collation.ai

Collation.AI, Inc.

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

Description of Collation.AI platform relevant to the Trust Services Criteria of Security, Availability, Confidentiality, Privacy and Processing Integrity

September 1, 2024 through August 31, 2025

STATEMENT OF CONFIDENTIALITY

This report, including the Description of tests of controls and results thereof in Section 4, is intended solely for the information and use of the Service Organization, User Entities of the Service Organization's system related to Collation.AI services relevant to the Security, Availability, Confidentiality, Privacy and Processing Integrity during some or all of the period September 1, 2024 through August 31, 2025, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties. Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITORS' REPORT

1 INDEPENDENT SERVICE AUDITORS' REPORT

To the management of Collation.AI

Scope

We have examined the description of the system provided by Management of Collation.AI, Inc., (the "Service Organization" or "Collation.AI") included in Section 3, "Description of Systems Provided by Service Organization" of its Collation.AI Services throughout the period September 1, 2024 through August 31, 2025 (the "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, in AICPA Description Criteria, ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period September 1, 2024 through August 31, 2025, to provide reasonable assurance that Collation.AI's service commitments and system requirements would be achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, Processing Integrity and Privacy (applicable trust services criteria) set forth in TSP section 100, 2017 AICPA Trust Services Criteria.

Collation.AI uses Azure ("subservice organization") as a cloud service provider. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Collation.AI, to achieve Collation.AI's service commitments and system requirements based on the applicable trust services criteria. The Description presents Collation.AI's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Collation.AI'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 Collation.AI, to achieve Collation.AI' service commitments and system requirements based on the applicable trust services criteria. The Description presents Collation.AI' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Collation.AI' controls. 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.

Service Organization's Responsibilities

Management of Collation.AI 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 Collation.AI service commitments and system requirements would be achieved. Management of Collation.AI has provided the accompanying assertion in Section 2 titled, "Management Assertion Provided by Collation.AI" (the "Assertion") about the Description and the suitability of the design and operating effectiveness of controls stated therein. Management of Collation.AI 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 the 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 operating effectively to provide reasonable assurance that the Collation.AI's service commitments and system requirements would be 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.

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

- Obtaining an understanding of the system and the 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 would achieve its service commitments and system requirements based the applicable trust services criteria.
- Testing the operating effectiveness of those controls stated in the Description to provide reasonable assurance that Collation.AI 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.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA. We have complied with those requirements. We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of report users and therefore may not include every aspect of the system that each individual report user may consider important to meet their informational needs.
There are inherent limitations in 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 tested, and the nature, timing, and results of those tests are listed in Section 4, "Information Provided by the Service auditor: Test of controls".

Opinion

In our opinion, in all material respects:

a) The Description presents Collation.AI's system that was designed and implemented throughout the period September 1, 2024 through August 31, 2025, in accordance with the description criteria.

b) The controls stated in the Description were suitably designed throughout the period September 1, 2024 through August 31, 2025, to provide reasonable assurance that Collation.AI'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 Collation.AI's controls throughout that period.

c) The controls stated in the Description operated effectively throughout the period September 1, 2024 through August 31, 2025, to provide reasonable assurance that Collation.AI's service commitments and system requirements would be achieved based on the applicable trust services criteria, and if the subservice organization and user entities applied the complementary controls assumed in the design of Collation.AI's controls operated effectively throughout that period.

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 management of Collation.AI, user entities of Collation.AI platform during some or all of the period September 1, 2024 through August 31, 2025, business partners of Collation.AI subject to risks arising from interactions with the Collation.AI's system, 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 Collation.AI.
- How Collation.AI'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 they interact with related controls at Collation.AI to achieve Collation.AI's commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use Collation.AI's services.
- The applicable trust services criteria.

- The risks that may threaten the achievement of Collation.AI'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.

Accorp Partners CPA LLC

ACCORP PARTNERS CPA LLC
License No.: PAC-FIRM-LIC-47383
Date: October 3, 2025
Kalispell, Montana

SECTION 2

MANAGEMENT'S ASSERTION PROVIDED BY SERVICE ORGANIZATION

collation.ai

MANAGEMENT ASSERTION PROVIDED BY Collation.AI, Inc.

For the period from September 1, 2024 to August 31, 2025

We have prepared the accompanying System Description Provided by Service Organization (Description) of Collation.AI, Inc. (the "Service Organization" or "CollationAI") in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria). The Description is intended to provide report users with information about the CollationAI Platform and services (System) that may be useful when assessing the risks arising from interactions with the System throughout the period September 1, 2024 to August 31, 2025, particularly information about system controls that the Service Organization 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, Availability and Confidentiality, Privacy and Processing Integrity (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.

CollationAI uses Azure (Microsoft Cloud) ("subservice organization"). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at CollationAI, to achieve CollationAI's service commitments and system requirements based on the applicable trust services criteria. The description presents CollationAI's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of CollationAI controls. The description does not disclose the actual controls at the subservice organization. The description does not extend to controls of the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at CollationAI, to achieve CollationAI's service commitments and system requirements based on the applicable trust services criteria. The description presents CollationAI's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of CollationAI's controls. The description does not extend to controls of the user entities.

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

a. The description presents the System that was designed and implemented throughout the period September 1, 2024 to August 31, 2025 in accordance with the description Criteria.

b. The controls stated in the description were suitably designed throughout the period September 1, 2024 to August 31, 2025, to provide reasonable assurance that CollationAI'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 organizations and user entities applied the complementary controls assumed in the design of CollationAI's controls throughout that period.

collation.ai

c. The controls stated in the description operated effectively throughout the period September 1, 2024 to August 31, 2025, to provide reasonable assurance that CollationAI's service commitments and system requirements were achieved based on the applicable trust services criteria, if the subservice organizations and user entities applied the complementary controls assumed in the design of CollationAI's controls operated effectively throughout that period.

For Collation.AI, Inc.

DocuSigned by:
Tanmai Sharma
87062074921248D...

Name: Tanmai Sharma
Title: CEO
Date: 3rd Oct 2025

SECTION 3

DESCRIPTION OF THE SYSTEM

3 DESCRIPTION OF SYSTEMS PROVIDED BY THE SERVICE ORGANIZATION

3.1 Overview of service organization and in-scope services

Company Overview

Collation.AI, Inc. (“Collation.AI”) is a is a SaaS based platform designed to revolutionize the way Wealth Managers, High Net Worth Individuals (HNIs), and Family offices handle their investment data and reporting needs

Company Details

Headquarters: Collation.AI, Inc., 263 Tresser Blvd Floor 9, Stamford, CT 06901 United States Tel: +1347449 4818
Industry: Software Development in Private Wealth
Experience: 2+ years in the industry
Employee Count: 20-25 (estimated)
Cloud Infrastructure: Azure (Microsoft Cloud)

Leadership Team

Tanmai Sharma - Founder & Chief Executive Officer (CEO)

Tanmai serves as the Founder and CEO of Collation.AI, overseeing business strategy, leadership, and vision. He drives the company's growth initiatives, strategic partnerships, and ensures alignment with long-term organizational goals. His leadership focuses on defining strategic direction, leading the executive team, driving partnerships and product vision, and managing investor relations while maintaining the company's financial health.

Leadership Philosophy: As a visionary leader, Tanmai is passionate about leveraging AI and technology to transform business operations, continuously seeking opportunities to drive innovation in the professional services industry. His leadership has been instrumental in establishing Collation.AI as a trusted technology partner while scaling operations globally.

Prashant Surana - Chief Technology Officer (CTO)

Prashant serves as the CTO, overseeing day-to-day Tech and Product roadmaps and operations, ensuring efficient strategy execution. He manages Product, Tech and operations, aligning processes with business goals and ensuring operational efficiency across the organization. His comprehensive approach to technology and operations has been fundamental in building Collation.AI's technical capabilities and platform offerings.

Shamara Pareira - Chief Product Officer (CPO)

Shamara serves as the CPO, leading Collation.AI's product roadmap, operational expansion and client account operations. She drives product growth strategies, manages client relationships, and ensures successful delivery of services. Her leadership has been pivotal in establishing Collation.AI's presence in the US market and building strategic partnerships with enterprise clients across the region.

Amit Prakash – Chief Information Security Officer (CISO)

Amit Prakash serves as the Chief Information Security Officer, overseeing the company’s security and

compliance programs. He is responsible for developing and implementing the organization's information security strategy, ensuring alignment with business objectives, and maintaining trust with clients and partners. Amit leads risk management, data protection, and governance initiatives across all operations. His leadership has been instrumental in strengthening the company's security posture and fostering a culture of security awareness and compliance excellence.

Core Services and Specializations

Primary Service Areas

Collation.AI delivers comprehensive data automation solutions through four specialized service categories, combining advanced AI Bot technology with deep financial services expertise and scalable data infrastructure.

1. Agentic AI Bot Solutions

Collation.AI provides a full spectrum of AI-powered data automation services designed to transform how wealth managers leverage their existing technology investments.

Data Extraction Bot: Automated data extraction from any source including CRMs, PDFs, custodian portals, and protected systems. Unlock trapped data across your entire technology stack without manual intervention.

Data Scrubbing Bot: Intelligent data reconciliation and cleansing that ensures consistency and reliability. Our Bot solves for data quality issues within individual systems and across multiple platforms, eliminating errors and inconsistencies.

Centralized Data Warehouse Bot: Creation and management of a single source of truth with unlimited access to unified data from all your technology systems. Monitor client relationships, predict retention patterns, and enable proactive client management.

Automated Workflows Bot: Intelligent automation across your existing technology stack. Recruit new financial advisors to join your RIA with a future-proof "AI ready" scalable, open platform.

Analytics Calculator Bot: Customizable financial calculations at scale. Simply bolt on top of your existing tech stack (e.g., accounting software). Smart analytics help wealth managers better understand client behaviors and needs, enabling more effective marketing and sales strategies.

AI Chatbot: Conversational interface to your data. Ask questions naturally to get instant and in-depth answers, eliminating the need to download canned reports from online portals.

2. Managed Services and Support

Our ongoing operational support ensures organizations maintain optimal data infrastructure performance and data quality:

Managed Data Services: Comprehensive AI-powered management of your data warehouse including regular data quality monitoring, performance optimization, system maintenance, and continuous improvement. The team acts as an extension of your IT department, ensuring your data infrastructure runs smoothly and evolves with business needs.

Data Infrastructure Assessment & Analysis: Detailed evaluation of existing technology stack and data workflows to identify optimization opportunities, technical debt, data quality vulnerabilities, and integration bottlenecks.

We provide actionable roadmaps for improving data accessibility, system efficiency, and overall operational effectiveness.

3. Strategic Advisory

Strategic consulting services to guide wealth management organizations in their AI and data transformation journey:

AI & Automation Strategy Consulting: Strategic advisory services focused on helping wealth managers leverage AI for operational transformation. We develop comprehensive AI adoption strategies, identify high-impact automation use cases, and create implementation roadmaps that align AI initiatives with business objectives while ensuring data security and regulatory compliance.

Business Transformation Advisory: Guidance on leveraging data and automation technology to transform business processes, reduce operational costs, and drive growth. Our consultants work closely with leadership teams to align technology initiatives with strategic business goals and scalability requirements.

4. Data Infrastructure Platform

Collation.AI's proprietary data infrastructure revolutionizes wealth management operations through AI-powered automation:

End-to-End Data Automation: Our platform serves as an AI-powered solution that transforms how wealth managers aggregate, process, and analyze financial data. The platform integrates seamlessly with existing technology stacks—no changes required—and delivers insights through centralized data warehouses and intelligent analytics dashboards.

Target Industries

Wealth Management Focus

Collation.AI specializes in serving the wealth management industry, addressing the unique data challenges faced by firms managing client assets and relationships.

Registered Investment Advisors (RIAs)

RIAs face significant challenges with disconnected data across multiple systems, wasting an average of 3 hours per day on data aggregation. Collation.AI helps RIAs recruit new financial advisors by providing a future-proof, scalable tech stack while reducing operational overhead. Our solutions enable 5x faster client onboarding and save on average 15 hours per week on mundane workload.

Family Offices (FOs)

Family Offices struggle with overpriced performance reporting software and fragmented Excel spreadsheets despite having robust general ledger systems. Collation.AI overlays affordable reporting and analytics software on existing GL systems, eliminating the need for expensive standalone solutions while providing comprehensive insights across all holdings.

External Asset Managers (EAMs)

External Asset Managers spend up to 15 hours per week on repetitive data entry and processing. Manual data management causes on average 2 weeks of delays for preparing reports. Collation.AI automates data workflows across portfolio management systems, CRM platforms, and alternative investment platforms, dramatically reducing processing time and eliminating manual errors.

Multi-Family Offices and Private Banks

Organizations managing complex client relationships across multiple custodians, asset classes, and reporting requirements benefit from Collation.AI's centralized data warehouse approach. Our platform enables consistent reporting, predictive client retention analytics, and unified views across all client portfolios and relationships.

Technology and Capabilities

Core Technology Infrastructure

Collation.AI's technology stack combines cutting-edge AI capabilities with enterprise-grade data infrastructure:

AI-Powered Data Extraction

Multi-Source Integration: Our technology extracts data from any source including CRMs, portfolio management systems, custodian portals, PDFs, protected systems, and legacy platforms. We utilize the best tool for each job—APIs, intelligent bots, web scraping, and custom integrations.

Automated Processing: Data flows into your centralized warehouse within 1-3 business days after initial setup, with ongoing automated synchronization eliminating manual data entry and reducing operational overhead.

Data Quality and Reconciliation

Intelligent Cleansing: Our AI bots automatically reconcile, cleanse, and ensure data consistency across all systems. We solve for data quality issues within individual platforms and across multiple systems, identifying and correcting discrepancies in real-time.

Cross-System Validation: Advanced reconciliation algorithms verify data accuracy across portfolio management systems, accounting software, CRM platforms, and custodian feeds, ensuring audit-ready data quality.

Centralized Data Warehouse

Flexible Deployment: Your data warehouse can be hosted on your cloud infrastructure or Collation.AI's secure cloud environment. Setup takes just 5 minutes, with full data population within 5-10 business days.

Unlimited Access: Single source of truth providing unlimited access to copies of your data from all technology systems, enabling comprehensive reporting and analytics without impacting production systems.

Scalable Architecture: Platform effortlessly manages and processes vast amounts of data, accommodating growing asset bases, client counts, and data complexity without infrastructure changes.

Analytics and Insights

Customizable Calculations: Financial calculations at scale, configured to your specific methodologies and reporting requirements. Analytics bolt on top of existing technology stacks without requiring system replacements.

Predictive Analytics: Monitor client relationships, predict retention patterns, understand client behaviors and needs, enabling proactive relationship management and more effective marketing strategies.

Real-Time Dashboards: Immediate access to critical information through online dashboards, enabling faster responses to market changes and eliminating 2-week delays in report preparation.

Security and Compliance

SOC 2 Certified: Collation.AI meets international information security standards with SOC 2 certification, ensuring enterprise-grade data protection and security controls.

Data Privacy: All engagements include NDA protection, with strict data access controls and encryption standards. Client data remains confidential and secure throughout the engagement lifecycle.

Company Philosophy and Approach

Our Mission

We solve data headaches for wealth managers by reducing operational costs and improving workflow efficiencies through AI-powered automation that works seamlessly with existing technology investments.

No-Change Integration Philosophy

Zero Disruption: We don't change or break anything in your existing tech stack. All automation and intelligence happen in the data warehouse layer, allowing you to maintain current systems while gaining advanced capabilities.

Leverage Existing Investments: Rather than requiring expensive platform replacements, Collation.AI enhances what you already have, maximizing ROI on existing technology while adding modern AI capabilities.

Risk-Free Approach

$0 Proof of Concept: Free proof of concept with no changes to your infrastructure, no specialized headcount requirements, and no financial risk. The PoC is quick, effortless, and demonstrates value before any commitment.

100% Free If It Doesn't Work: We stand behind our solutions with a complete money-back guarantee. If our platform doesn't deliver the promised value, there's no charge.

Predictable Pricing: Flat fee structure with no surprises. Our solutions cost less than a quarter of a full-time hire while delivering significantly more value.

Human-Centered Automation

Expert Support: While we leverage AI extensively, human expertise guides every implementation. Our team works closely with your leadership and operations teams to ensure successful adoption and ongoing optimization.

Specialized Expertise: No specialized headcount required on your side. We bring the technical expertise, implementation experience, and ongoing support, acting as an extension of your team.

Speed and Efficiency

Rapid Deployment: Data warehouse creation in 5 minutes, data flowing within 1-3 days, and initial insights visible within 5-10 business days. Our proven implementation methodology ensures fast time-to-value.

Immediate Impact: Save on average 15 hours per week on mundane workload, eliminate 3 hours per day wasted on data aggregation, and avoid 2 weeks of unnecessary delays in report preparation.

Industry Position

Market Differentiation

Collation.AI occupies a unique position in the wealth management technology landscape, combining AI automation with practical, implementation-focused solutions.

Proven Results

20+ Wealth Manager Clients: Serving RIAs, Family Offices, and External Asset Managers across multiple locations with demonstrated success in automating complex data workflows.

Measurable Impact: Clients experience 5x faster client onboarding, 200% year-over-year growth in client engagement, 32% reduction in infrastructure costs, and save 2/3 on staff salaries compared to manual approaches.

Industry Recognition: Featured in leading financial technology publications and recognized for innovative approaches to wealth management data challenges.

Competitive Advantages

AI-First Architecture: Unlike legacy data aggregation tools, Collation.AI is built from the ground up with AI automation at its core. Our agentic AI bots operate autonomously, continuously improving through machine learning.

No Technology Replacement Required: Most competitors force expensive platform migrations. Collation.AI works with your existing systems, eliminating migration risk and preserving technology investments.

Cost Efficiency: Wealth Managers spend USD 60K per annum more building in-house tech stacks versus outsourcing to Collation.AI. Our flat-fee pricing model delivers enterprise capabilities at a fraction of the cost of alternatives.

Speed to Value: While traditional data warehouse projects take months, Collation.AI delivers working solutions in days. Our proven methodology and pre-built integrations accelerate time-to-value dramatically.

Technology Leadership

Advanced AI Capabilities: Leveraging latest agentic AI technologies that autonomously extract, cleanse, reconcile, and analyze data across complex wealth management ecosystems.

Flexible Integration: Support for APIs, web scraping, bot automation, and custom integrations ensures connectivity to any system, regardless of age or API availability.

Conversational Analytics: AI chatbot interface allows natural language queries against your data, eliminating the need for technical expertise or pre-built report templates.

Client-Centric Engagement Model

Free Consultation: 30-minute consultation with Agentic AI Bot experts to understand specific challenges and recommend optimal solutions from our bot library.

Proof of Concept First: Risk-free POC demonstrates value before any financial commitment, building confidence and ensuring solution fit.

Ongoing Partnership: Managed services model provides continuous optimization, performance monitoring, and evolution as business needs change.

Security and Compliance Leadership

SOC 2 Certified: Meeting international information security standards provides enterprise clients with confidence in data protection and security controls.

Audit-Ready Data: Benefit from accurate and readily auditable data, ensuring regulatory compliance and informed decision-making across all client relationships.

3.2 Principal Service Commitments and System Requirements

Collation.AI designs its processes and procedures to meet objectives for its software application. Those objectives are based on the service commitments that Collation.AI makes to customers and the compliance requirements that Collation.AI has established for their services.

Security commitments to user entities are documented and communicated in Collation.AI's customer agreements, as well as in the description of the service offering provided online. Collation.AI's security commitments are standardized and based on some common principles.

As a SOC 2 compliant organization, Collation.AI (Collation.AI, Inc.) demonstrates its commitment to maintaining the highest standards of security, availability, processing integrity, confidentiality, and privacy in all aspects of professional services, consulting engagements and software development. Our comprehensive approach to these trust criteria ensures that client data and systems are protected, reliable, and handled with the utmost care is as below:

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

- **Access Controls and Authentication:** Implementation of multi-factor authentication, role-based access controls, and regular access reviews to ensure only authorized personnel can access systems and data
- **Network Security:** Deployment of firewalls, intrusion detection systems, and network segmentation to protect against unauthorized access and cyber threats
- **Vulnerability Management:** Regular security assessments, penetration testing, and timely patching of systems to address identified vulnerabilities
- **Security Incident Response:** Established procedures for detecting, responding to, and recovering from security incidents, including notification protocols for affected parties
- **Employee Security Training:** Ongoing security awareness training for all staff members to ensure understanding of security policies and procedures
- **Physical Security:** Secure facilities with controlled access, surveillance systems, and environmental controls to protect physical assets and infrastructure
- **Third-Party Security:** Security assessments of vendors and service providers to ensure they meet our security standards before engagement

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

- **System Performance and Availability Monitoring:** Continuous monitoring mechanisms to help ensure the consistent delivery of the system and its components, including real-time alerts for performance degradation
- **Timely Customer Response:** Responding to customer requests in a reasonably timely manner through established service level agreements and support channels
- **Business Continuity and Disaster Recovery:** Comprehensive plans that are tested on a periodic basis to ensure rapid recovery and continuation of critical business operations
- **Operational Procedures:** Well-documented procedures supporting the achievement of availability commitments to user entities, including maintenance schedules and change management processes
- **Redundancy and Backup Systems:** Implementation of redundant systems and regular backup procedures to minimize service interruptions and ensure data recovery capabilities
- **Capacity Planning:** Regular assessment and planning for system capacity to accommodate growth and peak demand periods
- **Infrastructure Maintenance:** Scheduled maintenance windows and proactive hardware/software updates to prevent system failures

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

- **Encryption Technologies:** The use of industry-standard encryption technologies to protect system data both at rest and in transit, ensuring sensitive information remains secure during storage and transmission
- **Confidentiality and Non-Disclosure Agreements:** Comprehensive agreements with employees, contractors, and third parties to legally bind all parties to maintain confidentiality of sensitive information
- **Purpose Limitation:** Confidential information must be used only for the purposes explicitly stated in agreements between Collation.AI and user entities, with strict controls preventing unauthorized use
- **Data Classification and Handling:** Clear classification of confidential information and corresponding handling procedures to ensure appropriate protection levels are applied
- **Secure Disposal:** Secure destruction of confidential information when no longer needed, following established data retention policies and industry best practices
- **Information Sharing Controls:** Strict controls on the sharing of confidential information, including approval processes and monitoring of data transfers, Trust Layer and LLM Gateway Implementation

- **Privacy Impact Assessments:** Regular assessments to identify and mitigate potential privacy risks in new processes or system changes

Processing integrity commitments include, but are not limited to, the following:

- **Data Validation and Verification:** Implementation of automated and manual checks to ensure data is processed completely, accurately, and in a timely manner
- **Error Detection and Correction:** Systematic procedures for identifying, documenting, and correcting processing errors before data is delivered to clients
- **Quality Assurance Protocols:** Multi-stage quality control processes for all professional services, consulting engagements and software development activities to ensure output meets specified requirements
- **Audit Trails and Logging:** Comprehensive logging of all system activities and data processing operations to maintain a complete audit trail for verification and compliance purposes
- **Change Management Controls:** Formal procedures for implementing system changes, including testing and approval processes to prevent processing disruptions
- **Data Integrity Monitoring:** Regular monitoring and validation of data integrity throughout all processing workflows to detect and prevent corruption or unauthorized modifications
- **Performance Metrics and Reporting:** Establishment of key performance indicators and regular reporting to measure and maintain processing accuracy and completeness

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

- **Privacy Policy and Notice:** Clear and comprehensive privacy policies that inform individuals about how their personal information is collected, used, disclosed, and protected
- **Consent Management:** Procedures for obtaining and managing appropriate consent for the collection, use, and disclosure of personal information in accordance with applicable privacy laws
- **Data Minimization:** Collection and processing of only the personal information necessary for specified business purposes, avoiding excessive or irrelevant data collection
- **Individual Rights Management:** Processes to handle individual requests regarding their personal information, including access, correction, deletion, and portability rights as required by applicable privacy legislation
- **Privacy Training and Awareness:** Regular training programs for employees on privacy requirements, best practices, and their responsibilities in protecting personal information
- **Third-Party Privacy Compliance:** Due diligence processes to ensure third-party service providers and partners maintain appropriate privacy protections for personal information
- **Privacy Incident Response:** Established procedures for detecting, investigating, and responding to privacy breaches, including notification requirements to regulatory authorities and affected individuals
- **Cross-Border Data Transfer Safeguards:** Appropriate safeguards and legal mechanisms for any transfer of personal information across international borders
- **Data Retention and Disposal:** Clear policies for retaining personal information only as long as necessary for business purposes and secure disposal when no longer needed
- **Privacy by Design:** Integration of privacy considerations into the design and implementation of new systems, processes, and business practices from the outset

Compliance and Monitoring

Collation.AI, Inc. maintains ongoing compliance with these trust criteria through:

- **Regular Internal Audits:** Periodic assessments of all trust criteria to ensure continued compliance and identify areas for improvement

- **External Auditor Validation:** Annual SOC 2 examinations by qualified independent auditors to verify the effectiveness of our controls
- **Continuous Improvement:** Regular review and enhancement of policies, procedures, and controls based on audit findings, industry best practices, and regulatory changes
- **Management Oversight:** Executive leadership commitment to maintaining the highest standards of security, availability, processing integrity, confidentiality, and privacy
- **Employee Accountability:** Clear roles and responsibilities for all staff members in maintaining compliance with trust criteria requirements

Commitment to Excellence

These comprehensive commitments demonstrate Collation.AI's dedication to protecting our clients' interests and maintaining the trust placed in our services. Our SOC 2 compliance reflects our commitment to operational excellence and provides assurance that we maintain the highest standards in all aspects of our business operations.

3.3 Components of the System used to provide services

Software

Collation.AI is responsible for managing the development and operation of the Collation.AI platform including infrastructure components such as servers, databases, and storage systems. The company leverages Amazon Web Services as its primary cloud infrastructure provider, implementing a comprehensive suite of Azure services to support its SaaS applications, CollationAI Platform Initiatives, development operations, and business functions.

The in-scope Collation.AI infrastructure and software components are shown in the table below:

System/ Application	Business Function / Description
Collation.AI Application	SaaS based platform designed to revolutionize the way Wealth Managers, High Net Worth Individuals (HNIs), and Family Offices handle their investment data and Reporting needs
Azure IAM	Identity and access management console for Azure resources.

Infrastructure & Network Architecture

The production infrastructure for the Collation.AI platform is hosted on Azure. The Collation.AI platform utilizes Azure's robust and secure cloud environment to ensure that the software application is always protected through multiple layers of security and network isolation.

Network Architecture

Azure Virtual Network (VNet)

Collation.AI platform operates within an Azure Virtual Network (VNet), which provides:

- **Network Isolation** from other Azure tenants and the public internet
- **Subnet segmentation** to separate application tiers and control traffic flow
- **Private IP address space** for secure internal communication between resources
- **Custom routing** through Azure Route Tables for traffic control

Security Implementation

The infrastructure implements defense-in-depth security through:

- **Application Gateway** with Azure Web Application Firewall (WAF) as the primary entry point
- **Azure Firewall** for network-level protection and traffic filtering
- **Network Security Groups (NSGs)** providing distributed network access control and security
- **Azure DDoS Protection Standard/Premium** for DDoS attack mitigation

Traffic Flow and Security - Client Connectivity

Secure Client Access

Client connections to the Collation.AI platform follow a secure, multi-layered approach:

- **TLS/SSL Encryption:** All client connections are encrypted using TLS 1.2 or higher protocols
- **Application Gateway Entry Point:** Client traffic enters through Azure Application Gateway with integrated WAF
- **Traffic Inspection:** WAF rules inspect and filter malicious requests before reaching application resources
- **Private Endpoints:** Azure Private Link enables secure connectivity to Azure services over private IP addresses
- **VPN Gateway/ExpressRoute:** For enterprise clients requiring dedicated connectivity, Azure VPN Gateway or ExpressRoute provides private network connections

Virtual Network Protection

Network-Level Defense

The Virtual Network implements comprehensive protection mechanisms:

- **Network Security Groups (NSGs):** Stateful firewall rules control inbound and outbound traffic at subnet and network interface levels
- **Azure Firewall:** Centralized network security policy enforcement with threat intelligence-based filtering
- **Service Tags:** Simplified security rule management using Azure service identifiers
- **Application Security Groups (ASGs):** Logical grouping of resources for simplified security policy management
- **Azure Bastion:** Secure RDP/SSH connectivity to virtual machines without exposing public IP addresses

Internal Network Security

East-West Traffic Protection

Internal network security ensures protection between application components:

- **Subnet Isolation:** Application tiers (web, application, database) are segregated into separate subnets with controlled traffic flow
- **NSG Rules:** Granular control of traffic between subnets based on least-privilege principles
- **Private Endpoints:** Database and storage services accessible only through private IP addresses within the VNet
- **Service Endpoints:** Secure and direct connectivity to Azure PaaS services over Azure backbone network
- **Network Virtual Appliances:** Optional integration of third-party security solutions for advanced inspection

Network Monitoring and Logging

Comprehensive Visibility

The platform implements extensive monitoring and logging capabilities:

- **Azure Monitor:** Centralized monitoring platform for metrics, logs, and alerts across all infrastructure components
- **Network Watcher:** Network performance monitoring, diagnostics, and topology visualization
- **NSG Flow Logs:** Detailed logging of network traffic flowing through Network Security Groups
- **Azure Firewall Logs:** Application and network rule logging for security analysis and compliance
- **Diagnostic Logs:** Resource-level logs for Application Gateway, VNet, and all Azure services
- **Log Analytics Workspace:** Centralized log aggregation and analysis with KQL query capabilities

Traffic Analysis

Network Traffic Intelligence

Advanced analytics provide insights into network behaviour:

- **Traffic Analytics:** AI-powered analysis of NSG flow logs to identify security threats and optimize network performance
- **Network Performance Monitor:** End-to-end network performance monitoring and diagnostics
- **Connection Monitor:** Continuous monitoring of connectivity and latency between resources
- **Packet Capture:** On-demand packet capture capabilities for detailed network troubleshooting
- **Azure Sentinel Integration:** Security information and event management (SIEM) with automated threat detection

High Availability and Resilience

Business Continuity Architecture

The infrastructure is designed for maximum uptime and resilience:

- **Availability Zones:** Application components deployed across multiple Azure Availability Zones for fault tolerance
- **Load Balancing:** Azure Load Balancer and Application Gateway distribute traffic across multiple instances
- **Auto-Scaling:** Automatic scaling of compute resources based on demand and performance metrics
- **Redundant Networking:** Multiple network paths and failover capabilities ensure continuous connectivity
- **Geo-Redundant Storage:** Data replicated across multiple Azure regions for disaster recovery
- **Health Probes:** Continuous health monitoring with automatic traffic redirection from unhealthy instances

Backup and Recovery

Data Protection and Recovery

Comprehensive backup and recovery capabilities protect client data:

- **Azure Backup:** Automated backup of virtual machines, databases, and file systems with configurable retention policies
- **Point-in-Time Restore:** Database recovery to specific points in time for data protection and compliance
- **Geo-Redundant Backups:** Backup data replicated to secondary Azure region for disaster recovery
- **Immutable Storage:** Write-once-read-many (WORM) storages for regulatory compliance and ransomware protection
- **Recovery Time Objective (RTO):** Designed for <4 hour recovery time for critical systems
- **Recovery Point Objective (RPO):** <15 minute data loss exposure through continuous backup and replication
- **Disaster Recovery Testing:** Regular DR drills validate recovery procedures and minimize downtime

Compliance and Governance

Regulatory Alignment

The infrastructure maintains compliance with industry standards:

- **SOC 2 Type II Certified:** Annual audits verify security, availability, and confidentiality controls
- **Azure Policy:** Automated enforcement of organizational standards and regulatory requirements
- **Azure Blueprints:** Repeatable deployment of compliant environments with pre-configured policies and controls
- **Compliance Manager:** Continuous assessment against regulatory frameworks (GDPR, HIPAA, SOC 2)
- **Data Residency:** Client data stored in specified Azure regions to meet geographic compliance requirements
- **Audit Logging:** Comprehensive activity logs retained for compliance reporting and forensic analysis
- **Encryption Standards:** Data encrypted at rest using AES-256 and in transit using TLS 1.2+

Access Control

Identity and Access Management

Strict access controls protect infrastructure and data:

- **Azure Active Directory (AAD):** Centralized identity management with multi-factor authentication (MFA)
- **Role-Based Access Control (RBAC):** Granular permissions assigned based on job responsibilities and least-privilege principles
- **Privileged Identity Management (PIM):** Just-in-time access to administrative roles with approval workflows
- **Conditional Access Policies:** Context-aware access controls based on user, location, device, and risk level
- **Service Principals:** Secure authentication for application-to-service communication
- **Managed Identities:** Automated credential management for Azure resources without storing secrets
- **Key Vault:** Centralized management of encryption keys, certificates, and secrets with hardware security module (HSM) protection
- **Access Reviews:** Periodic reviews and attestation of user permissions to maintain least-privilege access

Network and Security Infrastructure

System/ Application	Business Function / Description
Azure Firewall / Azure Application Gateway WAF	Front-end firewalls protect the network perimeter with rule-based ACLs and back-end firewalls segregate the database servers from internal traffic
Microsoft Defender for Cloud (formerly Azure Security Center)	Unified security management system providing security posture assessment and threat protection recommendations
Azure DDoS Protection Standard/Premium	Distributed Denial of Service protection with always-on monitoring and automatic attack mitigation
Azure Private Link	Private connectivity to Azure services over the Azure backbone network, eliminating exposure to public internet
Network Security Groups (NSGs) / Azure Firewall	Network-level security controls with stateful packet filtering rules for traffic control between subnets

Development and DevOps Platform

System/ Application	Business Function / Description
Azure DevOps & GitHub Actions	Comprehensive DevOps platform providing project management, source control, build automation, and release management
GitHub / Azure Repos	Git-based source code repository with branching strategies, pull requests, and code review workflows
Azure Pipelines / GitHub Actions	CI/CD service for automated build, test, and deployment processes across multiple environments
Azure Boards / Jira	Agile project management tools with work item tracking, sprint planning, and team collaboration features
Azure Artifacts	Package management service for NuGet, npm, Maven, and Python packages with security scanning
Azure Monitor / Application Insights	Observability platform for developers to monitor application performance

Compute and Storage Infrastructure

System/ Application	Business Function / Description
Azure App Service / Azure Container Apps	Platform-as-a-Service hosting for the Collation.AI web application with auto-scaling capabilities and integrated deployment slots
Azure SQL Database / Azure Database for PostgreSQL	Managed relational database service providing high availability, automated backups, and elastic scaling for application data
Azure Blob Storage	Object storage service for documents, images, and large files with multiple access tiers for cost optimization

Identity and Access Management

System/ Application	Business Function / Description
Azure IAM Identity Center	Cloud-based identity and access management service with single sign-on, multi-factor authentication, and conditional access
Google Workspace	Customer identity and access management service for external user authentication and profile management
Azure IAM Multi-Factor Authentication	Additional security layer requiring multiple forms of verification for user authentication

Development Tools and Platforms

System/ Application	Business Function / Description
Visual Studio Code	Lightweight code editor with extensive extension support for multiple programming languages
Terraform	Open-Source Infrastructure as a Code (IaaC) tool for deploying and managing Azure resources through declarative templates

System/ Application	Business Function / Description
Azure CLI	Command-line interface for managing Azure resources and automating deployment tasks
GitHub	Web-based platform using Git for version control, enabling developers to store, manage, share, and collaborate on code and projects
Claude Code	A terminal-based, AI-powered coding assistant by Anthropic enabling developer productivity.

Communication and Collaboration

System/ Application	Business Function / Description
Google Workspace	Productivity suite including Google Drive, Google Docs, Sheets, and Meet for collaboration
Slack	Unified communications platform for chat, video conferencing, file sharing, and application integration

Compliance and Governance

System/ Application	Business Function / Description
Konfirmity Policy	Governance service for creating, assigning, and managing policies to enforce organizational standards
Konfirmity Risk Manager	Risk assessment tool for managing compliance activities and providing compliance score tracking
Konfirmity Information Protection	Data classification and protection service with persistent labelling and encryption capabilities

Integration and API Management

System/ Application	Business Function / Description
Azure Functions	Serverless compute service for running event-triggered code without managing infrastructure
Azure Service Bus	Fully managed enterprise message broker with message queues and publish-subscribe topics
Azure API Management	Fully managed API service for creating, publishing, and managing RESTful and WebSocket APIs

Scalability and Future Growth

The current cloud infrastructure is designed to support:

- Scalable computing resources across Azure infrastructure for growing client demands
- AI provider integration with enterprise-grade providers (Azure OpenAI) for secure and compliant AI capabilities

- Multi-tenant architecture with dedicated client isolation and segregated data processing
- Compliance requirements for healthcare, insurance, financial services, and enterprise technology sectors

This comprehensive cloud infrastructure enables Collation.AI to deliver reliable, secure, and high-quality AI-powered solutions and Private Wealth reporting and insights implementations to clients across multiple industries while maintaining the flexibility to adapt to evolving technology requirements and scale seamlessly with business growth.

People

Collation.AI's staff have been organized into various functions like Sales, Support, Engineering, Product Management, etc. The personnel have also been assigned to the following key roles:

Senior Management: Senior management carries the ultimate responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization's mission. They also assess and incorporate the results of the risk assessment activity into the decision-making process. The senior management understands that their support and involvement is required in order to run an effective risk management program that assesses and mitigates IT-related mission risks.

Information Security Officer: The Senior Management assigns the role of Information Security Officer to one of its staff members who is responsible for the performance of the information security program of the organization. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, and vulnerabilities, and adding controls to mitigate these risks. Additionally, they also summarize remaining residual risks and report the same to Senior Management in a timely manner.

Compliance Program Manager or Privacy Officer: The company assigns the role of Compliance Program Manager to HOE (Head of Engineering) who would be responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of the effective and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organization.

System Users: The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, staff members that access IT resources are provided with annual security awareness training.

Data

Data, as defined by Collation.AI, constitutes the following:

- Transaction data
- Output reports
- Input reports
- System files
- Error logs
- Conversation History and User Session Logs
- AI interaction logs

- Session-based development artifacts
- Execution Logs
- AI-generate Code
- Prompts, workflows, SOPs, Playbooks for CollationAI Platform Agents

All data that is managed, processed and stored as a part of the Collation.AI platform is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value, and criticality to achieving the objectives of the organization. All data is to be assigned one of the following sensitivity levels:

Data Sensitivity	Description	Examples
Customer confidential	Highly valuable and sensitive information where the level of protection is dictated internally through policy and externally by legal and/or contractual requirements. Access to confidential information is limited to authorized employees, contractors, and business partners with a specific need.	- Customer system and operating data - Customer PII / Financial data - Anything subject to a confidentiality agreement with a customer - Client business requirements and proprietary processes - AI-generated code and solutions for clients
Company Confidential	Information that originated or is owned internally or was entrusted to Collation.AI by others. Company confidential information may be shared with authorized employees, contractors, and business partners but not released to the general	- Collation.AI's PII - Unpublished financial information - Documents and processes explicitly marked as confidential - Pricing/marketing and other undisclosed strategies - Proprietary AI platform configurations - Internal development methodologies - AI-generated code and solutions for company - Prompts, workflows, SOPs, Playbooks for CollationAI Platform
Public	Information that has been approved for release to the public and is freely shareable both internally and externally.	- Press releases - Public website - Published case studies - General service offerings information

Further, all customer data is treated as confidential. The availability of this data is also limited by job function. All customer data storage and transmission follow industry-standard encryption. The data is also regularly backed up as documented in the Data backup policy.

Procedures and Policies

Formal policies and procedures have been established to support the Collation.AI platform. These policies cover:

- Code of Business Conduct
- Change Management
- Data Retention
- Data Backup
- Information security
- Vendor management
- Physical security
- Risk management
- Password
- Media disposal
- Incident management
- Endpoint security
- Encryption
- Disaster recovery
- Data classification
- Confidentiality
- Business continuity
- Access control
- Acceptable usage
- Vulnerability management

All policies are made available to all staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring (and annually thereafter or as and when they change).

Collation.AI also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the services or systems provided by the Konfirmity platform, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

3.4 Relevant aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. This section provides information about the five interrelated components of internal control at Collation.AI, including:

1. Control environment
2. Risk assessment
3. Control activities
4. Information and communication
5. Monitoring controls

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Collation.AI's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Collation.AI's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include

the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct.

Collation.AI and its management team has established the following controls to incorporate ethical values throughout the organization:

- A formally documented "Code of business conduct" communicates the organization's values and behavioral standards to staff members
- Staff members are required to acknowledge (upon hiring and annually thereafter) comprehensive policies and procedures covering the areas of Information Security, Change Management, Incident Management, and Access Control. Staff Members also acknowledge that they understand their responsibility for adhering to the policies and procedures.
- All new employees go through an extension hiring processing including validation of identity, past performance, and other background checks as part of the hiring process.

Commitment to Competence

Collation.AI's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. The following controls have been established in order to incorporate the commitment to competence throughout the organization:

- Management outlines the roles and responsibilities of technical staff to ensure that they are clear about their responsibilities in the organization. These roles and responsibilities are reviewed annually by the senior management.
- Annual Security Awareness Training is provided to all staff which focuses on maintaining the security of the proprietary and customer-servicing systems and related data.
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of their job responsibilities.
- Employees are evaluated for competence in performing their job responsibilities at the time of hiring.

Management Philosophy and Operating Style

Collation.AI's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to monitoring business risks, and management's attitudes toward personnel and the processing of information.

Collation.AI's information security function, composed of senior management and the Information Security Officer, meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap. The security function, under the direction of senior management, oversees the security activities and communication of its policies and procedures.

Specific control activities that the Collation.AI has implemented in this area are described below:

- Senior management meetings are held to discuss major initiatives and issues that affect the business as a whole
- Senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment and high severity security incidents annually

Organizational Structure and Assignment of Authority and Responsibility

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

The management is committed to maintaining and improving its framework for how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are accessible to all employees of the company and are updated as required.

Human Resources

Collation.AI's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by the management's ability to hire and retain top-quality personnel who ensure the service organization is operating at maximum efficiency.

Specific control activities that the Collation.AI has implemented in this area are described below:

- Validation of identity, past performance, and other background checks are performed on new hires, who are evaluated for competence in performing their job responsibilities at the time of hiring.
- Job positions are supported by job descriptions.
- New employees are required to acknowledge company policy and confidentiality related agreements upon hire and annually thereafter.
- Upon hire and annually thereafter, all employees must complete training courses covering basic information security practices.
- Performance evaluations for each employee are performed on an annual basis.
- If an employee violates the Code of Conduct in the employee handbook or the company's policies or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.
- When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner.

Risk Assessment

Collation.AI's risk assessment process identifies and manages risks that could potentially affect its ability to provide reliable services to its customers. The management is expected to identify significant risks inherent in products and services as they oversee their areas of responsibility. Collation.AI identifies the underlying sources of risk, measures the impact on the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process identifies risks to the services provided by the Collation.AI platform, and the management has implemented various measures designed to manage these risks.
Collation.AI believes that effective risk management is based on the following principles:

- Senior management's commitment to the security of Collation.AI platform.
- The involvement, cooperation, and insight of all Collation.AI staff.
- Initiating risk assessments with discovery and identification of risks.
- A thorough analysis of identified risks.
- Commitment to the strategy and treatment of identified risks.
- Communicating all identified risks to the senior management.
- Encouraging all Collation.AI staff to report risks and threat vectors.

Scope

The Risk Assessment and Management program applies to all systems and data that are a part of the Collation.AI platform. The Collation.AI risk assessment exercise evaluates infrastructure such as computer infrastructure, containing networks, instances, databases, systems, storage, and services. The risk assessments also include an analysis of business/IT practices, procedures, and physical spaces as needed.

Risk assessments may be high-level or detailed to a specific organizational or technical change as the stakeholders and technologists see fit.

Overall, the execution, development, and implementation of risk assessment and remediation programs is the joint responsibility of Collation.AI's Information Security Officer and the department or individuals responsible for the area being assessed. All Collation.AI staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff is further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

Vendor Risk Assessment

Collation.AI uses a number of vendors to meet its business objectives. Collation.AI understands that risks exist when engaging with vendors and as a result, continuously assesses those risks that could potentially affect the Company's ability to meet its business objectives.

Collation.AI employs several activities to effectively manage their vendors. Firstly, the Information Security Officer performs an annual exercise of thoroughly examining the nature and extent of risks involved with each vendor relationship. For critical vendors, Collation.AI assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support Collation.AI's commitments to its customers. If a critical vendor is unable to provide a third-party security report or assessment, Collation.AI performs their own external surface scan periodically to assess their performance, security concerns, and their services. Any vendor risks identified are recorded in the risk assessment matrix, which is reviewed annually by the Senior Management of the company.

Integration with Risk Assessment

As part of the design and operation of the system, Collation.AI identifies the specific risks that service commitments may not be met, and designs control necessary to address those risks. Collation.AI's management

performs an annual Risk Assessment Exercise to identify and evaluate internal and external risks to the Company, as well as their potential impacts, likelihood, severity, and mitigating action.

Information and Communication

Collation.AI maintains a company-wide Information Security Policy, supported by detailed standards and training to ensure that employees understand their individual roles and responsibilities regarding security and significant events.

Further, Collation.AI also has additional policies and procedures that define access management, change management, and authentication requirements and procedures for critical systems. These policies and procedures are published and made available to internal staff via the company intranet.

Monitoring Controls

Collation.AI management monitors control to ensure that they are operating as intended and that the controls are modified as conditions change. Monitoring activities are undertaken to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Staff activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, independent evaluations, or a combination of the two.

Control Activities

Collation.AI's control activities are defined through its established policies and procedures which address individual risks associated with the achievement of the company's objectives. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.

Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Logical Access Control

The Collation.AI platform uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software application and authenticates to the database.

Collation.AI has identified certain systems that are critical to meet its service commitments. All-access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member as well as a role-based access matrix prior to being issued system credentials and granted the ability to access the system. When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner.

The Information Security Officer is responsible for performing quarterly reviews of everyone who has access to the system and assessing the appropriateness of the access and permission levels and making modifications based on the principle of least privilege, whenever necessary.

Access to critical systems requires multi-factor authentication (MFA) wherever possible. Staff members must

use complex passwords, wherever possible, for all of their accounts that have access to Collation.AI customer data. Staff is encouraged to use passwords that have at least 10 characters, are randomly generated, alphanumeric, and are special character based. Password configuration settings are configured on each critical system. Additionally, company- managed endpoints are configured to auto-screen-lock after 15 minutes of inactivity.

Change Management

A documented Change Management policy guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the Collation.AI system is reviewed, deployed, and managed. The policy covers all changes made to the Collation.AI platform, regardless of their size, scope, or potential impact.

The change management policy is designed to mitigate the risks of:

- Corrupted or destroyed information
- Degraded or disrupted software application performance
- Productivity loss
- Introduction of software bugs, configuration errors, vulnerabilities, etc.

A change to the Collation.AI platform can be initiated by a staff member with an appropriate role. Collation.AI uses a version control system to manage and record activities related to the change management process.

The version control system maintains source code versions and migrates source code through the development and testing process to the production environment. The version control software maintains a history of code changes to support rollback capabilities. It also facilitates the code review process which is mandated for all changes.

To initiate a change, the developer first creates a feature branch with the updated code. Once the code change is ready for review, the developer submits the code for peer review and automated testing, known as a pull request. For all code changes, the reviewer must be different from the author. Once a pull request is approved, the change can be released to production.

The ability to implement changes in the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities.

Incident Management

Collation.AI has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact Collation.AI via the support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event there were problems.

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analyzed for anomalous or suspicious activity.

Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s)

and assigned a severity rating. Operational events are automatically resolved by the self-healing system.

- Low severity incidents are those that do not require immediate remediation. These typically include a partial service of Collation.AI being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.
- Medium severity incidents are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium-severity incidents usually cover the large majority of incidents found.
- High severity incidents are problems an active security attack has not yet happened but is likely. This includes situations like backdoors, malware, and malicious access to business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed, and immediate remediation steps should begin.
- Critical severity incidents are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

Post-mortem activities are conducted for incidents with critical severity ratings. Results of post- mortems may include updates to the security program or changes to systems required as a result of incidents.

Cryptography

User requests to Collation.AI's systems are encrypted using Transport Layer Security (TLS) using certificates from an established third-party certificate authority. Remote system administration access to Cloud Infrastructure is available through a cloud native Azure cryptographic network protocols (i.e., SSH) over an encrypted virtual private network (VPN) connection. Data at rest and in transit is encrypted using Advanced Encryption Standard (AES) 256-bit.

Asset Management (Hardware and Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. Collation.AI uses tagging tools to automatically facilitate the company's hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technology assets with the potential to store or process information is maintained.

Endpoint Management

Endpoint management solutions are in place that includes policy enforcement on company-issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include but are not limited to enabling screen lock, OS updates, and encryption at rest on critical devices/ workstations.

Physical Security

The in-scope system and supporting infrastructure are hosted by Azure. As such, Azure is responsible for the physical security controls of the in-scope system. Collation.AI reviews the SOC 2 report provided by Azure on an annual basis, to ensure their controls are in accordance with standards expected by the customers of the

Collation.AI platform.

Availability

Collation.AI has a documented business continuity plan (BCP), and testing performed against the recovery time objectives (RTOs) and recovery point objectives (RPOs). At least daily backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

Boundaries of the System

The scope of this report includes the Collation.AI platform. It also includes the people, processes, and IT systems that are required to achieve our service commitments toward the customers of this application.

Collation.AI depends on a number of vendors to achieve its objectives. The scope of this report does not include the processes and controls performed by the vendors. The management understands that risks exist when engaging with vendors and has formulated a process for managing such risks, as detailed in the Risk Assessment section of this document.

Significant Events and Conditions

Collation.AI has implemented automated and manual procedures to capture and address significant events and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with all relevant information for any impact on the software application.

3.5 Complementary User Entity Controls

Collation.AI's controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for Collation.AI customers.

For customers to rely on the information processed through the Collation.AI's software application, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

- Customers are responsible for managing their organization's Collation.AI platform account as well as establishing any customized security solutions or automated processes through the use of setup features
- Customers are responsible for ensuring that authorized users are appointed as administrators for granting access to their Collation.AI platform account
- Customers are responsible for notifying Collation.AI of any unauthorized use of any password or account or any other known or suspected breach of security related to the use of Collation.AI platform.
- Customers are responsible for any changes made to user and organization data stored within the Collation.AI platform.

- Customers are responsible for communicating relevant security and availability issues and incidents to Collation.AI through identified channels.

3.6 Complementary Subservice Organization Controls

Controls at Service organization and controls at User organization related to Collation.AI platform to its customers relevant to the Security, Availability, and Confidentiality ("in-scope trust service criteria"), cover only a portion of the overall internal control structure of its clients. The control objectives cannot be achieved without taking into consideration operating effectiveness of controls at subservice organization providing services to service organization to perform services provided to user entity that are likely to be relevant to that user entity internal control over financial reporting.

This section highlights those internal control structure responsibilities, Collation.AI believes should be present at all applicable subservice organization, and which Collation.AI has considered in developing its control structure policies and the procedures described in this report.

The subservice organization used by Collation.AI relevant to providing services related to Collation.AI platform is shown below:

Subservice Organization	Service Provided
Azure	Cloud computing services

Control Activity Expected to be Implemented by Subservice Organization	Applicable Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	CC6.1, CC6.2, CC6.3, CC6.5, CC7.2
Physical access and security to the data center facility are restricted to authorized personnel.	CC6.4, CC6.5
Environmental protection, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	CC6.4, A1.2
Encryption methods are used to protect data in transit and at rest.	CC6.1
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	A1.3
Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other physical security components.	A1.2
A defined Data Classification Policy specifies classification levels and control requirements to meet the company's commitments related to confidentiality.	C1.1
A defined process is in place to sanitize and destroy hard drives and back up media containing customer data prior to leaving company facilities.	C1.2

3.7 Trust services criteria and Description of Related Controls:

The description of the in-scope trust service criteria and related controls over its Collation.AI platform is included only within Section 4 of this report to eliminate the redundancy that would result from listing them in this section and repeating them in section 4. Although the in-scope trust service criteria and related controls in Section 4 are presented separately, they form an integral part of Collation.AI's description of the Collation.AI platform.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR: TEST OF CONTROLS

4 INFORMATION PROVIDED BY INDEPENDENT SERVICE AUDITOR EXCEPT FOR APPLICABLE TRUST SERVICES CRITERIA AND CONTROL ACTIVITIES

4.1 Objective of Our Examination

This report, including the description of tests of controls and results thereof in this section are intended solely for the information and use of Collation.AI, user entities of the Collation.AI system related to Collation.AI platform during some or all of the period October 1, 2025 through August 31, 2025, business partners of Collation.AI subject to risks arising from interactions with Collation.AI's system, 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, subservice Organizations, and other parties;
- internal control and its limitations;
- complementary user-entity controls and how they interact with related controls at the service Organization to meet the applicable trust services criteria; the applicable trust services criteria;
- and the risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

This section presents the following information provided by Collation.AI:

- The controls established and specified by Collation.AI to achieve the specified trust services criteria.

Also included in this section is the following information provided by auditors:

- A description of the tests performed by auditors to determine whether Collation.AI's controls were operating with sufficient effectiveness to achieve specified trust services criteria. Auditors determined the nature, timing, and extent of the testing performed.
- The results of tests of controls.

The examination was conducted in accordance with the criteria as set forth in DC Section 200. 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period September 1, 2024 to August 31, 2025 to provide reasonable assurance that Collation.AI's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality ("applicable trust services criteria") set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, of the American Institute of Certified Public Accountants (AICPA), and the AICPA Statement on Standards for Attestation Engagements No. 18 (SSAE 18). SSAE 18 is inclusive of the following: (1) AT-C 105, Concepts Common to all Attestation Engagements; and (2) AT-C 205, Examination Engagements. Our testing of Collation.AI's controls was restricted to the controls identified by Collation.AI to meet the criteria related to Security, Availability and Confidentiality listed in Section 1 of this report and was not extended to controls described in Section 3 but not included in Section 4, or to controls that may be in effect at user Organizations or subservice Organizations.

It is each user's responsibility to evaluate the information included in this report in relation to internal control in place at individual user entities and subservice Organizations to obtain an understanding and to assess control risk at the user entities. The controls at user entities, subservice Organizations, and Collation.AI's controls should be evaluated together. If effective user entity or subservice Organizations controls are not in place, Collation.AI's controls may not compensate for such weaknesses.

4.2 Control Environment Elements

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. In addition to the tests of design, implementation, and operating effectiveness of controls identified by Collation.AI our procedures included tests of the following relevant elements of the Collation.AI control environment:

1. Environment
2. Internal Risk Assessment
3. Information and Communication
4. Monitoring
5. Control Activities

Such tests included inquiry of the appropriate management, supervisory, and staff personnel; observation of Collation.AI activities and operations, inspection of Collation.AI documents and records, and re-performance of the application of Collation.AI controls. The results of these tests were considered in planning the nature, timing, and extent of our testing of the control activities described in this section.

4.3 Applicable Trust Services Criteria, Controls, Tests of Operating Effectiveness, and Results of Tests

Our tests were designed to examine the Collation.AI description of the system related to Collation.AI as well as the suitability of the design and operating effectiveness of controls for a representative number of samples throughout the period of September 1, 2024, to August 31, 2025.

In selecting particular tests of the operational effectiveness of controls, we considered the (a) nature of the items being tested, (b) the types of available evidential matter, (c) the nature of the trust services principles and criteria to be achieved and (d) the expected efficiency and effectiveness of the test.

Testing the accuracy and completeness of information provided by Collation.AI is also a component of the testing procedures performed. Information we are utilizing as evidence may include, but is not limited to:

1. Standard 'out of the box' reports as configured within the system.
2. Parameter-driven reports generated by Collation.AI systems.
3. Custom-developed reports that are not standard to the application such as scripts, report writers, and queries.
4. Spreadsheets that include relevant information utilized for the performance or testing of a control.
5. Collation.AI - prepared analyses, schedules, or other evidence manually prepared and utilized by the Company.

While these procedures are not specifically called out in the test procedures listed in this section, they are completed as a component of our testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by Collation.AI.

4.4 Description of Testing Procedures Performed

Our examination included inquiry of management, supervisory, and staff personnel; inspection of documents and records; observation of activities and operations; and re-performance of controls surrounding and provided by Collation.AI. Our tests of controls were performed on controls as they existed during the period of September 1, 2024, to August 31, 2025, and were applied to those controls relating to the trust services principles and criteria.

Tests performed of the operational effectiveness of controls are described below:

Test	Description
Inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control multiple times throughout the report period to evidence application of the specific control activity.
Examination of Documentation/Inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Re-performance of Monitoring Activities or Manual Controls	Obtained documents used in the monitoring activity or manual control activity and independently re-performed the procedures. Compared any exception items identified with those identified by the responsible control owner.
Re-performance of Programmed Processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.

Reporting on Results of Testing

The concept of materiality is not applied when reporting the results of tests of controls for which deviations have been identified because auditors does not have the ability to determine whether a deviation will be relevant to a particular user entity. Consequently, auditor reports all deviations.

4.5 Testing Procedures Performed by Independent Service Auditor

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
CC1.1	ACF-1	Entity has a documented policy to define behavioral standards and acceptable business conduct.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected code of conduct document and acceptable usage policy to ascertain whether entity has a documented policy to define behavioral standards and acceptable business conduct.	No exceptions noted.
	ACF-2	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample new joiners, policy acceptance logs and HR policies to ascertain whether entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	No exceptions noted.
	ACF-3	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample employees, policy acceptance logs and HR policies information to ascertain whether entity has established procedures for staff to acknowledge applicable company policies periodically.	No exceptions noted.
	ACF-4	Entity outlines and documents cybersecurity responsibilities for all personnel.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected documented roles and responsibilities to ascertain whether entity outlines and documents cybersecurity responsibilities for all personnel.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
CC1.2	ACF-5	Entity's Senior Management reviews and approves all company policies annually.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected policy and process review sign-off logs to ascertain whether entity's Senior Management reviews and approves all company policies annually.	No exceptions noted.
	ACF-6	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected policy and process review sign-off logs to ascertain whether entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	No exceptions noted.
	ACF-7	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected organization chart and its review records to ascertain whether entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	No exceptions noted.
	ACF-8	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected risk assessment report and review evidence to ascertain whether entity's Senior Management reviews and approves the Risk Assessment Report annually.	No exceptions noted.
	ACF-9	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected vendor assessment register and reports to ascertain	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
			whether entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	
CC1.3	ACF-10	Entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected organizational structure to ascertain whether entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.	No exceptions noted.
	ACF-11	Entity has established procedures to communicate with staff about their roles and responsibilities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample joiners, communications showing roles and responsibilities were shared to ascertain whether entity has established procedures to communicate with staff about their roles and responsibilities.	No exceptions noted.
	ACF-12	Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected organizational structure and roles and responsibility document of Information Security Officer to ascertain whether entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.	No exceptions noted.
	ACF-13	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected policy and process review sign-off logs to ascertain whether entity's Senior Management reviews and approves the state of the Information Security program including policies,	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		ensure their continuing suitability, adequacy, and effectiveness.	standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	
	ACF-14	Entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected asset register to ascertain whether entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	No exceptions noted.
	ACF-15	Entity appoints a People Operations Officer to develop and drive all personnel-related security strategies.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected organizational structure and roles and responsibility document of People Operations Officer to ascertain whether entity appoints a People Operations Officer to develop and drive all personnel-related security strategies.	No exceptions noted.
	ACF-16	Entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected organizational structure and roles and responsibility document of compliance program manager to ascertain whether entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.	No exceptions noted.
CC1.4	ACF-17	Entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample new joiners, candidate evaluation forms and HR policies to ascertain whether entity has procedures to	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
			ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	
	ACF-18	Entity has established procedures to perform security risk screening of individuals before authorizing access.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample new joiners, background verification records and HR policies to ascertain whether entity has established procedures to perform security risk screening of individuals before authorizing access.	No exceptions noted.
	ACF-19	Entity provides information security and privacy training to staff that is relevant to their job function.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected attendance records from the last Security and privacy training to ascertain whether entity provides information security and privacy training to staff that is relevant to their job function.	No exceptions noted.
CC1.5	ACF-20	Entity provides information security and privacy training to staff that is relevant to their job function.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected attendance records from the last Security and privacy training to ascertain whether entity provides information security and privacy training to staff that is relevant to their job function.	No exceptions noted.
	ACF-21	Entity requires that all employees in client serving, IT, Engineering, and Information Security roles are periodically evaluated regarding their job responsibilities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Employee performance reviews, Job Descriptions and hiring records to assess that hiring is done for a role, and roles	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
			are evaluated aligned to organization growth and changing needs.	
	ACF-22	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample employees, policy acceptance logs and HR policies information to ascertain whether entity has established procedures for staff to acknowledge applicable company policies periodically.	No exceptions noted.
	ACF-23	Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample new joiners, inspected Security awareness and Privacy training completion records and HR policies to ascertain whether entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	No exceptions noted.
	ACF-24	Entity documents, monitors, and retains individual training activities and records.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected attendance records from the last Security and privacy training to ascertain whether entity documents, monitors, and retains individual training activities and records.	No exceptions noted.
CC2.1	ACF-25	Entity systems generate information that is reviewed and evaluated to determine impacts on the functioning of internal controls.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected logs from event monitoring tool to ascertain whether entity systems generate information that is reviewed and	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
			evaluated to determine impacts on the functioning of internal controls.	
	ACF-26	Entity makes all policies and procedures available to all staff members for their perusal.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, shared folder where all the policies are stored and noted all the employees have access to published policies.	No exceptions noted.
	ACF-27	Entity displays the most current information about its services on its website, which is accessible to its customers.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected their publicly accessible website to ascertain whether entity displays the most current information about its services on its website, which is accessible to its customers.	No exceptions noted.
	ACF-28	Entity has a documented policy outlining guidelines for the disposal and retention of information.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected data disposal and retention policy to ascertain whether entity has a documented policy outlining guidelines for the disposal and retention of information.	No exceptions noted.
	ACF-29	Entity has documented policy and procedures for physical and/or logical labelling of information via documented policy for data classification.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected data classification policy and procedures related to asset and information labelling to ascertain whether entity has documented policy and procedures for physical and/or logical labelling of information via documented policy for data classification.	No exceptions noted.
CC2.2	ACF-30	Entity has a documented policy to define behavioral standards and acceptable business conduct.	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
			Inspected code of conduct document and acceptable usage policy to ascertain whether entity has a documented policy to define behavioral standards and acceptable business conduct.	
	ACF-31	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample new joiners, policy acceptance logs and HR policies to ascertain whether entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	No exceptions noted.
	ACF-32	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample employees, policy acceptance logs and HR policies information to ascertain whether entity has established procedures for staff to acknowledge applicable company policies periodically.	No exceptions noted.
	ACF-33	Entity makes all policies and procedures available to all staff members for their perusal.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, shared folder where all the policies are stored and noted all the employees have access to published policies.	No exceptions noted.
	ACF-34	Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Information Security policy and procedures to ascertain whether entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		provided by the entity in the event there are problems.	complaints related to the services or systems provided by the entity in the event there are problems.	
	ACF-35	Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected password management policy and password configuration to ascertain whether entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.	No exceptions noted.
	ACF-36	Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample new joiners, inspected Security awareness and Privacy training completion records and HR policies to ascertain whether entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	No exceptions noted.
	ACF-37	Entity documents, monitors, and retains individual training activities and records.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected attendance records from the last Security and privacy training to ascertain whether entity documents, monitors, and retains individual training activities and records.	No exceptions noted.
CC2.3	ACF-38	Entity displays the most current information about its services on its website, which is accessible to its customers.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected their publicly accessible website to ascertain whether	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
			entity displays the most current information about its services on its website, which is accessible to its customers.	
	ACF-39	Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected incident management and sample of incident tickets to ascertain whether entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	No exceptions noted.
	ACF-40	Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected privacy policy to ascertain whether entity has documented guidelines on notifying customers and other stakeholders in case of a breach.	No exceptions noted.
CC3.1	ACF-41	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected risk register to ascertain whether entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	No exceptions noted.
	ACF-42	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected risk management policy to ascertain whether entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		commitments and system requirements	assessed and mitigated. The objectives incorporate the entity's service commitments and system requirements.	
CC3.2	ACF-43	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample new joiners, policy acceptance logs and HR policies to ascertain whether entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	No exceptions noted.
	ACF-44	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected risk register to ascertain whether entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	No exceptions noted.
	ACF-45	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected documented risk mitigation strategy within risk register to ascertain whether each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	No exceptions noted.
	ACF-46	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected vendor risk assessment forms to ascertain whether entity performs a formal vendor risk assessment exercise	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		to the systems' security commitments and requirements.	annually to identify vendors that are critical to the systems' security commitments and requirements.	
	ACF-47	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest security assessment report to ascertain whether entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	No exceptions noted.
	ACF-48	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected risk management policy to ascertain whether entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the entity's service commitments and system requirements.	No exceptions noted.
	ACF-49	Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected vendor management policy to ascertain whether entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors.	No exceptions noted.
CC3.3	ACF-50	Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected risk register and risks related to fraud to ascertain whether entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
CC3.4	ACF-51	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected risk register to ascertain whether entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	No exceptions noted.
	ACF-52	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected documented risk mitigation strategy within risk register to ascertain whether each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	No exceptions noted.
	ACF-53	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected vendor risk assessment forms to ascertain whether entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	No exceptions noted.
CC4.1	ACF-54	Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected organizational structure and roles and responsibility document of Information Security Officer to ascertain whether entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage,	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
			coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.	
	ACF-55	Entity uses a continuous monitoring tool to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected monitoring logs the monitoring tool to ascertain whether entity uses a monitoring tool to track and report the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
	ACF-56	Entity's Senior Management reviews and approves all company policies annually.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected policy and process review sign-off logs to ascertain whether entity's Senior Management reviews and approves all company policies annually.	No exceptions noted.
	ACF-57	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected policy and process review sign-off logs to ascertain whether entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	No exceptions noted.
	ACF-58	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected organization chart and its review records to ascertain	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
			whether entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	
	ACF-59	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected risk assessment report and review evidence to ascertain whether entity's Senior Management reviews and approves the Risk Assessment Report annually.	No exceptions noted.
	ACF-60	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected vendor assessment register and reports to ascertain whether entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	No exceptions noted.
	ACF-61	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected SOC 2 type II reports of subservice organization and evaluation report prepared by entity to ascertain whether entity reviews and evaluates all subservice organizations periodically, to ensure commitments to entity's customers can be met.	No exceptions noted.
	ACF-62	Entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected asset register to ascertain whether entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-63	Entity periodically updates and reviews the inventory of systems as a part of installations, removals, and system updates.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected asset register to ascertain whether entity periodically updates and reviews the inventory of systems as a part of installations, removals, and system updates.	No exceptions noted.
CC4.2	ACF-64	Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Information Security policy and procedures to ascertain whether entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	No exceptions noted.
	ACF-65	Entity uses a continuous monitoring tool to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected monitoring logs the monitoring tool to ascertain whether entity uses a monitoring tool to track and report the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
	ACF-66	Entity's Senior Management reviews and approves all company policies annually.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected policy and process review sign-off logs to ascertain whether entity's Senior Management reviews and approves all company policies annually.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-67	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected policy and process review sign-off logs to ascertain whether entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	No exceptions noted.
CC5.1	ACF-68	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected information security policy and acceptable usage policy to ascertain whether entity has documented a set of policies and procedures that establish expected behavior with regard to the Company's control environment.	No exceptions noted.
	ACF-69	Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected user access list to ascertain whether entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	No exceptions noted.
	ACF-70	Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Information Security Policy to ascertain whether entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-71	Entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected information security policy and acceptable usage policy to ascertain whether entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.	No exceptions noted.
CC5.2	ACF-72	Entity uses a continuous monitoring tool to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected monitoring logs the monitoring tool to ascertain whether entity uses a monitoring tool to track and report the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
	ACF-73	Entity's Senior Management reviews and approves all company policies annually.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected policy and process review sign-off logs to ascertain whether entity's Senior Management reviews and approves all company policies annually.	No exceptions noted.
	ACF-74	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected policy and process review sign-off logs to ascertain whether entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-75	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected organization chart and its review records to ascertain whether entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	No exceptions noted.
	ACF-76	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected risk assessment report and review evidence to ascertain whether entity's Senior Management reviews and approves the Risk Assessment Report annually.	No exceptions noted.
	ACF-77	Entity's Infosec officer reviews and approves the list of people with access to production console annually.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected user access review records to ascertain whether entity's Infosec officer reviews and approves the list of people with access to production console annually. Noted that no changes were requested as part of the user access review activity.	No exceptions noted.
	ACF-78	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected vendor assessment register and reports to ascertain whether entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-79	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected SOC 2 type II reports of subservice organization and evaluation report prepared by entity to ascertain whether entity reviews and evaluates all subservice organizations periodically, to ensure commitments to entity's customers can be met.	No exceptions noted.
	ACF-80	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected information security policy and acceptable usage policy to ascertain whether entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.	No exceptions noted.
	ACF-81	Entity uses a continuous monitoring tool to alert the security team to update the access levels of team members whose roles have changed.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected logs from monitoring tool to ascertain whether entity uses a continuous monitoring too to alert the security team to update the access levels of team members whose roles have changed.	No exceptions noted.
CC5.3	ACF-82	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample new joiners, policy acceptance logs and HR policies to ascertain whether entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-83	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample employees, policy acceptance logs and HR policies information to ascertain whether entity has established procedures for staff to acknowledge applicable company policies periodically.	No exceptions noted.
	ACF-84	Entity makes all policies and procedures available to all staff members for their perusal.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, shared folder where all the policies are stored and noted all the employees have access to published policies.	No exceptions noted.
	ACF-85	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected information security policy and acceptable usage policy to ascertain whether entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.	No exceptions noted.
	ACF-86	Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Access Control policy to ascertain whether entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	No exceptions noted.
	ACF-87	Entity has established a policy and procedure which includes guidelines to be undertaken in	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected incident management policy to ascertain whether	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		response to information security incidents.	entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. Trust Layer Implementation for Upfront Classification/Detection/Blocking of user inputs which are off topic and security threats on user inputs	
	ACF-88	Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Backup policy to ascertain whether entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	No exceptions noted.
	ACF-88	Entity has documented policies and procedures to manage changes to its operating environment.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected change management policy and SDLC process document to ascertain whether entity has documented policies and procedures to manage changes to its operating environment.	No exceptions noted.
	ACF-89	Entity has procedures to govern changes to its operating environment.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected change management policy and SDLC process document to ascertain whether entity has procedures to govern changes to its operating environment. Entity also complies with client's change management policy where applicable.	No exceptions noted.
	ACF-90	Entity has established procedures for approval when implementing changes to the operating environment.	Inquired with the management regarding the control activity to ascertain that the control operates as described.	Operating effectiveness of this control activity could not be tested as there was

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
			Noted that there were no changes implemented during the audit period.	no related activity during the audit period.
	ACF-90	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected risk management policy to ascertain whether entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the entity's service commitments and system requirements.	No exceptions noted.
	ACF-91	Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Information Security Policy to ascertain whether entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems.	No exceptions noted.
	ACF-92	Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected password management policy and password configuration to ascertain whether entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.	No exceptions noted.
	ACF-93	Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected information security policy and vulnerability management policy to ascertain whether entity has a	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
			documented policy and procedures to establish guidelines for managing technical vulnerabilities.	
CC6.1	ACF-94	Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Access Control policy to ascertain whether entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	No exceptions noted.
	ACF-95	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample new joiner, access approval forms to ascertain whether entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	No exceptions noted.
	ACF-96	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected firewall configuration and database access ruleset to ascertain whether entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	No exceptions noted.
	ACF-97	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest user access review records to ascertain whether entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		who require such access to perform their job functions.	systems is restricted to only those individuals who require such access to perform their job functions.	
	ACF-98	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest user access review records to ascertain whether entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	No exceptions noted.
	ACF-99	Entity uses a continuous monitoring tool to alert the security team to update the access levels of team members whose roles have changed.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected logs from monitoring tool to ascertain whether entity uses a continuous monitoring too to alert the security team to update the access levels of team members whose roles have changed.	No exceptions noted.
	ACF-100	Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected password management policy and password configuration to ascertain whether entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.	No exceptions noted.
CC6.2	ACF-101	Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Access Control policy to ascertain whether entity has documented policies and procedures to manage Access Control	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		which grant the ability to access the critical systems.	and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	
	ACF-102	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample new joiner, access approval forms to ascertain whether entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	No exceptions noted.
	ACF-103	Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample leavers, access revocation logs and last working date to ascertain whether entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.	No exceptions noted.
CC6.3	ACF-104	Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Access Control policy to ascertain whether entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	No exceptions noted.
	ACF-105	Entity ensures that logical access provisioning to critical systems requires approval from authorized	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample new joiner, access approval forms to ascertain whether entity ensures that logical access provisioning	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		personnel on an individual need or for a predefined role.	to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	
	ACF-106	Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample leavers, access revocation logs and last working date to ascertain whether entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.	No exceptions noted.
	ACF-107	Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected list of users having access to production databases to ascertain whether entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.	No exceptions noted.
	ACF-108	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest user access review records to ascertain whether entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	No exceptions noted.
	ACF-109	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest user access review records to ascertain whether entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		access to perform their job functions.	the critical systems is restricted to only those individuals who require such access to perform their job functions.	
	ACF-110	Entity uses a continuous monitoring tool to alert the security team to update the access levels of team members whose roles have changed.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected logs from monitoring tool to ascertain whether entity uses a continuous monitoring too to alert the security team to update the access levels of team members whose roles have changed.	No exceptions noted.
CC6.4	ACF-111	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Not applicable as all the applications and information are hosted on cloud services provided by Azure. Backup media and other sensitive data is also stored digitally on Cloud. Client restricts physical access to their office and Client Production Resources via a RBAC on need basis. Default access is NONE.	No exceptions noted.
CC6.5	ACF-112	Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample leavers, access revocation logs and last working date to ascertain whether entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.	No exceptions noted.
	ACF-113	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected asset disposal policy to ascertain whether entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
CC6.6	ACF-114	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected firewall configuration and database access ruleset to ascertain whether entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	No exceptions noted.
	ACF-115	Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor authentication.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected MFA configuration to ascertain whether entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor authentication.	No exceptions noted.
	ACF-116	Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample endpoint, anti-virus and malware protection software version and installation status to ascertain whether where applicable, entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.	No exceptions noted.
	ACF-117	Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample endpoint, encryption status to ascertain whether entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-118	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest security patching report to ascertain whether entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	No exceptions noted.
	ACF-119	Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected screen lock configuration at domain level to ascertain whether entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.	No exceptions noted.
	ACF-120	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected firewall configuration to ascertain whether production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the entity's cloud provider.	No exceptions noted.
	ACF-121	Entity has documented policies and procedures for endpoint security and related controls.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected information security policy and endpoint protection policy to ascertain whether entity has documented policies and procedures for endpoint security and related controls.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-122	Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample endpoints, encryption configuration and password configuration to ascertain whether entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	No exceptions noted.
	ACF-123	Entity has documented guidelines to manage communications protections and network security of critical systems.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected network security policy and approved hardening standard to ascertain whether entity has documented guidelines to manage communications protections and network security of critical systems.	No exceptions noted.
	ACF-124	Entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected asset register to ascertain whether entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.	No exceptions noted.
CC6.7	ACF-125	Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample endpoint, encryption status to ascertain whether entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	No exceptions noted.
	ACF-126	Entity has set up cryptographic mechanisms to encrypt all	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		production database[s] that store customer data at rest.	Inspected encryption status of production databases to ascertain whether entity has set up cryptographic mechanisms to encrypt all production databases that store customer data at rest.	
	ACF-127	Entity has set up processes to utilize standard encryption methods, including HTTPS with the TLS algorithm, to keep transmitted data confidential.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected TLS certificate to ascertain whether entity has set up processes to utilize standard encryption methods, including HTTPS with the TLS algorithm, to keep transmitted data confidential.	No exceptions noted.
	ACF-128	Entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected asset inventory to ascertain whether entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	No exceptions noted.
	ACF-129	Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected encryption status and firewall configuration for non-prod environment to ascertain whether entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment. As an necessary measure Trust Layer and LLM Gateway Implementations are extended for such environments as well.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-130	Entity has a documented policy to manage encryption and cryptographic protection controls.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected encryption and cryptographic policy to ascertain whether entity has a documented policy to manage encryption and cryptographic protection controls.	No exceptions noted.
	ACF-131	Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample endpoints, encryption configuration and password configuration to ascertain whether entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	No exceptions noted.
CC6.8	ACF-132	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest security patching report to ascertain whether entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	No exceptions noted.
	ACF-133	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected firewall configuration to ascertain whether production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the entity's cloud provider.	No exceptions noted.
CC7.1	ACF-134	Entity uses a continuous monitoring tool to track and report the health of the information	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		security program to the Information Security Officer and other stakeholders.	Inspected monitoring logs the monitoring tool to ascertain whether entity uses a monitoring tool to track and report the health of the information security program to the Information Security Officer and other stakeholders.	
	ACF-135	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest security assessment report to ascertain whether entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	No exceptions noted.
	ACF-136	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest security assessment report to ascertain whether entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	No exceptions noted.
	ACF-137	Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected event monitoring tool configuration and logs to ascertain whether entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	No exceptions noted.
	ACF-138	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected event monitoring tool configuration and logs to ascertain whether entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		protect against denial-of-service attacks.	optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	
	ACF-139	Entity uses a continuous monitoring tool to alert the security team to update the access levels of team members whose roles have changed.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected logs from monitoring tool to ascertain whether entity uses a continuous monitoring too to alert the security team to update the access levels of team members whose roles have changed.	No exceptions noted.
	ACF-140	Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected information security policy and vulnerability management policy to ascertain whether entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.	No exceptions noted.
	ACF-141	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected event monitoring tool configuration and logs to ascertain whether entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	No exceptions noted.
CC7.2	ACF-142	Entity uses a continuous monitoring tool to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected monitoring logs the monitoring tool to ascertain whether entity uses a monitoring tool to track and report the	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
			health of the information security program to the Information Security Officer and other stakeholders.	
	ACF-143	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest security assessment report to ascertain whether entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	No exceptions noted.
	ACF-144	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest security assessment report to ascertain whether entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	No exceptions noted.
	ACF-145	Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected event monitoring tool configuration and logs to ascertain whether entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	No exceptions noted.
	ACF-146	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected event monitoring tool configuration and logs to ascertain whether entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-147	Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected information security policy and vulnerability management policy to ascertain whether entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.	No exceptions noted.
	ACF-148	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected event monitoring tool configuration and logs to ascertain whether entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	No exceptions noted.
CC7.3	ACF-149	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest security patching report to ascertain whether entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	No exceptions noted.
	ACF-150	Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected list of incidents and noted that there was no security incident reported during the audit period.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-151	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest security assessment report to ascertain whether entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	No exceptions noted.
	ACF-152	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest security assessment report to ascertain whether entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	No exceptions noted.
	ACF-153	Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected event monitoring tool configuration and logs to ascertain whether entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	No exceptions noted.
	ACF-154	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected event monitoring tool configuration and logs to ascertain whether entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-155	Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected privacy policy to ascertain whether entity has documented guidelines on notifying customers and other stakeholders in case of a breach.	No exceptions noted.
	ACF-156	Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected information security policy and vulnerability management policy to ascertain whether entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.	No exceptions noted.
	ACF-157	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected event monitoring tool configuration and logs to ascertain whether entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	No exceptions noted.
CC7.4	ACF-158	Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected incident management policy to ascertain whether entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. Trust Layer Implementation for Upfront Classification/Detection/Blocking of user inputs which are off topic and security threats on user inputs	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-159	Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected list of incidents and noted that there was no security incident reported during the audit period.	No exceptions noted.
CC7.5	ACF-160	Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected list of incidents and noted that there was no security incident reported during the audit period.	No exceptions noted.
	ACF-161	Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Backup policy to ascertain whether entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	No exceptions noted.
	ACF-162	Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inquired with the HOE and Management regarding the control activity to ascertain that the control operates as described. Inspected business continuity policy and plan to ascertain whether entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	No exceptions noted.
	ACF-163	Entity has documented policies and procedures that establish guidelines for continuing business	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		operations and facilitate the application of contingency planning controls.	Inspected business continuity policy and plan to ascertain whether entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	
CC8.1	ACF-164	Entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected asset inventory to ascertain whether entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	No exceptions noted.
	ACF-165	Entity has documented policies and procedures to manage changes to its operating environment.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected change management policy and SDLC process document to ascertain whether entity has documented policies and procedures to manage changes to its operating environment.	No exceptions noted.
	ACF-166	Entity has procedures to govern changes to its operating environment.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected change management policy and SDLC process document to ascertain whether entity has procedures to govern changes to its operating environment. Entity also complies with client's change management policy where applicable.	No exceptions noted.
	ACF-167	Entity has established procedures for approval when implementing changes to the operating environment.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected <Secure Development Policy>, < Release Management Policy> and <Change Management Policy> to ascertain whether	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
			entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	
CC9.1	ACF-168	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected risk register to ascertain whether entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	No exceptions noted.
	ACF-169	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected documented risk mitigation strategy within risk register to ascertain whether each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	No exceptions noted.
	ACF-170	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest security assessment report to ascertain whether entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	No exceptions noted.
	ACF-171	Entity has a documented policy on managing Data Backups and makes	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Backup policy to ascertain whether entity has a	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		it available for all relevant staff on the company employee portal.	documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	
	ACF-172	Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected backup configuration and logs to ascertain whether entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups. Dedicated Environments are deployed using Infrastructure as a Code (IaaC) with a VPC level Isolation for clients with necessary provisions for Disaster Recovery and Backups.	No exceptions noted.
	ACF-173	Entity tests backup information periodically to verify media reliability and information integrity.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest back restoration logs to ascertain whether entity tests backup information periodically to verify media reliability and information integrity.	No exceptions noted.
	ACF-174	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected event monitoring tool configuration and logs to ascertain whether entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	No exceptions noted.
	ACF-175	Entity has documented policies and procedures that describe how to identify risks to business objectives	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements.	Inspected risk management policy to ascertain whether entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the entity's service commitments and system requirements.	
CC9.2	ACF-176	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected vendor risk assessment forms to ascertain whether entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	No exceptions noted.
	ACF-177	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected risk management policy to ascertain whether entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the entity's service commitments and system requirements.	No exceptions noted.
	ACF-178	Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected vendor management policy to ascertain whether entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors.	No exceptions noted.
A1.1	ACF-179	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to	Inquired with the management regarding the control activity to ascertain that the control operates as described.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Inspected event monitoring tool configuration and logs to ascertain whether entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	
A1.2	ACF-180	Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Backup policy to ascertain whether entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	No exceptions noted.
	ACF-181	Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected backup configuration and logs to ascertain whether entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups. Dedicated Environments are deployed using Infrastructure as a Code (IaaC) with a VPC level Isolation for clients with necessary provisions for Disaster Recovery and Backups.	No exceptions noted.
	ACF-182	Entity tests backup information periodically to verify media reliability and information integrity.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest back restoration logs to ascertain whether entity tests backup information periodically to verify media reliability and information integrity.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-183	Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected business continuity policy and plan to ascertain whether entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	No exceptions noted.
	ACF-184	Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected business continuity policy and plan to ascertain whether entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	No exceptions noted.
A1.3	ACF-185	Entity tests backup information periodically to verify media reliability and information integrity.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected latest back restoration logs to ascertain whether entity tests backup information periodically to verify media reliability and information integrity.	No exceptions noted.
	ACF-186	Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected BCP plan and test report to ascertain whether entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
			Dedicated Environments are deployed using Infrastructure as a Code (IaaC) with a VPC level Isolation for clients with necessary provisions for Business Continuity and Disaster Recovery	
	ACF-187	Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected BCP plan and test report to ascertain whether entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan. Dedicated Environments are deployed using Infrastructure as a Code (IaaC) with a VPC level Isolation for clients with necessary provisions for Business Continuity and Disaster Recovery	No exceptions noted.
	ACF-188	Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected business continuity policy and plan to ascertain whether entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	No exceptions noted.
C1.1	ACF-189	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample new joiners, policy acceptance logs and HR policies to ascertain whether entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-190	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample employees, policy acceptance logs and HR policies information to ascertain whether entity has established procedures for staff to acknowledge applicable company policies periodically.	No exceptions noted.
	ACF-191	Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected, for sample endpoint, encryption status to ascertain whether entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	No exceptions noted.
	ACF-192	Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected encryption status of production databases to ascertain whether entity has set up cryptographic mechanisms to encrypt all production databases that store customer data at rest.	No exceptions noted.
	ACF-193	Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected Information Security Policy to ascertain whether entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems.	No exceptions noted.
	ACF-194	Entity performs physical and/or logical labelling of information	Inquired with the <HOE/Privacy officer> regarding the control activity to ascertain that the control operates as described.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		systems as per the guidelines documented policy defined for data classification.	Inspected <Organization of Information Security Policy>, Client Agreements and Employee Agreements to ascertain whether entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems.	
C1.2	ACF-195	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected asset disposal policy to ascertain whether entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	No exceptions noted.
	ACF-196	Entity has a documented policy outlining guidelines for the disposal and retention of information.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Inspected data disposal and retention policy to ascertain whether entity has a documented policy outlining guidelines for the disposal and retention of information.	No exceptions noted.
P1.1	ACF-197	Entity maintains a comprehensive Privacy Policy published on Collation.AI.ai website describing data collection practices, use purposes, disclosure practices, data subject rights, and contact information for privacy inquiries.	Browsed and read through their customer facing privacy policy. Tested the control for a representative sample period within the audit timeframe and confirmed availability of Privacy Policy at all times.	No exceptions noted.
	ACF-198	Entity provides clear notice to data subjects at point of collection describing what personal information is collected, purpose of	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Privacy handling policy/procedure documentation to verify it addresses the stated control objective with respect to	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		collection, and how information will be used and shared.	Customers and Employee data. Tested the control for a representative sample period within the audit timeframe.	
	ACF-199	Entity reviews and updates Privacy Policy annually or when material changes occur to privacy practices, with version history maintained and changes communicated to affected data subjects.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Privacy handling policy/procedure/change log to verify it addresses the stated control objective with respect to Customers and Employee data. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-200	Entity provides notice to customers within 30 days prior to implementing material changes to privacy practices through email notifications and prominent website announcements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Privacy handling policy/procedure/change log to verify it addresses the stated control objective with respect to Customers and Employee data. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-202	Entity includes within the Privacy Policy information about AI processing activities, LLM Gateway usage, third-party AI providers (OpenAI/Anthropic), and data protection measures.	Read through the Privacy Policy regarding the control activity to ascertain that the control operates as described. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-203	Entity provides layered privacy notices with short-form summaries for quick understanding and detailed full notices for comprehensive information about privacy practices.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Privacy policy to verify it addresses the stated control objective with respect to Customers and Employee data. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
P1.2	ACF-204	Entity obtains explicit opt-in consent from data subjects before collecting personal information for	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Privacy handling policy/procedure/change log to verify it	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		AI-assisted development services with clear explanation of processing purposes.	addresses the stated control objective with respect to Customers and Employee data. Tested the control for a representative sample period within the audit timeframe.	
	ACF-205	Entity provides data subjects with granular consent choices allowing separate consent decisions for different processing purposes including analytics, marketing communications, and third-party sharing.	Inquired with the management regarding the design and implementation of the control. Inspected vendor contracts, due diligence documentation, and assessment reports. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-206	Entity documents legal basis for all personal information processing activities including consent, contract performance, legitimate interests, or legal obligations per applicable privacy regulations.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Privacy handling policy/procedure/change log to verify it addresses the stated control objective with respect to Customers and Employee data. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-207	Entity maintains consent records capturing consent timestamp, scope of consent, method of consent collection, and version of privacy notice presented at time of consent.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Privacy handling policy/procedure/change log to verify it addresses the stated control objective with respect to Customers and Employee data. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-208	Entity allows data subjects to withdraw consent at any time through self-service mechanisms in user account settings with processing ceased within 48 hours of withdrawal.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected their self-service DASR Konfirmity Module to verify it addresses the stated control objective with respect to Customers and Employee data. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-209	Entity communicates consequences of withholding or withdrawing consent including potential inability to provide certain services or features requiring the personal information.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Privacy handling policy/procedure/change log to verify it addresses the stated control objective with respect to Customers and Employee data. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-210	Entity obtains parental consent before collecting personal information from individual's underage of majority in applicable jurisdictions, with age verification mechanisms implemented.	Inquired with the management regarding the control activity to ascertain that the control operates as described. The client is an <Private Wealth reporting and Insights company> and the nature of business ensures that they do not deal with underage or do not need age verification. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
P2.1	ACF-211	Entity limits personal information collection to data elements necessary for providing Private Wealth reporting and Insights services and platform functionality (purpose limitation principle).	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Privacy handling policy/procedure/change log/collection and storage of privacy information to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-212	Entity documents purpose specifications for each category of personal information collected including user account data, authentication credentials, usage analytics, and support communications.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Privacy handling policy/procedure/change log/collection and storage of privacy information to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-213	Entity prohibits collection of sensitive personal information including health data, financial account numbers, biometric data,	Inquired with the management regarding the control activity to ascertain that the control operates as described. The client is an <Private Wealth reporting and insights company> and the nature of business ensures that they do not deal with mentioned data points. Where needed, they conduct DPIA.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		or government identifiers unless explicitly required and authorized.	Tested the control for a representative sample period within the audit timeframe.	
	ACF-214	Entity conducts Privacy Impact Assessments (PIAs) before implementing new processing activities involving personal information to evaluate privacy risks and mitigation measures.	Inquired with the management regarding the control activity to ascertain that the control operates as described. The client is an < Private Wealth reporting and insights company > and the nature of business ensures that they do not deal with privacy related data. Each client / project goes through DPIA process where applicable. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-215	Entity reviews data collection practices quarterly to identify and eliminate collection of unnecessary personal information implementing data minimization principles.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Quarterly User Access Review Report to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-216	Entity trains employees on purpose limitation requirements ensuring personal information is not collected beyond stated purposes without updated consent and privacy notice.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Employee Awareness Report which includes 'Privacy Practices' to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
P3.1	ACF-217	Entity uses personal information only for purposes disclosed in Privacy Policy and consented to by data subjects, prohibiting secondary uses without additional consent.	Inquired with the management regarding the control activity to ascertain that the control operates as described. The client is an <Private Wealth reporting and insights company > and the 'nature of business', 'access of client data' and existing privacy documentation verifies usages of personal information for stated purposes. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-218	Entity implements technical controls preventing unauthorized	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		use of personal information including access restrictions, data masking, and audit logging of all data access.	Production resource access restrictions, current accesses, data masking and encryption and audit logging to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	
	ACF-219	Entity prohibits use of customer personal information for AI model training purposes with contractual protections ensuring OpenAI and Anthropic do not retain or train on customer data.	Inquired with the management regarding the control activity to ascertain that the control operates as described. The company is a user of Ai models and does not train any models on customer data. Also, Inspected LLM Gateway Implementation details to verify that none of confidential client details are passed on to existing integrated models thereby addressing the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-220	Entity conducts quarterly privacy compliance audits reviewing actual personal information usage against stated purposes and consent records to identify deviations.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Quarterly User Access Review Report to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-221	Entity implements purpose-binding controls in application code restricting personal information access and processing to functions aligned with collected purposes.	Inquired with the management regarding the control activity to ascertain that the control operates as described. The client is an <Private Wealth reporting and insights company > and the 'nature of business', 'access of client data' and existing privacy documentation verifies restrictions on usages of personal information. Also, Inspected LLM Gateway Implementation details to verify that client-stated data points or access methods at are not passed on to existing integrated models thereby addressing the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-222	Entity maintains data flow documentation mapping personal information flows from collection	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Privacy handling policy/procedure/data flow documentation	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		through processing to disposal ensuring alignment with stated purposes.	and Architecture Documents to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	
P3.2	ACF-223	Entity has documented Data Retention Policy specifying retention periods for each category of personal information aligned with business needs and regulatory requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Backup Data Management Procedure> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-224	Entity retains user account information for duration of active account plus 7 years after account closure to meet contractual and legal obligations including tax and audit requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Backup Data Management Procedure> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-225	Entity implements automated data retention enforcement through Azure Bucket lifecycle policies and database retention rules ensuring personal information is deleted upon expiration.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Backup Data Management Procedure> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-226	Entity provides data subjects with information about retention periods in Privacy Policy and responds to inquiries about how long specific personal information will be retained.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Privacy handling policy/Data Subject Access Request procedure to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-227	Entity conducts annual retention period reviews assessing whether	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		established retention periods remain appropriate and adjusting based on legal requirements and business needs.	the <Backup Data Management Procedure> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	
	ACF-228	Entity securely deletes personal information at end of retention period using cryptographic erasure for encrypted data and multi-pass wiping for unencrypted storage.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Backup Data Management Procedure> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
P4.1	ACF-229	Entity restricts access to personal information based on job role and business need implementing role-based access controls with quarterly access reviews.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Quarterly User Access Review Report to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-230	Entity requires multi-factor authentication for all access to systems containing personal information using Azure or Google Workspace IAM.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Access Control Policy / Quarterly User Access Review Report to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-231	Entity logs all access to personal information capturing user identity, timestamp, data accessed, and purpose of access for audit trail and accountability.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Access Control Policy / Quarterly User Access Review Report to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-232	Entity prohibits bulk export or mass download of personal information without explicit authorization from	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Access Control Policy / Quarterly User Access Review	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		Privacy Officer and documented business justification.	Report/ Audit Logs to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	
	ACF-233	Entity implements data loss prevention (DLP) controls preventing unauthorized transmission of personal information via email, removable media, or unapproved cloud services.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Access Control Policy to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-234	Entity disposes of personal information in accordance with Data Retention Policy using secure deletion methods ensuring data cannot be recovered or reconstructed.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Backup Data Management Procedure> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
P4.2	ACF-235	Entity maintains privacy incident register documenting all unauthorized disclosures including incident date, affected data subjects, data categories, root cause, and remediation actions.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Access Control Policy / Quarterly User Access Review Report/Incident Register to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-236	Entity classifies privacy incidents by severity based on volume of affected individuals, sensitivity of data, and potential harm to data subjects determining notification obligations.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Access Control Policy / Quarterly User Access Review Report/Incident Register to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-237	Entity notifies affected data subjects of unauthorized disclosures within 72 hours when required by applicable privacy regulations (GDPR, CCPA, etc.) providing incident details and remediation steps.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Incident Management Policy / Procedure/Incident Register to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-238	Entity notifies relevant supervisory authorities of privacy breaches within regulatory timeframes (72 hours for GDPR) with comprehensive incident reports including impact assessment.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Incident Management Policy / Procedure/Incident Register to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-239	Entity conducts root cause analysis for all privacy incidents identifying control failures and implementing corrective actions to prevent recurrence.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Incident Management Policy / Procedure/Incident Register to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-240	Entity provides annual privacy incident summary to senior management and board reporting incident trends, systemic issues, and privacy program effectiveness.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Incident Management Policy / Procedure/Incident Register to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
P5.1	ACF-241	Entity provides authenticated users with self-service access to their personal information through account settings interface enabling	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Access Control Policy / Procedure/Account Management related Customer Support Tickets to verify it addresses the	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		review of profile data, preferences, and usage history.	stated control objective. Tested the control for a representative sample period within the audit timeframe.	
	ACF-242	Entity responds to data subject access requests (DSARs) within 30 days providing complete copy of personal information in portable electronic format (JSON or CSV).	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Konfirmity DSAR Module including requests, to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-243	Entity implements identity verification procedures for access requests received outside platform requiring government-issued ID verification before disclosing personal information.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Access Control Policy / Quarterly User Access Review Report/ Konfirmity DSAR Module including requests, to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-244	Entity documents reasons for denying or restricting access requests including legal prohibitions, third-party rights, or security concerns with explanations provided to data subjects.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Access Control Policy / Quarterly User Access Review Report/ Konfirmity DSAR Module including requests, to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-245	Entity provides personal information in clear, understandable format with explanations of data categories, processing purposes, and retention periods to enhance transparency.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Access Control Policy / Quarterly User Access Review Report/ Konfirmity DSAR Module including requests, to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-246	Entity maintains DSAR tracking system documenting all access requests, response actions and any	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Konfirmity DSAR Module including requests, to verify it	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		denials with justifications for audit purposes.	addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	
P5.2	ACF-247	Entity enables data subjects to correct inaccurate personal information through self-service account settings with immediate updates reflected across all systems.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Client Platform/Account Management related Customer Support Tickets to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-248	Entity responds to correction requests within 30 days validating requested changes and updating personal information across all systems and backups.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Konfirmity DSAR Module including requests, to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-249	Entity notifies third parties to whom inaccurate personal information was disclosed of corrections made enabling them to update their records accordingly.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Access Control Policy / Quarterly User Access Review Report/ Konfirmity DSAR Module including requests, to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-250	Entity documents reasons for denying correction requests including lack of verification, conflicts with legal obligations, or insufficient evidence supporting requested change.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Access Control Policy / Quarterly User Access Review Report/ Konfirmity DSAR Module including requests, to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-251	Entity allows data subjects to supplement incomplete personal information providing additional	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Access Control Policy / Quarterly User Access Review Report/ Konfirmity DSAR Module including requests, to verify it	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		context or information to existing records.	addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	
	ACF-252	Entity maintains audit trail of all personal information corrections documenting original value, corrected value, correction date, and requesting party for accountability.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Access Control Policy / Quarterly User Access Review Report/ Konfirmity DSAR Module including requests, to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
P6.1	ACF-253	Entity obtains explicit consent before disclosing personal information to third parties for purposes beyond service provision including marketing partnerships or data analytics.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Privacy Policy and Terms of Use to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-254	Entity provides data subjects with detailed information about third-party recipients including recipient identity, data to be shared, and purpose of disclosure before obtaining consent.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Privacy Policy and Trust Center to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-255	Entity maintains third-party disclosure agreements documenting data protection obligations, permitted uses, security requirements, and audit rights for all recipients of personal information.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <DPIA>, <Backup Data Management Procedure>, <Customer Contracts> and Third-Party Security Posturing to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-256	Entity allows data subjects to withdraw consent for third-party	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		disclosures at any time ceasing further disclosures within 48 hours of withdrawal request.	the Konfirmity DSAR Module including requests, to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	
	ACF-257	Entity conducts annual reviews of third-party recipients validating continued need for disclosures and assessing recipient compliance with data protection obligations.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <DPIA>, <Supplier Relationship Policy> and Third-Party Security Posturing module in Konfirmity to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-258	Entity prohibits onward transfers of personal information by third-party recipients without Entity's explicit authorization and data subject consent.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <DPIA>, <Supplier Relationship Policy>, < Risk Management Policy> and <Risk Register> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
P6.2	ACF-259	Entity documents all authorized third-party disclosures in disclosure register including Azure infrastructure services	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <DPIA>, <Supplier Relationship Policy> and Third-Party Security Posturing module in Konfirmity to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-260	Entity maintains current Data Processing Agreements (DPAs) with all third-party recipients documenting their roles as processors or controllers and data protection commitments.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <DPIA>, <Supplier Relationship Policy> and Third-Party Security Posturing module in Konfirmity to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-261	Entity requires all third-party recipients to maintain SOC 2 Type II	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		or equivalent certifications validating their security and privacy control effectiveness.	the <DPIA>, <Supplier Relationship Policy> and Third-Party Security Posturing module in Konfirmity to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	
	ACF-262	Entity updates Privacy Policy promptly when engaging new third-party recipients of personal information providing notice to data subjects of new disclosures.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Privacy Policy>, <Terms of Use> changelog and subsequent communication records to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-263	Entity monitors third-party compliance with data protection obligations through periodic audits, security assessments, and review of certification reports.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Third-Party Security Posturing module in Konfirmity to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
P7.1	ACF-264	Entity implements comprehensive quality controls ensuring personal information is accurate, complete, and current throughout its lifecycle from collection to disposal.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the < Access Control Policy> and <User Access Review Report> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-265	Entity validates personal information at point of collection using format validation, domain verification, and reasonableness checks to ensure data quality.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Client Platform, <Secure Development Policy>, <Release Management Policy> and <Change Management Policy and records> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-266	Entity provides data subjects with mechanisms to review and update their personal information regularly ensuring accuracy and currency of stored data.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Client Platform, User Profile Management and Customer Support tickets related to updating of personal information to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-267	Entity implements data quality monitoring identifying and remediating incomplete, duplicate, or inconsistent personal information records.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Client Platform, <Task Management Board - clickup>, <Release Management Policy> and <Change Management Policy and records> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-268	Entity establishes data quality metrics including accuracy rates, completeness percentages, and currency measures with quarterly reporting to management.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Management Review Meeting Minutes to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-269	Entity documents data quality procedures including validation rules, correction processes, and quality assurance testing aligned with ISO 27001:2022 requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Operations Security Policy>, <Release Management Policy> and <Change Management Policy and records> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
P8.1	ACF-270	Entity maintains privacy@Collation.AI.ai email address and web form enabling data subjects to submit privacy	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Konfirmity DSAR module that includes internal as well as external interfaces to verify it addresses the stated control	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		inquiries, complaints, and rights requests.	objective. Tested the control for a representative sample period within the audit timeframe.	
	ACF-271	Entity responds to privacy inquiries within 5 business days acknowledging receipt and providing expected resolution timeline aligned with regulatory requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Konfirmity DSAR module to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-272	Entity designates Privacy Officer responsible for coordinating responses to privacy complaints and ensuring timely resolution of privacy issues.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Infosec Organization Structure and <Organization of Information Security Policy> that includes internal as well as external interfaces to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-273	Entity documents all privacy complaints in tracking system capturing complaint details, investigation findings, resolution actions, and data subject communications.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Konfirmity DSAR module to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-274	Entity escalates unresolved privacy complaints to senior management and provides data subjects with information about regulatory complaint options if internal resolution fails.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Konfirmity DSAR module and Management Review Meeting minutes to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-275	Entity conducts quarterly analysis of privacy complaints identifying	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		systemic issues, control deficiencies, and improvement opportunities with corrective actions implemented.	the Konfirmity DSAR module, User Access Review reports and Management Review Meeting minutes to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	
	ACF-276	Entity monitors compliance with privacy commitments through internal audits, annual external audits, and continuous monitoring of privacy controls.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Konfirmity DSAR module, Internal Audit report and Management Review Meeting minutes to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
PI1.1	ACF-277	Entity maintains comprehensive documentation of the <Collation AI> platform processing objectives, including data input requirements, processing logic, output specifications, and quality standards.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Task Management Board, Technology Architecture, System Specifications and Documentation to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-278	Entity documents data definitions and specifications for all processing activities including client source code inputs, AI model interactions, and generated code outputs with version control.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Task Management Board, Static Code Analysis Report, AI Gateway Logs and CloudWatch to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-279	Entity provides clear service documentation to customers describing CollationAI platform capabilities, processing workflows, data handling procedures, and	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the website, client onboarding records and <Backup Data Management Procedure> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		expected service outputs through Collation.AI.ai website.		
	ACF-280	Entity maintains API documentation for all system interfaces including input validation requirements, expected response formats, error handling procedures, and integration guidelines.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Task Management Board, Technology Architecture, API Specifications and Documentation to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-281	Entity communicates system updates, processing changes, and feature enhancements to customers through release notes, documentation updates, and proactive notifications.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Release Notes, <Release Management Policy> and <Change Management Policy and records> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-282	Entity documents processing integrity objectives in Quality Management System requirements including accuracy, completeness, timeliness, and authorization requirements.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Secure Development Policy>, <Release Management Policy>, <Change Management Policy and records> and <Backup Data Management Procedure> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
PI1.2	ACF-283	Entity implements comprehensive input validation controls for all user-submitted data including source code, configuration files, and API requests to ensure data quality and prevent injection attacks.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Secure Development Policy> and <Release Management Policy> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-284	Entity has documented procedures requiring validation of client requirements and specifications before initiating AI-assisted development work to ensure accurate understanding of processing needs.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Secure Development Policy>, <Change Management Policy> and <Release Management Policy> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-285	Entity implements automated data validation rules for API endpoints checking data type conformity, required field presence, value range constraints, and format specifications.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Secure Development Policy>, <Change Management Policy> and <Release Management Policy> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-286	Entity maintains data quality controls for client source code inputs including syntax validation, encoding verification, and completeness checks before processing through AI models.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Secure Development Policy>, <Change Management Policy> , <Release Management Policy> and Static Code Analysis Report to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-287	Entity implements authorization controls ensuring only authenticated and authorized users can submit processing requests and input data to the CollationAI platform.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Secure Development Policy> and < Access Control Policy> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-288	Entity logs all input submissions with timestamps, user identification, and validation results	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Task Management Board, AI Gateway Logs and CloudWatch to verify it addresses the stated control objective. Tested the	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		to support auditability and error investigation.	control for a representative sample period within the audit timeframe.	
PI1.3	ACF-289	Entity has implemented comprehensive LLM Gateway processing controls that redact confidential information before data reaches external AI models (OpenAI/Anthropic), ensuring processing integrity and data protection.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Task Management Board, AI Gateway Logs and CloudWatch to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-290	Entity implements session-based isolation for all AI processing activities using dedicated directory structures (user{userId}/chat{sessionId}/) preventing cross-contamination between client workloads.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Task Management Board, AI Gateway Logs and CloudWatch to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-291	Entity maintains processing audit trails capturing all AI model interactions including input prompts (post-redaction), model responses, processing timestamps, and session identifiers.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Task Management Board, AI Gateway Logs and CloudWatch to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-292	Entity implements processing timeout controls and resource limits preventing infinite loops, runaway processes, and resource exhaustion that could impact service quality.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Task Management Board, AI Gateway Logs and CloudWatch to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-293	Entity has documented Standard Operating Procedures (SOPs) for AI-assisted code generation workflows including quality checkpoints, human review requirements, and output validation steps.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Secure Development Policy> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-294	Entity implements version control for all processing logic and AI model configurations enabling traceability of processing changes and rollback capability if issues are identified.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Secure Development Policy>, <Change Management Policy> and <Release Management Policy> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-295	Entity enforces processing integrity through Infrastructure as Code (IaC) using Terraform ensuring consistent, repeatable, and auditable deployment of processing infrastructure.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Secure Development Policy>, <Change Management Policy> and <Release Management Policy> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
PI1.4	ACF-296	Entity implements output validation controls verifying AI-generated code meets syntax requirements, functional specifications, and quality standards before delivery to clients.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Secure Development Policy>, <Change Management Policy> , <Release Management Policy> and Static Code Analysis Report to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-297	Entity maintains Service Level Objectives (SLOs) for processing timeliness including API response times (95th percentile < 2 seconds)	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Secure Development Policy>, <Change Management Policy> , <Release Management Policy>, <Operations Security Policy> and Incident Register to verify it addresses the stated	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		and job completion times aligned with customer expectations.	control objective. Tested the control for a representative sample period within the audit timeframe.	
	ACF-298	Entity implements automated testing of generated code outputs including unit test execution, integration testing, and quality gate validation before marking processing complete.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Secure Development Policy>, <Change Management Policy> , <Release Management Policy and records>, <Task Management Board> and Incident Register to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-299	Entity provides real-time processing status updates to users through application interface enabling visibility into job progress, completion status, and any processing errors.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Change Management Policy>, Client Platform and Incident Register to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-300	Entity implements output completeness checks verifying all requested processing components are generated and delivered without truncation or data loss.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Secure Development Policy>, <Change Management Policy> , <Release Management Policy and records>, <Task Management Board> and Incident Register to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-301	Entity maintains output delivery logs capturing successful deliveries, failed deliveries, retry attempts, and final disposition for all processing jobs.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Secure Development Policy>, <Change Management Policy> , <Release Management Policy and records>, <Task Management Board> and Incident Register to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
	ACF-302	Entity implements error handling and user notification procedures ensuring clients are promptly informed of processing failures with actionable error messages and resolution guidance.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Secure Development Policy>, <Change Management Policy> , <Release Management Policy and records>, <Task Management Board> and Incident Register to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
PI1.5	ACF-303	Entity implements encrypted storage for all processing data including inputs, intermediate processing artifacts, and outputs using AES-256 encryption with Azure KMS customer-managed keys.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Secure Development Policy>, <Encryption Policy> , Azure Production Resources' encryption status and Incident Register to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-304	Entity maintains data integrity controls including checksums and hash verification for stored data ensuring detection of any corruption or unauthorized modification.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the Release Management Procedure including Software Quality management and <Backup Data Management Procedure including Dry run records> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-305	Entity implements retention policies for processing data aligned with contractual requirements and regulatory obligations with automated lifecycle management and secure deletion procedures.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Backup Data Management Procedure including Dry run records> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-306	Entity stores all client processing data within dedicated instances with session-based file system	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the client platform, access controls, physical and logical	No exceptions noted.

TSC Ref. #	Control Ref. #	Control Activity as specified by Collation.AI	Testing Performed	Test Results
		isolation preventing unauthorized access to other clients' data.	separation of client data and <Backup Data Management Procedure> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	
	ACF-307	Entity implements automated backup procedures for processing data with point-in-time recovery capability ensuring data can be restored if corruption or loss occurs.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Backup Data Management Procedure including Dry run records> to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.
	ACF-308	Entity maintains storage audit logs capturing all data access, modifications, and deletions with user attribution and timestamp information for accountability.	Inquired with the management regarding the control activity to ascertain that the control operates as described. Also, Inspected the <Backup Data Management Procedure including Dry run records> and CloudWatch to verify it addresses the stated control objective. Tested the control for a representative sample period within the audit timeframe.	No exceptions noted.