linford & co llp cpa firm

TK

TwinKnowledge Inc.

TYPE II SOC 2

REPORT ON CONTROLS RELEVANT TO SECURITY

DECEMBER 1, 2024 TO MAY 31, 2025

TwinKnowledge Inc.

Report on TwinKnowledge's Description of Its AI Project Intelligence and Its Controls Relevant to Security

Table of Contents

Description **Page**

TwinKnowledge Inc.

Report on TwinKnowledge's Description of Its AI Project Intelligence and Its Controls Relevant to Security

Table of Contents (continued)

Section I – Independent Service Auditor's Report

To the Board of Directors of TwinKnowledge Inc.:

Scope

We have examined TwinKnowledge Inc.'s (TwinKnowledge or the Company) accompanying description of its AI project intelligence titled, "TwinKnowledge's Description of Its AI Project Intelligence" throughout the period December 1, 2024 to May 31, 2025 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance—2022)*, in AICPA *Description Criteria* (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period December 1, 2024 to May 31, 2025 to provide reasonable assurance that TwinKnowledge's service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022),* in AICPA *Trust Services Criteria*.

TwinKnowledge uses Amazon Web Services (AWS), a subservice organization, to provide hosting and managed services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TwinKnowledge, to achieve TwinKnowledge's service commitments and system requirements based on the applicable trust services criteria. The description presents TwinKnowledge's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TwinKnowledge's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at TwinKnowledge, to achieve TwinKnowledge's service commitments and system requirements based on the applicable trust services criteria. The description presents TwinKnowledge's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of TwinKnowledge's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

TwinKnowledge is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that TwinKnowledge's service commitments and system requirements were achieved. TwinKnowledge has provided the accompanying assertion titled "Assertion of TwinKnowledge Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein.

TwinKnowledge is also 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; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

- ✓ Obtaining an understanding of the system and service organization's service commitments and system requirements.
- ✓ Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- ✓ Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- ✓ Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- ✓ Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- ✓ Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations
The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls
The specific controls we tested and the nature, timing, and results of those tests are presented in Section IV of this report titled, *Independent Service Auditor's Description of Tests of Controls and Results*.

Opinion
In our opinion, in all material respects:

a. The description presents TwinKnowledge's AI project intelligence that was designed and implemented throughout the period December 1, 2024 to May 31, 2025 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period December 1, 2024 to May 31, 2025 to provide reasonable assurance that TwinKnowledge's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of TwinKnowledge's controls throughout that period.
c. The controls stated in the description operated effectively throughout the period December 1, 2024 to May 31, 2025 to provide reasonable assurance that TwinKnowledge's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of TwinKnowledge's controls operated effectively throughout that period.

Restricted Use
This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of TwinKnowledge, user entities of TwinKnowledge's AI project intelligence during some or all of the period December 1, 2024 to May 31, 2025, business partners of TwinKnowledge subject to risks arising from interactions with the AI project intelligence practitioners providing services to

such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- ✓ The nature of the service provided by the service organization.
- ✓ How the service organization’s system interacts with user entities, business partners, subservice organizations, and other parties.
- ✓ Internal control and its limitations.
- ✓ Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements.
- ✓ User entity responsibilities and how they may affect the user entity’s ability to effectively use the service organization’s services.
- ✓ The applicable trust services criteria.
- ✓ The risks that may threaten the achievement of the service organization’s service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

linford&co llp

June 17, 2025
Denver, Colorado

Section II – Assertion of TwinKnowledge Management

June 17, 2025

We have prepared the accompanying description of TwinKnowledge Inc.'s (TwinKnowledge or the Company) AI project intelligence titled, "TwinKnowledge's Description of Its AI Project Intelligence" throughout the period December 1, 2024 to May 31, 2025 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance—2022)* in AICPA *Description Criteria* (description criteria). The description is intended to provide report users with information about the AI project intelligence that may be useful when assessing the risks arising from interactions with TwinKnowledge's system, particularly information about system controls that TwinKnowledge has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022),* in AICPA *Trust Services Criteria*.

TwinKnowledge uses AWS, a subservice organization, to provide hosting and managed services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TwinKnowledge, to achieve TwinKnowledge's service commitments and system requirements based on the applicable trust services criteria. The description presents TwinKnowledge's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TwinKnowledge's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at TwinKnowledge, to achieve TwinKnowledge's service commitments and system requirements based on the applicable trust services criteria. The description presents TwinKnowledge's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of TwinKnowledge's controls.

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

a. The description presents TwinKnowledge's AI project intelligence that was designed and implemented throughout the period December 1, 2024 to May 31, 2025 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period December 1, 2024 to May 31, 2025 to provide reasonable assurance that TwinKnowledge's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user

entities applied the complementary controls assumed in the design of TwinKnowledge’s controls throughout that period.

c. The controls stated in the description operated effectively throughout the period December 1, 2024 to May 31, 2025 to provide reasonable assurance that TwinKnowledge’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of TwinKnowledge’s controls operated effectively throughout that period.

Ivan Panushev
CEO and Founder

Section III – TwinKnowledge's Description of Its AI Project Intelligence

Overview of Operations

Overview of TwinKnowledge

TwinKnowledge is a New York-based AI software company founded in 2023. It specializes in developing AI-powered copilots tailored for professionals in the architecture, engineering, construction, and operations (AECO) industries. These AI agents assist in streamlining project workflows by analyzing complex data from construction documents, specifications, and other critical materials, thereby enhancing decision-making and reducing inefficiencies.

Description of TwinKnowledge's AI Project Intelligence

With custom, highly accurate AI assistants over project drawing sets, contract documents, and more, TwinKnowledge puts project information at the fingertips of project teams to reduce project complexity and streamline error detection, driving higher-quality drawing sets at every phase of the project.

Components of the System Used to Provide the AI Project Intelligence

The system used by TwinKnowledge to deliver the AI project intelligence is comprised of a combination of components that includes the products and the data processed, but also extends to the underlying infrastructure, subservice organizations that support the system and internal control, the Company's employees, as well as the policies and procedures followed to maintain the security of the AI project intelligence and client data. The following is a summary of the components that comprise the system. Specific processes and controls relevant to the security criteria are described in the remainder of this section of the report.

Infrastructure

TwinKnowledge's information technology (IT) environment is hosted in AWS. AWS provides cloud hosting and infrastructure managed services, and TwinKnowledge has configured and utilizes various AWS security and performance monitoring tools

Subservice Organization: TwinKnowledge uses a subservice organization to achieve operating efficiency and to obtain specific expertise. The following is the principal subservice organization used by TwinKnowledge:

- ✓ **Amazon Web Services (AWS)** – AWS hosts a portion of TwinKnowledge's production IT environment and provides certain managed services. AWS undergoes an annual Type II SOC 2 examination and the report may be obtained directly from them. TwinKnowledge obtains and reviews the SOC 2 report provided by AWS related to their hosting operations to determine whether controls are designed and operating effectively at AWS. Additionally, any listed complementary user entity controls in the AWS SOC reports are also reviewed and addressed by TwinKnowledge.

Software
TwinKnowledge's AI project intelligence services are enabled by its privately owned applications, and the use of reputable and SOC examined third party tools and applications. The AI project intelligence services are supported by TwinKnowledge's applications, servers, and tools. The TwinKnowledge applications are developed and maintained by TwinKnowledge IT personnel. Role-based access controls (RBAC) govern the capabilities employees and users can execute within the TwinKnowledge applications and tools.

Data
Client data is stored within TwinKnowledge's production database instances in AWS. TwinKnowledge has implemented security controls to protect the confidentiality of the data. Client data within the databases is encrypted at rest. Additionally, all data transfers between users and TwinKnowledge are secured using Transport Layer Security (TLS) and industry-standard encryption.

People
TwinKnowledge has a staff of personnel organized into functional areas so that personnel understand their responsibilities within the organization.

Policies and Procedures
TwinKnowledge has established and maintains security policies and procedures over the AI project intelligence services. TwinKnowledge makes these internal policies and procedures, including security policies, available to its personnel on its internal shared drives to provide direction regarding their responsibilities related to the functioning of internal control.

Principal Service Commitments and System Requirements

TwinKnowledge designs its processes and procedures to meet objectives for its AI project intelligence. Those objectives are based on the service commitments that TwinKnowledge company makes to user entities and the compliance requirements that TwinKnowledge has established for their services.

Security commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security and confidentiality principles within the fundamental design of the AI project intelligence are implemented to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Controlled access to the production environment and the supporting infrastructure.
- Segregation of client data.
- Monitoring of system performance metrics and critical application services.

TwinKnowledge establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in TwinKnowledge's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal networks are managed, and how personnel are onboarded and trained.

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication, Monitoring, and Control Activities for the Security Criteria

Note: *Parenthetical references have been included in the following narratives as a cross reference to the applicable control activities included in Section IV of this report.*

A company's entity-level controls reflect the overall attitude, awareness, and actions of management and others concerning the importance of controls and the emphasis given to controls in the company's policies, procedures, methods, and organizational structure. Entity-level controls are not specific to any individual transaction but apply to the company as a whole. These types of controls are necessary to facilitate the proper functioning of activity-level controls supporting the AI project intelligence. Throughout this section, a description is presented of the five components of internal control (control environment, risk assessment, information and communication, monitoring, and control activities) as they relate to the services TwinKnowledge provides to its clients.

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. The security criteria and the controls designed, implemented, and operated to meet them such that the system is protected against unauthorized access (both physical and logical). Entity-level controls and specific control activities supporting the applicable trust services criteria are provided in the descriptions of this section of the report, and in *Section IV – Independent Service Auditor's Description of Tests of Controls and Results.*

Control Environment

The control environment is the umbrella under which the control components of internal control fall. The control environment at TwinKnowledge includes "tone at the top," which management sets by example in adhering to ethical business practices and company policies, and by conducting business with integrity. Management's example and leadership are the primary mechanisms used to guide employees in the execution of TwinKnowledge's operations. The control environment is the collective responsibility of the management team.

Integrity and Ethical Values: The organizational values and behavioral standards at TwinKnowledge are built into the day-to-day activities. Management leads by example and encourages ethical behavior in all aspects of the business. Additionally, management sets an expectation that all employees will conduct themselves honestly and ethically, which is communicated in the employee handbook **(1.1)**. Integrity and ethical values are emphasized during the hiring and onboarding process. In addition, employees each agree through signed agreements that are part of the offer letter to maintain the confidentiality of company and client information and abide by company policies.

Board of Directors and Management Team: A board of directors (the Board) exercises independent oversight of TwinKnowledge's strategic direction, operational performance, and internal control **(1.2)**. The Board consists of individuals who bring experience and expertise needed to direct the Company. The Board meets quarterly to review TwinKnowledge's services, business strategy, financial information, and other items that are related to the organization as a whole. The Board plays an important role in the oversight and governance of the organization. Additionally, there is an all company meeting periodically so that all employees are current on what is happening in the organization.

Management Philosophy and Operating Style: Management understands the importance of oversight and governance and believes this is best accomplished when executives are highly involved in the day-to-day operations of TwinKnowledge. In this environment, management is able to address business issues in a timely manner and consequently reduce risks to the Company and clients. Management and employees meet periodically to discuss system requirements, upcoming changes, and progress against outstanding deadlines.

Organizational Structure: A properly defined organizational structure is critical for operating a sound control environment. TwinKnowledge's organizational structure is formally documented to make sure that employees understand their roles and positioning within the organization **(1.3)**. In addition, lines of authority are established throughout TwinKnowledge. These lines of authority are communicated through management's operational style, the organizational structure, and employee job descriptions. To increase the operational effectiveness of employees within this structure, every position has a job description so that individuals understand their responsibilities **(1.4)**.

New Hires and Terminations: When a position is open at TwinKnowledge, a job description and posting will be created and posted on various job forums and/or LinkedIn by TwinKnowledge with the assistance of outside recruiters. Resumes of applicants are received and reviewed by members of management. Those that pass the initial resume review are invited to participate in a number of interviews based on the position they are applying for. During the interview process and resume review, technical competence is evaluated for applicants applying for technical positions **(1.5)**.

Once an applicant is selected internally, a background screening is performed to validate employment history, education, and reference checks **(1.6)**. If the background screening is passed, an offer letter and employment agreement is sent to the selected applicant. New employees are required to review the TwinKnowledge offer letter, employment agreement, and employee handbook, agreeing to abide by the policies **(1.7)**. As part of the terms of the agreement with individuals, TwinKnowledge maintains the right to discipline or terminate individuals based on a pattern of poor job performance.

Performance reviews are completed for full-time employees on an ongoing basis through one-on-one meetings with each employee's direct supervisor **(1.8)**. Employees meet with their direct supervisor to discuss feedback related to their performance and their fit with the TwinKnowledge culture.

If it is determined that an employee needs to be terminated from TwinKnowledge, an employee exit checklist is filled out to determine that all access is removed and assets are returned. All access is removed within two business days of the employee's last day. See the *Logical and Physical Access* section for further testing on the termination of employees.

Information and Communication

The information and communication component of internal control consists of procedures designed to initiate, authorize, record, process, and report transactions affecting TwinKnowledge's clients. To assist with this aspect of internal control, management has implemented information systems that are used to provide services to clients. Management's ability to conduct operations with efficiency and precision is partially contingent on the timeliness and accuracy of the information management receives from these systems.

Internal Communication: TwinKnowledge maintains internal documentation to communicate responsibilities and system boundaries to TwinKnowledge personnel, which helps them understand their roles within the organization **(2.1)**. These policies highlight important internal controls that strengthen TwinKnowledge's overall control environment. TwinKnowledge's organizational structure defines authorities across the Company to facilitate information flow and establish responsibilities **(2.2)**. See the *Control Environment* section for additional details.

External Communication: TwinKnowledge has created an overview of the TwinKnowledge solutions used to describe the services provided to clients **(2.3)**. This information is available on the TwinKnowledge website.

TwinKnowledge's and client's responsibilities and commitments regarding the acceptable use of the TwinKnowledge solutions are included within the signed agreements with clients **(2.4)**. TwinKnowledge has clients sign an agreement that outlines the terms and conditions between TwinKnowledge and the client. The agreement contains language around topics such as licenses, restrictions, confidentiality, and termination.

Security Awareness Training: To assist with TwinKnowledge's commitments to security and privacy, TwinKnowledge management provides annual security training for employees that covers information security, data protection and confidentiality of client information, and privacy **(2.5)**.

TwinKnowledge provides information to clients and employees on how to report failures, incidents, concerns, or other matters related to the services or systems provided by TwinKnowledge in the event there are problems **(2.6)**. Clients are instructed to contact a TwinKnowledge representative, or they may communicate via email with their TwinKnowledge contact and then set up meetings, if required. TwinKnowledge personnel may contact their manager for important matters requiring attention or use the internal communication tool.

Information pertaining to TwinKnowledge's service commitments, deliverables, and applicable changes are communicated to internal and external users **(2.7)**. Various forms of communication are used when communication is deemed necessary. Methods of delivery include the use of email and coordinated meetings.

Risk Assessment

An organization's risk assessment process is its identification, analysis, and management of risks relevant to the services provided to its clients. It is the responsibility of management and their designees to perform these ongoing risk assessments. Key business and operational risks are closely monitored, particularly those related to the security of TwinKnowledge's production environment, as these are especially critical risks that have the potential to affect the services provided to clients. TwinKnowledge also mitigates business risks by adhering to industry practices to reduce risks related to the system.

TwinKnowledge management periodically evaluates the risks that may affect TwinKnowledge's business operations. TwinKnowledge's risk evaluation is discussed and documented in a risk assessment **(3.1)**. The risk assessment includes security and operational risks associated with the TwinKnowledge environment. Risk mitigation considerations are documented in the risk assessment **(3.2)**. The risk evaluation is updated periodically, and at least annually, to take into consideration relevant changes in TwinKnowledge's operations and relevant technology changes **(3.3)**.

TwinKnowledge policies take into consideration the business, privacy, and IT risks noted within the periodic risk evaluation **(3.4)**. The TwinKnowledge information security policy is detailed and addresses TwinKnowledge internal controls around security. The TwinKnowledge policies have been disseminated within TwinKnowledge and are posted in an internal knowledge base so that personnel know and understand their responsibilities related to information security and privacy, which includes risk management **(3.5)**.

Monitoring Activities

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changing conditions. Management has instituted mechanisms to determine that potential problems within the organization are identified and resolved in a timely manner. TwinKnowledge uses monitoring tools to monitor the production infrastructure, and these monitoring tools alert system administrators when the application is not operating within defined boundaries **(4.1)**.

Application and Infrastructure Logging: TwinKnowledge logs authentication and error events on the production infrastructure **(4.2)**.

Vulnerability Management: TwinKnowledge's vulnerability monitoring keeps up with new threats while validating security controls put in place so that TwinKnowledge's security posture is maintained.

Internal Vulnerability Scanning: TwinKnowledge performs internal vulnerability scanning and package monitoring on a continuous basis **(4.3)**. Production servers are monitored continuously within AWS. The objective of the tests is to identify weaknesses within the TwinKnowledge production infrastructure that could lead to the exposure of sensitive information or result in unauthorized systems access. Management analyzes the results of vulnerability scans and remediates vulnerabilities based on risk **(4.4)**.

Control Activities

TwinKnowledge selects and develops control activities that contribute to the achievement of objectives through mitigating risks to an acceptable level. Control activities included at TwinKnowledge are inclusive of a variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.

Management has established and implemented policies and procedures requiring the performance of periodic assessments and evaluations that consider elements of security as it applies to the AICPA trust services criteria **(5.1)**.

The policies include control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats **(5.2)**. Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary. In addition, management takes corrective action when issues are identified with control activities **(5.3)**.

Logical and Physical Access

Each TwinKnowledge employee and contractor has limited access to TwinKnowledge systems and applications. Access is provisioned on a minimum-necessary (least-privilege) basis. TwinKnowledge has developed a process to register and authorize users prior to being issued system credentials and granted the ability to access the system **(6.1)**.

User Access Administration: TwinKnowledge personnel are granted access to TwinKnowledge systems according to their role and/or team **(6.2)**. If a TwinKnowledge employee or contractor requires access outside of the standard for their role or team, either they or their manager may initiate an access request which must be approved by a member of IT management.

Access Reviews: User access is reviewed on an annual basis **(6.3)**. The review includes the inspection of accounts and their access to the production environment and other critical IT resources. Any changes to access required as a result of the review will be documented in a ticket and updated immediately.

Revocation – Role Changes and Termination: In the case of termination, the former employee or contractor's access is required to be revoked within two business days **(6.4)**. In the case of a role change, the person's access should be revised timely after changing roles. In some cases, access could be revoked as a disciplinary measure for policy violation.

Administrator and Remote Access: Administrator-level access privileges to the production environment are restricted to only those individuals who require such access to perform their respective job functions **(6.5)**. Remote access to critical infrastructure is limited to authorized individuals **(6.6)**.

Access to Client Data: Client data is stored within TwinKnowledge's AWS databases. Access to client data within the TwinKnowledge environment by TwinKnowledge personnel is restricted to authorized users **(6.7)**.

Multifactor Authentication: Strong password requirements and multifactor authentication are configured to access TwinKnowledge's cloud infrastructure **(6.8)**.

Workstation Controls: TwinKnowledge policies and procedures provide guidance to its personnel concerning the physical safeguarding of workstations with access to the IT environment **(6.9)**. Personnel are prohibited from storing sensitive data on removable media (e.g., USB drives, CDs/DVDs, external hard drives) unless explicitly authorized and provided by IT management **(6.10)**.

Inventory of Information Assets: TwinKnowledge maintains an asset inventory listing of its infrastructure and workstations in order to protect them from security events **(6.11)**.

Network Access Rules: Network access rules are configured to block unauthorized traffic into the production environment **(6.12)**. Access to modify network access rules is restricted to authorized individuals **(6.13)**.

Customer Data Segmentation: Customer users have access to their data only and no other customer's data **(6.14)**.

Encryption: TwinKnowledge understands the sensitivity of its clients' data and has therefore implemented security controls to protect the confidentiality of the data. Data transfers between users and the TwinKnowledge system are secured using TLS and industry standard encryption **(6.15)**. Furthermore, client data within the production databases housing sensitive customer data are encrypted at rest **(6.16)**.

Physical Access: TwinKnowledge maintains offices in New York City, USA and Sofia, Bulgaria. Access to TwinKnowledge's offices is limited to current personnel **(6.17)**.

System Operations

Incident Response Program: TwinKnowledge has a documented Incident Response Plan (IRP) which establishes the procedures to be undertaken in response to information security incidents **(7.1)**. TwinKnowledge's IRP outlines the process of identifying, prioritizing, communicating, assigning, and tracking incidents through to resolution. Security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the Company's IRP **(7.2)**. Incident records include a description of the incident and relevant facts (i.e., information that was disclosed) as well as mitigations. The Company tests the IRP at least annually **(7.3)**. Gaps, areas of improvement, and lessons learned are utilized to modify the plan, as needed.

Antivirus and Patching: Malware detection software is installed on user workstations that can access the production environment **(7.4)**. To reduce the risk of compromise, TwinKnowledge applies security patches to user workstations and requires the use of disk encryption **(7.5)**.

Backups: Production data is backed up daily and backups are maintained for seven days **(7.6)**.

Business Continuity / Disaster Recovery Plans: TwinKnowledge has a documented disaster recovery and business continuity (DR/BC) plan and tests it at least annually **(7.7)**. The plan defines procedures and communication protocols in the event of a business disruption.

Complementary User Entity Controls: *User entities are responsible for developing and testing an incident response plan for security incidents that occur within the user entity's environment.*

Complementary User Entity Controls: *User entities are responsible for developing and testing a disaster recovery plan for disaster scenarios that may impact the user entity's environment.*

Change Management

An effective system development and maintenance process is critical to the availability and integrity of TwinKnowledge's solutions. TwinKnowledge follows a defined development process when making changes to systems used to support services provided to clients **(8.1)**.

TwinKnowledge's change management policy applies to production software systems where TwinKnowledge is responsible for the development and/or maintenance of the software system's code base. TwinKnowledge uses a code repository for all software systems to record software development activities **(8.2)**.

Code that is submitted to the code repository must go through a testing and approval process before being deployed into a production environment. Specifically:

- All merge or pull requests require at least one approver other than the developer prior to being merged to production **(8.3)**. TwinKnowledge has defined a limited number of employees who can provide approval for changes.
- All merge or pull requests require an attestation of testing prior to being merged to production **(8.4)**. Attestations are documented and noted in each merge or pull request.

Approvals and documentation of testing are included in the merge request. TwinKnowledge has more than one person involved in every change to help maintain segregation of duties while performing changes **(8.5)**.

TwinKnowledge maintains separate development, testing, and production environments so that a structured change management process is followed **(8.6)**.

Risk Mitigation

Vendor Onboarding: When a potential vendor is identified, there is an onboarding process that is followed to vet the vendor and get the costs approved. Depending on the fees, the budget is submitted and approved by appropriate personnel (management) before the vendor is added.

Vendor Risk Assessments: TwinKnowledge understands that risks exist when engaging in business relationships and, as a result, continuously considers those risks that could potentially affect TwinKnowledge's ability to meet its internal and external business objectives. See the preceding *Risk Assessment* section for additional information on TwinKnowledge's risk assessment process.

Subservice Providers Monitoring: TwinKnowledge uses vendors to assist with elements of security and infrastructure to assist with the services they provide. TwinKnowledge completes an annual review of key vendors that includes obtaining and reviewing each vendor's SOC examination **(9.1)**. The vendor review is completed by IT personnel. TwinKnowledge documents the results of the review, which includes the review of the complementary user entity controls included in the vendor SOC reports **(9.2)**.

(The remainder of this page is left blank intentionally.)

Complementary Subservice Organization Controls (CSOC)

TwinKnowledge's controls related to the AI project intelligence cover only a portion of the overall internal control for each user entity of TwinKnowledge. It is not feasible for the applicable trust services criteria related to the AI project intelligence to be achieved solely by TwinKnowledge. Therefore, each user entity's internal controls must be evaluated in conjunction with TwinKnowledge's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations, described as follows:

	AWS Complementary Subservice Organization Controls	**Related Control Criteria**
1.	AWS is responsible for providing the physical security controls protecting the production servers from unauthorized access.	CC6.4-CC6.5
2.	AWS is responsible for providing the environmental controls protecting the production servers.	CC6.4-CC6.5
3.	AWS is responsible for maintaining the availability of the hosting facility 24/7/365.	CC7.3-CC7.5
4.	AWS is responsible for managing and resolving security and availability incidents related to the data center facility in a timely manner.	CC7.3-CC7.5

(The remainder of this page is left blank intentionally.)

Complementary User Entity Controls (CUEC)

TwinKnowledge's controls related to its AI project intelligence cover only a portion of overall internal control for each user entity of TwinKnowledge. It is not feasible for the applicable trust services criteria related to the AI project intelligence to be achieved solely by TwinKnowledge. Therefore, each user entity's internal controls should be evaluated in conjunction with TwinKnowledge's controls, and the related tests and results described in Section IV of this report, taking into account the related complementary user entity controls identified under each control area, where applicable.

This section highlights additional control activities that TwinKnowledge believes should be considered and/or present at each user entity. Each user entity must evaluate its own system of internal control to determine if the following controls are in place. User auditors should consider whether the following controls have been placed in operation at user organizations:

	Complementary User Entity Controls	**Related Control Criteria**
1.	User entities are responsible for developing and testing an incident response plan for security incidents that occur within the user entity's environment.	CC7.2-CC7.5
2.	User entities are responsible for developing and testing a disaster recovery plan for disaster scenarios that may impact the user entity's environment.	CC7.2-CC7.5

(The remainder of this page is left blank intentionally.)

Section IV – Independent Service Auditor's Description of Tests of Controls and Results

Purpose and Objective of the Independent Auditor's Examination

This report on controls placed in operation and tests of the suitability of the design and operating effectiveness is intended to provide users of the report with information sufficient to obtain an understanding of those aspects of TwinKnowledge's controls that may be relevant to user entities' internal controls. This report, when coupled with an understanding of the internal controls in place at each user entity, is intended to assist in the assessment of the total internal control surrounding TwinKnowledge's AI project intelligence.

Our examination was limited to those controls performed by TwinKnowledge. It is each user entity's responsibility to evaluate this information in relation to the internal controls in place at each user entity to obtain an overall understanding of the internal controls and assess control risk. The portion of controls provided by each user entity and TwinKnowledge must be evaluated together. If effective control activities are not in place at the user entity, TwinKnowledge's controls may not compensate for such weaknesses.

Our examination included inquiries of appropriate management, supervisory, and staff personnel; inspection of documents and records; observation of activities and operations; and tests of controls surrounding TwinKnowledge's AI project intelligence. Our tests of controls were performed for the period of December 1, 2024 to May 31, 2025 and were applied to those controls relating to the applicable trust services criteria.

The description of controls is the responsibility of TwinKnowledge's management. Our responsibility is to express an opinion that the controls are suitably designed and operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the applicable trust services criteria, specified by the AICPA, were achieved for the period of December 1, 2024 to May 31, 2025.

Any exceptions noted by Linford & Company LLP regarding the suitability of the design or operating effectiveness of the controls identified related to the applicable control criteria or the level of compliance with the controls are presented in this section under the caption, "Results of Testing." Concerns identified herein are not necessarily weaknesses in the total system of internal control at TwinKnowledge as this determination can only be made after consideration of controls in place at each client. Complementary user entity controls that should be exercised by clients in order to complement the controls of TwinKnowledge to attain the stated criteria are presented in Section III when considered applicable.

Overview of the Internal Control Environment

Entity-Level Controls

Our examination considered the control environment and included inquiry of appropriate management and staff, inspection of documents and records, and observation of activities and operations. Our examination of the tests of design and operational effectiveness was for the period of December 1, 2024 to May 31, 2025 and was applied to those controls relating to the applicable trust services criteria.

The control environment represents the collective effect of various elements in establishing, enhancing, or mitigating the effectiveness of specified controls. In addition to our review of the controls placed into operation, our procedures included tests of the relevant elements of TwinKnowledge's control environment, including TwinKnowledge's organizational structure and management control methods.

Our evaluation of the control environment included the following procedures, to the extent necessary:

- ✓ *Inspected* TwinKnowledge's organizational structure and noted the segregation of functional responsibilities, personnel policies, and other policies and procedures.
- ✓ *Inquired* through discussion with management personnel responsible for developing, monitoring, and enforcing controls.
- ✓ *Observed* personnel in the performance of their assigned duties.

No exceptions were noted in entity-level testing.

*   *   *   *   *

The results of these procedures were considered in planning the nature, timing, and extent of evaluation procedures around the suitability of the design and operating effectiveness of controls.

Controls Specified by TwinKnowledge, Testing Procedures, and Results of Tests

The following tables include a description of the control activities, testing procedures performed, and results of tests. TwinKnowledge management specified the control activities and the AICPA specified the related control criteria in *Section V – Trust Services Criteria*.

Control Activities Relevant to the Security Criteria

Control Environment

Ref	Controls Specified by TwinKnowledge	Testing Performed by Linford & Company	Results of Testing
1.1	Management sets an expectation that all employees will conduct themselves honestly and ethically, which is communicated in the employee handbook.	*Inspected* the TwinKnowledge employee handbook and noted that it explicitly stated the expectations for employee conduct and integrity was documented as a core value of the organization.	No exceptions noted.
1.2	The Board exercises independent oversight of TwinKnowledge's strategic direction, operational performance, and internal control.	*Inspected* Board meeting minutes and noted that the Board met during the period and included independent oversight.	No exceptions noted.
1.3	TwinKnowledge's organizational structure is formally documented to make sure that employees understand their roles and positioning within the organization.	*Inspected* TwinKnowledge's detailed organizational chart and noted that the chart defined the organizational structure.	No exceptions noted.
1.4	To increase the operational effectiveness of employees within this structure, every position has a job description so that individuals understand their responsibilities.	For a sample of job positions, *inspected* the documented job descriptions and noted that the descriptions correlated with the job role and responsibilities.	No exceptions noted.

Control Environment (continued)

Ref	Controls Specified by TwinKnowledge	Testing Performed by Linford & Company	Results of Testing
1.5	During the interview process and resume review, technical competence is evaluated for applicants applying for technical positions.	*Inspected* the technical assessment questions and noted that a process to evaluate technical competence during the screening and interview process for applicants applying for technical positions was documented.	No exceptions noted.
1.6	Once an applicant is selected internally, a background screening is performed to validate employment history, education, and reference checks.	For a sample of employees hired during the period, *inspected* their background screenings and noted that screenings were completed prior to employment.	No exceptions noted.
1.7	New employees are required to review the TwinKnowledge offer letter, employment agreement, and employee handbook, agreeing to abide by the policies.	For a sample of employees hired during the period, *inspected* their documented sign offs and noted that they signed the required employee acknowledgement documentation.	No exceptions noted.
1.8	Performance reviews are completed for full-time employees on an ongoing basis through one-on-one meetings with each employee's direct supervisor.	For a sample of full-time employees, *inspected* their recurring one-on-one meetings with their supervisor and noted that regular meetings occurred to provide performance feedback.	No exceptions noted.

Information and Communication

Ref	Controls Specified by TwinKnowledge	Testing Performed by Linford & Company	Results of Testing
2.1	TwinKnowledge maintains internal documentation to communicate responsibilities and system boundaries to TwinKnowledge personnel, which helps them understand their roles within the organization.	Through *inspection* of the TwinKnowledge employee handbook, IT Security Policy, and Acceptable Use Policy, noted that the policies communicated employee responsibilities and expectations regarding the functioning of internal control.	No exceptions noted.
2.2	TwinKnowledge's organizational structure defines authorities across the Company to facilitate information flow and establish responsibilities.	*Inspected* the organizational chart and noted that reporting lines and authority were delineated in the chart.	No exceptions noted.
2.3	TwinKnowledge has created an overview of the TwinKnowledge solutions used to describe the services provided to clients.	*Inspected* the TwinKnowledge website and noted that an overview of provided solutions was made available to internal and external users.	No exceptions noted.
2.4	TwinKnowledge's and client's responsibilities and commitments regarding the acceptable use of the TwinKnowledge solutions are included within the signed agreements with clients.	Through *inspection* of a sample client agreement, noted that TwinKnowledge and client acceptable use was documented in the executed agreement.	No exceptions noted.

Information and Communication (continued)

Ref	Controls Specified by TwinKnowledge	Testing Performed by Linford & Company	Results of Testing
2.5	To assist with TwinKnowledge's commitments to security and privacy, TwinKnowledge management provides annual security training for employees that covers information security, data protection and confidentiality of client information, and privacy.	*Inspected* the annual security awareness training materials and noted that security, data protection, and confidentiality were addressed in the training. For a sample of employees and contractors, *inspected* their annual security awareness training attendance records and noted that their training was completed during the period.	No exceptions noted. No exceptions noted.
2.6	TwinKnowledge provides information to clients and employees on how to report failures, incidents, concerns, or other matters related to the services or systems provided by TwinKnowledge in the event there are problems.	*Inspected* the communication methods provided to clients and noted that clients were provided with information on how to report issues to TwinKnowledge. *Inspected* the employee handbook and noted that with the document employees were instructed on who to contact internally if there were issues.	No exceptions noted. No exceptions noted.
2.7	Information pertaining to TwinKnowledge's service commitments, deliverables, and applicable changes are communicated to internal and external users.	*Inspected* a sample client communication and noted that notifications to clients and employees were sent when deemed appropriate or necessary by management.	No exceptions noted.

Risk Assessment

Ref	Controls Specified by TwinKnowledge	Testing Performed by Linford & Company	Results of Testing
3.1	TwinKnowledge’s risk evaluation is discussed and documented in a risk assessment.	*Inspected* the documented risk assessment and noted that TwinKnowledge completed a risk assessment during the period.	No exceptions noted.
3.2	Risk mitigation considerations are documented in the risk assessment.	Through *inspection* of the risk assessment, noted that risk mitigation strategies were documented in the risk assessment.	No exceptions noted.
3.3	The risk evaluation is updated periodically, and at least annually, to take into consideration relevant changes in TwinKnowledge’s operations and relevant technology changes.	*Inspected* the risk assessment and noted that it was updated during the period and took into consideration relevant changes in TwinKnowledge’s operations and relevant technology changes.	No exceptions noted.
3.4	TwinKnowledge policies take into consideration the business, privacy, and IT risks noted within the periodic risk evaluation.	Through *inspection* of the TwinKnowledge policies, noted that TwinKnowledge policies addressed aspects of the risks identified through the risk assessment.	No exceptions noted.
3.5	The TwinKnowledge policies have been disseminated within TwinKnowledge and are posted in an internal knowledge base so that personnel know and understand their responsibilities related to information security and privacy, which includes risk management.	*Inspected* the TwinKnowledge internal knowledge base and noted that policies were available to employees.	No exceptions noted.

Monitoring Activities

Ref	Controls Specified by TwinKnowledge	Testing Performed by Linford & Company	Results of Testing
4.1	TwinKnowledge uses monitoring tools to monitor the production infrastructure, and these monitoring tools alert system administrators when the application is not operating within defined boundaries.	*Inspected* TwinKnowledge's monitoring tools and an example alert and noted that management monitored the production infrastructure and was alerted when the application was outside of defined boundaries.	No exceptions noted.
4.2	TwinKnowledge logs authentication and error events on the production infrastructure.	*Inspected* logging tools and determined that TwinKnowledge logged and monitored events including authentication, availability, and error events.	No exceptions noted.
4.3	TwinKnowledge performs internal vulnerability scanning and package monitoring on a continuous basis.	*Inspected* the vulnerability scanning tools and noted that TwinKnowledge had configured the tools to perform continuous vulnerability scans.	No exceptions noted.
4.4	Management analyzes the results of vulnerability scans and remediates vulnerabilities based on risk.	Through *inspection* of an example vulnerability, noted that management addressed vulnerabilities based on risk.	No exceptions noted.

Control Activities

Ref	Controls Specified by TwinKnowledge	Testing Performed by Linford & Company	Results of Testing
5.1	Management has established and implemented policies and procedures requiring the performance of periodic assessments and evaluations that consider elements of security as it applies to the AICPA trust services criteria.	*Inspected* the policies and procedures and noted that they provided direction regarding the performance of assessments and evaluations over security which included risk assessments, vulnerability scanning, and access reviews.	No exceptions noted.
5.2	The policies include control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.	*Inspected* TwinKnowledge's information security policy and noted that it included control activities designed to restrict access to authorized individuals only with access commensurate to job duties. *Inspected* the policy document repository location and noted that the policies were available to company personnel.	No exceptions noted. No exceptions noted.
5.3	Management takes corrective action when issues are identified with control activities.	*Inspected* internal communication regarding an example control issue identified during the period and noted that management took corrective action as necessary to resolve the issue.	No exceptions noted.

Logical and Physical Access

Ref	Controls Specified by TwinKnowledge	Testing Performed by Linford & Company	Results of Testing
6.1	TwinKnowledge has developed a process to register and authorize users prior to being issued system credentials and granted the ability to access the system.	*Inspected* TwinKnowledge's onboarding procedure and information security policy and noted that the policy and procedure specified the process for being granted system access and that personnel were granted access to systems with a minimum access necessary approach.	No exceptions noted.
6.2	TwinKnowledge personnel are granted access to TwinKnowledge systems according to their role and/or team.	For a sample of new hires during the period, *inspected* access provisioning tickets and noted that access was granted according to the person's role or team.	No exceptions noted.
6.3	User access is reviewed on an annual basis.	*Inspected* the latest access review and noted that the review was performed during the period and the results of the review were documented.	No exceptions noted.
6.4	In the case of termination, the former employee or contractor's access is required to be revoked within two business days.	Through *inquiry* of management, noted that access for terminated users must be removed within two business days. *Inquired* of management and noted that no employee or contractor terminations had occurred during the period.	No exceptions noted. Non-occurrence: Since no terminations took place during the period, we were unable to test the operating effectiveness of this control.

Logical and Physical Access (continued)

Ref	Controls Specified by TwinKnowledge	Testing Performed by Linford & Company	Results of Testing
6.5	Administrator-level access privileges to the production environment are restricted to only those individuals who require such access to perform their respective job functions.	For all users with administrator-level access to the production environment, *inspected* user listings and the personnel listing and determined that each user was a current employee or contractor with a role that appeared to align with their access.	No exceptions noted.
		Inquired of management and ascertained that administrator access was appropriate.	No exceptions noted.
6.6	Remote access to critical infrastructure is limited to authorized individuals.	For a sample of users with remote access to critical infrastructure, *inspected* user listings and the personnel listing and determined that each user's access appeared to align with their job function.	No exceptions noted.
		Inquired of management and ascertained that remote access was appropriate	No exceptions noted.
6.7	Access to client data within the TwinKnowledge environment by TwinKnowledge personnel is restricted to authorized users.	For users with access to client data in the TwinKnowledge environment, *inspected* user listings and HR lists and determined that each user's access appeared to align with their job functions.	No exceptions noted.
		Inquired of management and ascertained that access to client data was appropriate.	No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by TwinKnowledge	Testing Performed by Linford & Company	Results of Testing
6.8	Strong password requirements and multifactor authentication are configured to access TwinKnowledge's cloud infrastructure.	*Inspected* password configurations and noted that strong password requirements and multifactor authentication were required for authentication to the cloud infrastructure.	No exceptions noted.
6.9	TwinKnowledge policies and procedures provide guidance to its personnel concerning the physical safeguarding of workstations with access to the IT environment.	*Inspected* TwinKnowledge's acceptable use policy and noted that it specified that company personnel were responsible for protecting workstations and promptly reporting any loss or theft.	No exceptions noted.
6.10	Personnel are prohibited from storing sensitive data on removable media (e.g., USB drives, CDs/DVDs, external hard drives) unless explicitly authorized and provided by IT management.	*Inspected* TwinKnowledge's information security policy and noted that per policy, personnel were prohibited from storing sensitive data on removable media.	No exceptions noted.
6.11	TwinKnowledge maintains an asset inventory listing of its infrastructure and workstations in order to protect them from security events.	*Inspected* the asset inventory listing and determined that TwinKnowledge devices were tracked.	No exceptions noted.
6.12	Network access rules are configured to block unauthorized traffic into the production environment.	*Inspected* network access rules and noted that the production infrastructure was configured to block unauthorized traffic into TwinKnowledge's production environment.	No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by TwinKnowledge	Testing Performed by Linford & Company	Results of Testing
6.13	Access to modify network access rules is restricted to authorized individuals.	For all users with access to modify network access rules, *inspected* user listings and the personnel listing and determined that each user was a current employee or contractor with a role that appeared to align with their access. *Inquired* of management and noted that their access was commensurate with their responsibilities.	No exceptions noted. No exceptions noted.
6.14	Customer users have access to their data only and no other customer's data.	*Inspected* the production infrastructure and noted that customers had access to their data only and no other customers' data.	No exceptions noted.
6.15	Data transfers between users and the TwinKnowledge system are secured using TLS and industry-standard encryption.	*Inspected* third-party security reports and certificate information and determined that data transfers between users and TwinKnowledge used TLS 1.3 and industry-standard encryption.	No exceptions noted.
6.16	Client data within the production databases housing sensitive customer data are encrypted at rest.	*Inspected* configurations for the production databases and noted they were encrypted at rest.	No exceptions noted.
6.17	Access to TwinKnowledge's offices is limited to current personnel.	For a sample of people with physical access to TwinKnowledge's offices, *inspected* HR records and determined that access was limited to current employees and contractors.	No exceptions noted.

System Operations

Ref	Controls Specified by TwinKnowledge	Testing Performed by Linford & Company	Results of Testing
7.1	TwinKnowledge has a documented IRP which establishes the procedures to be undertaken in response to information security incidents.	*Inspected* the IRP and noted that it detailed procedures for incident response and specified roles and responsibilities in the event of a security incident.	No exceptions noted.
7.2	Security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the Company's IRP.	*Inquired* of management and noted that no security incidents had been identified during the period. *Inspected* the ticketing system and noted that no security incidents were recorded. For an example operational incident, *inspected* incident documentation and determined that incidents were tracked to resolution.	No exceptions noted. No exceptions noted. No exceptions noted.
7.3	The Company tests the IRP at least annually.	*Inspected* test documentation from the last test of the IRP and noted that the IRP was tested during the period.	No exceptions noted.
7.4	Malware detection software is installed on user workstations that can access the production environment.	For a sample of active personnel, *inspected* the software installed on their workstations and noted that malware detection software was installed on each workstation selected.	No exceptions noted.

System Operations (continued)

Ref	Controls Specified by TwinKnowledge	Testing Performed by Linford & Company	Results of Testing
7.5	To reduce the risk of compromise, TwinKnowledge applies security patches to user workstations and requires the use of disk encryption.	For a sample of active personnel during the period, *inspected* the OS version on each workstation and noted that the workstation had been patched to the current operating system. For a sample of active personnel during the period, *inspected* workstation configurations and noted that each was protected with disk encryption.	No exceptions noted. No exceptions noted.
7.6	Production data is backed up daily and backups are maintained for seven days.	*Inspected* backup configurations and determined that backups were configured to occur daily and maintained for seven days.	No exceptions noted.
7.7	TwinKnowledge has a documented DR/BC plan and tests it at least annually.	*Inspected* the DR/BC plan and determined that the Company had formally documented its business continuity and disaster recovery plan. *Inspected* the most recent DR/BC test and noted that the plan had been tested during the period.	No exceptions noted. No exceptions noted.

Change Management

Ref	Controls Specified by TwinKnowledge	Testing Performed by Linford & Company	Results of Testing
8.1	TwinKnowledge follows a defined development process when making changes to systems used to support services provided to clients.	*Inspected* the documented change management procedures and noted that TwinKnowledge followed a defined development process for making changes to TwinKnowledge products.	No exceptions noted.
8.2	TwinKnowledge uses a code repository for all software systems to record software development activities.	*Inspected* a sample of changes made during the period and noted that a code repository tool was used to record information pertaining to the change life cycle.	No exceptions noted.
8.3	All merge or pull requests require at least one approver other than the developer prior to being merged to production.	*Inspected* the branch restrictions in the code repository and noted that a separate approval was required for a merge to production.	No exceptions noted.
8.4	All merge or pull requests require an attestation of testing prior to being merged to production.	*Inspected* a sample of changes made during the period and noted that the changes were tested prior to being merged to production.	No exceptions noted.
8.5	TwinKnowledge has more than one person involved in every change to help maintain segregation of duties while performing changes.	For a sample of changes during the period, *inspected* the change support and noted that more than one person was involved in the changes.	No exceptions noted.
8.6	TwinKnowledge maintains separate development, testing, and production environments so that a structured change management process is followed.	*Inspected* environment configurations and noted that separate environments existed to develop and test the changes prior to merging to production.	No exceptions noted.

Risk Mitigation

Ref	Controls Specified by TwinKnowledge	Testing Performed by Linford & Company	Results of Testing
9.1	TwinKnowledge completes an annual review of key vendors that includes obtaining and reviewing each vendor's SOC examination.	*Inspected* the completed key vendor review and noted that TwinKnowledge completed an annual review of its key vendor's SOC report to establish that it had been monitored during the period.	No exceptions noted.
9.2	TwinKnowledge documents the results of the review, which includes the review of the complementary user entity controls included in the vendor SOC reports.	Through *inspection* of the completed vendor review, noted that TwinKnowledge was monitoring the complementary user entity controls noted by the key subservice organization in their SOC report.	No exceptions noted.

Section V – Trust Services Criteria

The TwinKnowledge management team is responsible for establishing and maintaining effective controls over its AI project intelligence. The controls are designed to provide reasonable assurance to TwinKnowledge management and the board of directors that the following SOC 2 security criteria were achieved.

In the table that follows, the columns have the following meaning:

> **SOC 2 Criteria** – This column contains, for each criterion evaluated, the reference citation. Each criterion sources from a requirement of the trust services criteria.
>
> **Requirement(s)** – This column contains the text of the criterion (requirement) directly from the trust services criteria.
>
> **Reference** – This column contains the reference to the control activities in *Section III – TwinKnowledge's Description of Its AI Project Intelligence,* which are relevant to the achievement of the criterion.

The purpose of this table is to demonstrate that all SOC 2 control criteria in scope were assessed and that the control activities described in *Section III – TwinKnowledge's Description of Its AI Project Intelligence,* address the SOC 2 control criteria.

Many of the criteria used to evaluate a system are shared amongst all of the criteria. For example, the criteria related to risk management apply to the security, availability, processing integrity, confidentiality, and privacy criteria. As a result, the criteria for the security criteria are organized into the criteria that are applicable to all five criteria (common criteria). The common criteria (CC1.0 through CC9.0 in the tables that follow) constitute the complete set of criteria for the security criteria.

Common/Security Criteria

Security. Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives.

Security refers to the protection of:

i. information during its collection or creation, use, processing, transmission, and storage and
ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft, or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CC1.0 Common Criteria Related to Control Environment

SOC 2 Criteria	Requirement(s)	Reference
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	1.1
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	1.2
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	1.3-1.4

CC1.0 Common Criteria Related to Control Environment (continued)

SOC 2 Criteria	Requirement(s)	Reference
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	1.5-1.7
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	1.8

CC2.0 Common Criteria Related to Information and Communication

SOC 2 Criteria	Requirement(s)	Reference
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	2.1
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	2.1-2.2, 2.5-2.7
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	2.3-2.4, 2.6-2.7

CC3.0 Common Criteria Related to Risk Assessment

SOC 2 Criteria	Requirement(s)	Reference
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	3.1-3.5
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	3.1-3.3
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	3.1-3.5
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	3.1-3.5

CC4.0 Common Criteria Related to Monitoring Activities

SOC 2 Criteria	Requirement(s)	Reference
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	4.1-4.4
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	4.4

CC5.0 Common Criteria Related to Control Activities

SOC 2 Criteria	Requirement(s)	Reference
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	5.1-5.3
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	5.1-5.3
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	5.1-5.3

CC6.0 Common Criteria Related to Logical and Physical Access

SOC 2 Criteria	Requirement(s)	Reference
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity’s objectives.	6.1-6.17
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	6.2, 6.5-6.6

CC6.0 Common Criteria Related to Logical and Physical Access (continued)

SOC 2 Criteria	Requirement(s)	Reference
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	6.2-6.7
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	6.9-6.10, 6.17
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	6.3-6.4
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	6.8, 6.10, 6.12-6.13, 6.15-6.16
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	6.15-6.16
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	6.10-6.13, 7.4

CC7.0 Common Criteria Related to System Operations

SOC 2 Criteria	Requirement(s)	Reference
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	7.1-7.7
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	4.1-4.4, 7.2, 7.4
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	7.1-7.3
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	7.1-7.2
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	7.5-7.7

CC8.0 Common Criteria Related to Change Management

SOC 2 Criteria	Requirement(s)	Reference
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	8.1-8.6

CC9.0 Common Criteria Related to Risk Mitigation

SOC 2 Criteria	Requirement(s)	Reference
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	9.1-9.2
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	9.1-9.2