable assurance that invoice deactivation processes are managed securely and on schedule.			
CO 11.1	The finance team follows a formal approval workflow upon receipt of client invoice deactivation requests.	Inspected the approval records for deactivation for a sample of terminated clients to determine that the finance team followed a formal approval workflow upon receipt of client invoice deactivation requests.	No exceptions noted.
CO 11.2	The finance team performs monthly reconciliation of pending invoices from deactivated customers to ensure in-full payment.	Inspected the monthly pending invoice reconciliation documentation for a sample of terminated customers to determine that the finance team performed monthly reconciliation of pending invoices from deactivated customers to ensure full payment.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 12 - CLIENT ACCESS DEACTIVATION			
CO 12 - Controls provide reasonable assurance that client cancellations are processed accurately, completely, in a timely manner and that all credentials and services are disconnected from our infrastructure to avoid their misuse (e.g., refund quote and fulfillment).			
CO 12.1	Disable client credentials: The integration managers disable client credentials in the Deal Engine system infrastructure within 24 hours of clients notifying Deal Engine.	Inspected the disabling of credentials for a sample of terminated clients to determine that the integration managers disabled client credentials in the Deal Engine system infrastructure within 24 hours of clients notifying Deal Engine.	No exceptions noted.
CO 12.2	Disable active products: The integration managers disable all active products from the Deal Engine infrastructure within 24 hours of clients notifying Deal Engine.	Inspected the disabling of active products for a sample of terminated clients to determine that the integration managers disabled all active products from the company's infrastructure within 24 hours of clients notifying Deal Engine.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 13 - CONTROL ENVIRONMENT			
CO 13 - Controls provide reasonable assurance that provides oversight, standards of conduct, and a structure for carrying out internal controls and identifies and assesses risks.			
CO 13.1	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the company's organizational chart to determine that the company maintained an organizational chart that described the organizational structure and reporting lines.	No exceptions noted.
CO 13.2	The company performs background checks on new employees.	Inspected the completed background checks for a sample of new employees to determine that the company performed background checks on new employees.	No exceptions noted.
CO 13.3	The company requires employees and contractors to acknowledge a Code of Conduct at the time of hire. Employees and contractors who violate the Code of Conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the acknowledgments of the Code of Conduct for a sample of new employees and contractors to determine that the Code of Conduct was acknowledged at the time of hire.	No exceptions noted.
		Per inquiry with management and inspection of the company's code of conduct violation listing, there were no violations identified during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CO 13.4	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected the signed Non-Disclosure Agreements (NDAs) for a sample of contractors to determine that the company required contractors to sign a confidentiality agreement at the time of engagement.	No exceptions noted.
CO 13.5	The company requires employees to sign a confidentiality agreement during onboarding.	Inspected the signed NDAs for a sample of new employees to determine that the company required employees to sign a confidentiality agreement during onboarding.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 13 - CONTROL ENVIRONMENT			
CO 13 - Controls provide reasonable assurance that provides oversight, standards of conduct, and a structure for carrying out internal controls and identifies and assesses risks.			
CO 13.6	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.
CO 13.7	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CO 13.8	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 company's Risk Management Policy to determine that the 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 exceptions noted.
CO 13.9	The company requires employees to complete security awareness training within thirty days of hire and active employees to complete security awareness training at least annually.	Inspected the training records for a sample of new employees to determine that the company required employees to complete security awareness training within thirty days of hire.	No exceptions noted.
		Inspected the training records for a sample of active employees to determine that the company required employees to complete security awareness training at least annually.	No exceptions noted.

| Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 14 - LOGICAL ACCESS SECURITY			
CO 14 - Controls provide reasonable assurance that security measures are in place around sensitive data and logical access to programs, data, and computer resources is restricted to authorized and appropriate users.			
CO 14.1	The company ensures that user access to in-scope system components is based on job role and function.	Inspected the access provisioning documentation for a sample of new contractors and employees to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.
CO 14.2	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Inspected the anti-malware configurations for a sample of workstations to determine that anti-malware technology was deployed, routinely updated, logged, and installed on all relevant systems.	No exceptions noted.
CO 14.3	Access to production applications, servers, and databases is restricted to authorized users with a business need.	Inspected the administrator user listing and access roles to determine that access to production applications, servers, and databases was restricted to authorized users with a business need.	No exceptions noted.
CO 14.4	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the user access revocation documentation for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process within the company's SLAs.	No exceptions noted.
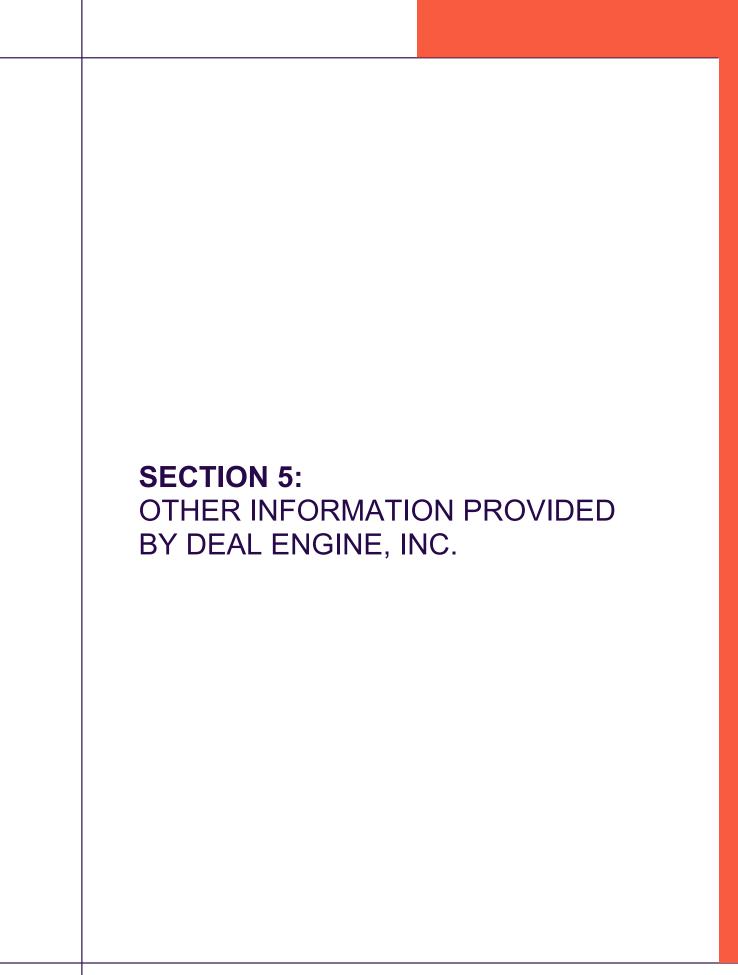
Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 14 - LOGICAL ACCESS SECURITY			
CO 14 - Controls provide reasonable assurance that security measures are in place around sensitive data and logical access to programs, data, and computer resources is restricted to authorized and appropriate users.			
CO 14.5	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the password configurations and written password policy to determine that the company required passwords for in-scope system components to be configured according to the company's policy.	Exceptions noted: The password parameters for the company-developed application were not configured to match the company's documented policy.
CO 14.6	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved, encrypted connection.	No exceptions noted.
CO 14.7	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Inspected the company's third-party penetration test report to determine that penetration testing was performed at least annually.	No exceptions noted.
		Per inquiry with management and inspection of the penetration test report, it was noted that there were no critical or high-risk vulnerabilities identified in the report; therefore, no testing was performed.	No testing performed. See footnote 1 above.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 14 - LOGICAL ACCESS SECURITY			
CO 14 - Controls provide reasonable assurance that security measures are in place around sensitive data and logical access to programs, data, and computer resources is restricted to authorized and appropriate users.			
CO 14.8	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's website and TLS certificate to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CO 14.9	The company uses firewalls and configures them to prevent unauthorized access.	Inspected the firewall ruleset configurations to determine that the firewall was configured to prevent unauthorized access to the company's network.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 15 - SYSTEM AND SUBSERVICE ORGANIZATION MONITORING			
CO 15 - Controls provide reasonable assurance that systems are monitored and deviations, problems and errors are identified, tracked, and recorded in a complete, accurate and timely manner.			
CO 15.1	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the monitoring tool configurations to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 16 - CHANGE MANAGEMENT			
CO 16 - Controls provide reasonable assurance that changes to systems, applications, databases, and infrastructure are authorized, tested, documented, approved and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.			
CO 16.1	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.	Inspected the change management documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
CO 16.2	The company restricts access to migrate changes to production to authorized personnel.	Inspected the branch protection rule configurations and the users with the ability to deploy changes to production to determine that the company restricted access to migrate changes to production to authorized personnel.	No exceptions noted.

Control Number	Controls	Detailed Tests of Controls	Test Results
CONTROL OBJECTIVE 17 - BACKUPS AND RECOVERY			
CO 17 - Controls provide reasonable assurance that critical applications and data are backed up regularly and are available for restoration in the event of processing errors or unexpected processing interruptions.			
CO 17.1	The company performs periodic backups for production data. Data is backed up to a different location than the production system.	Inspected the system backup configurations for the in-scope environments to determine that the company performed periodic backups for production data.	No exceptions noted.
		Inspected the multi-region location configurations for the in-scope environments to determine that data was backed up to a different location than the production system.	No exceptions noted.
CO 17.2	Access to production applications, servers, and databases is restricted to authorized users with a business need.	Inspected the administrator user listing and access roles to determine that access to production applications, servers, and databases was restricted to authorized users with a business need.	No exceptions noted.
CO 17.3	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests the business continuity/disaster recovery (BC/DR) plan at least annually.	Inspected the company's BC/DR Plan to determine that the company has a documented BC/DR plan.	No exceptions noted.
		Inspected the company's disaster recovery tabletop exercise meeting minutes to determine that the BC/DR plan was tested annually.	Exceptions noted: The disaster recovery tabletop exercise documentation did not demonstrate that a hands-on restoration test occurred.

SECTION 5:
OTHER INFORMATION PROVIDED
BY DEAL ENGINE, INC.

MANAGEMENT'S RESPONSES TO THE NOTED EXCEPTIONS

Control Activity	Noted Exceptions	Management's Responses
Set up invoice rules: The finance team and the IT team maintain a formal approval process for all billing initial configuration every time a client is registered.	Exceptions noted: For five of five (100%) samples of new clients, the company did not maintain formal approval documentation for all billing initial configurations.	The approval process was performed during the audit period and supported through management meetings, internal minutes, and operational reviews within Dry Run. Management has since implemented a centralized evidence-retention process to ensure all approvals are properly documented going forward.
Generation of the invoices: The finance manager, once the client integration is completed, ensures all invoicing setups match Deal Engine's customers' contract terms.	Exceptions noted: For five of five (100%) samples of new clients, the company did not maintain formal documentation demonstrating that the finance manager reviewed and confirmed that the invoicing setups aligned with the customers' contract terms.	
The company requires passwords for in-scope system components to be configured according to the company's policy.	Exceptions noted: The password parameters for the company-developed application were not configured to match the company's documented policy.	Management acknowledges the exception noted regarding the misalignment between the password settings of the company-developed application and the requirements outlined in the company's password policy. Upon identification of the issue, the application's configuration was updated to fully comply with the established policy. The remediation has been completed, and the control is now operating in accordance with requirements.

Control Activity	Noted Exceptions	Management's Responses
The company has a documented business continuity/disaster recovery (BC/DR) plan and tests the business continuity/disaster recovery (BC/DR) plan at least annually.	Exceptions noted: The disaster recovery tabletop exercise documentation did not demonstrate that a hands-on restoration test occurred.	Management acknowledges the exception related to the absence of documented restoration testing for both production environments. While annual tabletop exercises are performed using various simulated scenarios, full restoration testing had not been conducted as required. Management will perform restoration testing in alignment with policy requirements going forward and will incorporate it into the annual testing cycle.