



Talentas Technology's

SOC 2 Type 1 Report on the description of the Offshore Software Development and Managed services and on the Suitability of the Design Effectiveness of controls relevant to Security, Availability and Confidentiality Trust Service Criteria as of April 07, 2025.

Statement of Confidentiality

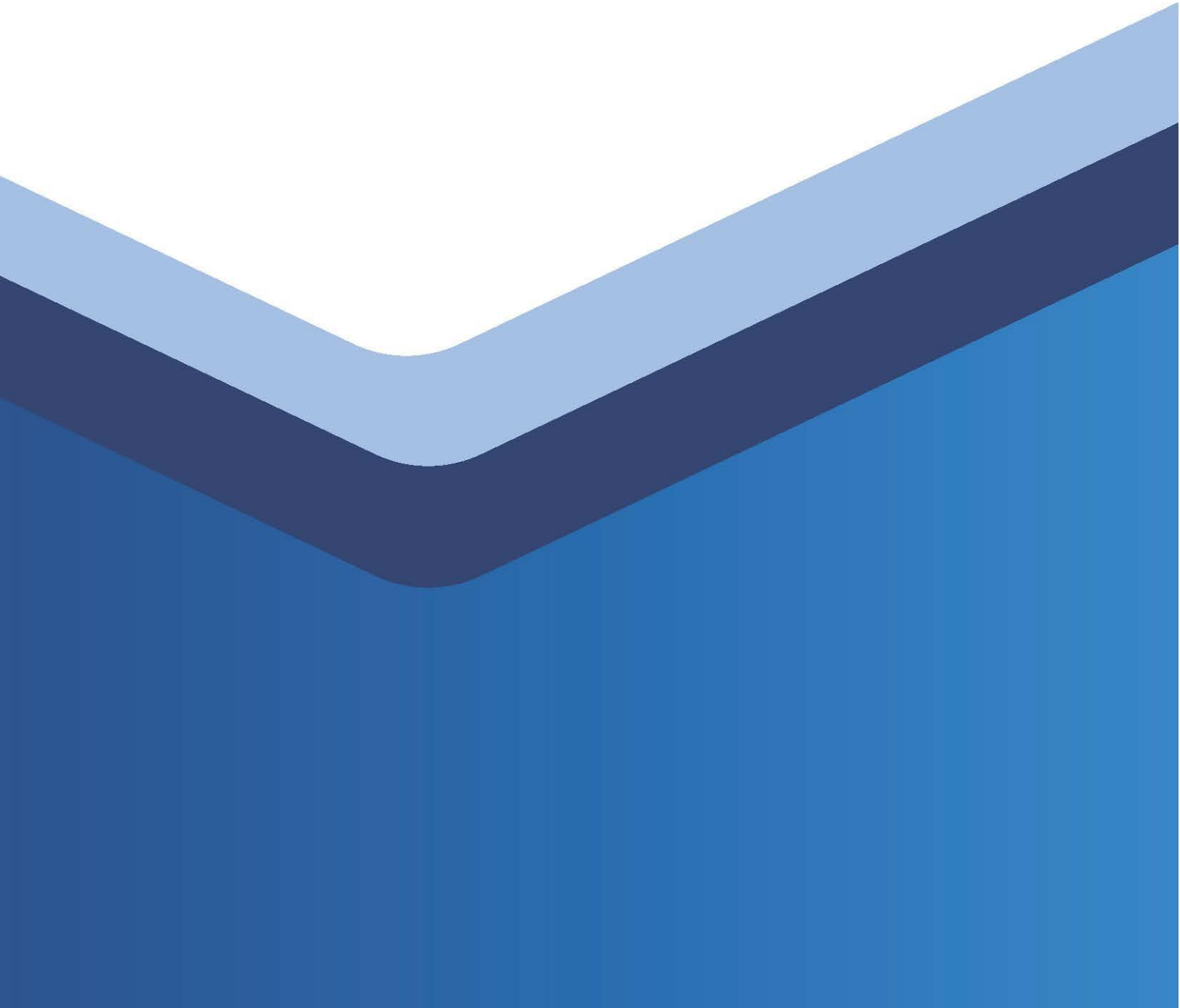
This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of the Service Organization, User Entities of the Service Organization's system related to the Offshore Software Development and Managed services relevant to Security, Availability and Confidentiality as of April 07, 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

1.	Section 1 Independent Service Auditors' Report	5
2.	Section 2 Assertion by Management of Talentas Technology	9
3.	Section 3 System Description Provided by Service Organization.....	11
4.	Section 4 Information Provided by Service Auditor Except for Applicable Trust Services Criteria and Controls	33

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT



1. Independent Service Auditors' Report

Independent Service Auditors' Report on Description of Talentas Technology 's System and the Suitability of the Design and Operating Effectiveness of Controls relevant to Security, Availability and Confidentiality trust service criteria.

To the Management of Talentas Technology

Scope

We have examined Talentas Technology's accompanying description of its Offshore Software Development and Managed services system found in Talentas Technology's Offshore Software Development and Managed services system titled Talentas Technology's Description of the Offshore Software Development and Managed services as of April 07, 2025 (description) based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022), in AICPA, Description Criteria, (description criteria) and the suitability of the design of controls stated in the description as of April 07, 2025, to provide reasonable assurance that Talentas Technology's service commitments and system requirements would be achieved based on the trust services criteria relevant to Security, Availability and Confidentiality (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022), in AICPA, Trust Services Criteria.

Talentas Technology uses a subservice organization to provide cloud and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Talentas Technology, to achieve Talentas Technology 's service commitments and system requirements based on the applicable trust services criteria. The description presents Talentas Technology's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Talentas Technology '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 also indicates that Talentas Technology's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Talentas Technology's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

Talentas Technology 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 Talentas Technology 's service commitments and system requirements would be achieved. In Section 2, Talentas Technology has provided the accompanying assertion titled Management Assertion Provided by Service Organization (assertion) about the description and the suitability of design of controls stated therein. Talentas Technology 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 of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization'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. We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

An examination of a description of a service organization's system and the suitability of the design 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.
- 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 on the applicable trust services criteria.
- evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects:

- a. the description presents Talentas Technology 's Offshore Software Development and Managed services system that was designed and implemented as of April 07, 2025 in accordance with the description criteria.
- b. the controls stated in the description were suitably designed as of April 07, 2025 to provide reasonable assurance that Talentas Technology 's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization applied the complementary controls assumed in the design of Talentas Technology 's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Talentas Technology; user entities of Talentas Technology's Offshore Software Development and Managed services system as of April 07, 2025 ; business partners of Talentas Technology subject to risks arising from interactions with the Offshore Software Development and Managed services 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, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

For,

Accorp Partners CPA LLC

Accorp Partners CPA LLC

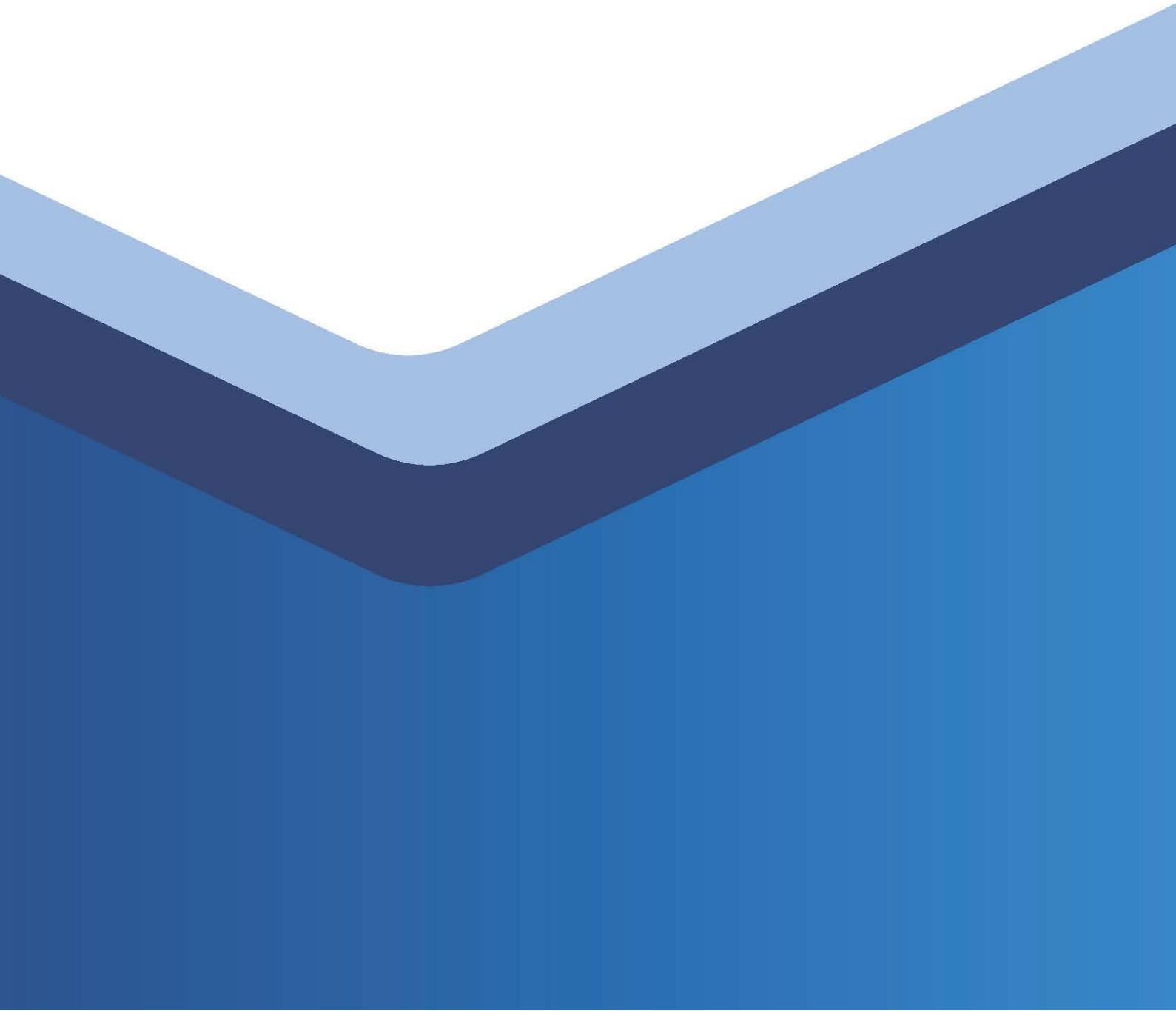
License No.: PAC-FIRM-LIC-47383

Kalispell, Montana

Date: April 16, 2025

SECTION 2

MANAGEMENT ASSERTION PROVIDED BY SERVICE ORGANIZATION



Assertion of the Management of Talentas Technology

We have prepared the accompanying description of Talentas Technology's Offshore Software Development and Managed services system titled Talentas Technology's Description of the Offshore Software Development and Managed services as of April 07, 2025 (description) based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022) , in AICPA, Description Criteria (description criteria). The description is intended to provide report users with information about the Offshore Software Development and Managed services system that may be useful when assessing the risks arising from interactions with Talentas Technology's system, particularly information about system controls that Talentas Technology 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 (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022) , in AICPA, Trust Services Criteria.

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

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

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

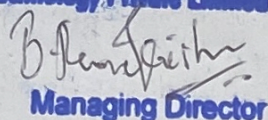
1. The description presents Talentas Technology's Offshore Software Development and Managed services system that was designed and implemented as of April 07, 2025 in accordance with the description criteria.
2. The controls stated in the description were suitably designed as of April 07, 2025 to provide reasonable assurance that Talentas Technology'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 Talentas Technology's controls throughout that period.

For Talentas Technology

For Talentas Technology Private Limited

Name:
Title:
Date:

Ramakrishna Badarathy
CEO
16-04-2025


Managing Director

SECTION 3

TALENTAS TECHNOLOGY 'S DESCRIPTION OF THE OFFSHORE SOFTWARE DEVELOPMENT AND MANAGED SERVICES





3. System Description Provided by Service Organization

3.1 Overview of the Company and Services Delivered by the Report

Talentas Technology Private Limited (hereby referred to as <Talentas>) is a global offshore software services provider specializing in secure, compliant IT solutions, including:

- **Web & Mobile Application Development, Ecommerce application** design and development for the clients.
- **BI & Data Analytics Consulting Services** – Helping clients derive value from their data.
- **Integration Services** – Provide seamless integration services through API Development and middleware development
- **QA & Testing** – Help clients test their applications.
- **Compliance-Focused IT Solutions** – Ensuring adherence to security and regulatory standards.

3.1 Components of the System used to provide services

Infrastructure

Talentas operates with a fully secured digital infrastructure designed for seamless and protected connectivity with clients. This includes:

- **Private Internet Connectivity** for dedicated and secure network access.
- **Enterprise-grade Cisco Meraki Firewall** to safeguard network traffic and prevent unauthorized access.
- **Sophos Central Endpoint Protection** deployed on all company-issued laptops, ensuring advanced threat detection and data security."

Talentas Relies on client-provided or cloud-hosted systems for service delivery.

Software

Talentas utilizes Microsoft 365 Enterprise Premium for all secure email communications and document management, featuring:

- **Enterprise-grade email security** with Microsoft Defender for Office 365
- **End-to-end encryption** for all email transmissions
- **Secure cloud documentation** via OneDrive with advanced data protection
- **Compliance-ready infrastructure** meeting global security standards (ISO 27001, SOC 2)
- **Granular access controls** and audit trails for all documents"
- No proprietary hosted applications.
- Sprinto (subservice provider) for continuous compliance monitoring.

Supporting Tools	
System / Application	Business Function / Description
Sprinto	Provide continuous compliance monitoring of the company's system.
O365 Premium	Office communication services
Azure AD	Secure authentication



People

Talentas has established a robust organizational framework with clearly defined functional divisions to maintain operational excellence. The personnel have also been assigned the following key roles:

Role	Responsibilities
Senior Management	Oversee risk management, resource allocation
Information Security Officer (ISO)	Risk assessment, security controls
Compliance Program Manager	Policy enforcement, audit coordination
System Users	Adherence to security policies, annual training

Procedures and Policies

Formal policies and procedures have been established to support the Talentas services. These policies cover:

- **Access Control** (RBAC, least privilege)
- **Incident Management** (reporting & resolution)
- **Data Protection** (encryption, classification)
- **Vendor Risk Management** (third-party assessments)

All employees acknowledge policies upon hiring and annually via **Sprinto**.

Data Management

All data that is managed, processed, and stored as a part of the Talentas analytics and consulting services 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.

Further, all customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. The access to the customers' critical data is only for a limited time period, during their onboarding phase which is revoked after onboarding is successfully completed.

Security Controls:

Logical Access

- Multi-factor authentication (MFA) enforced.
- Access reviews conducted quarterly.

Physical Security

- No owned data centres – Relies on client/cloud infrastructure.

Change Management

- No codebase maintenance (analytics/consulting only).



Risk Assessment

- **Annual risk assessments** (internal/external threats).
- **Vendor Risk Management** – Critical vendors audited annually.

Trust Services Criteria (SOC 2)

Category	Scope
Security	System safeguards against unauthorized access
Confidentiality	Protection of sensitive client data
Availability	Service uptime commitments

Complementary Customer Controls

Customers must ensure:

- Access governance (user provisioning/deprovisioning).
- Incident reporting (breaches, anomalies).
- Data integrity (accuracy of shared datasets).

3.2 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. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part of Talentas Technology's description of the system. This section provides information about the five interrelated components of internal control at Talentas Technology, including:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring controls

3.3 Control Environment

Integrity & 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 Talentas Technology's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Talentas Technology'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.

Talentas Technology and its management team have 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 background checks as a part of the hiring process.

Commitment to Competence

Talentas Technology'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

Talentas Technology'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.

Talentas Technology'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.

- 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

Talentas Technology'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 Policies and Practices

Talentas Technology'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 Talentas Technology has implemented in this area are described below:

- Employees are evaluated for competence in performing their job responsibilities at the time of hiring
- New employees are required to acknowledge company policy up on hiring and re-acknowledge annually
- Performance evaluations for each employee are performed on an annual basis
- When a person is relieved of duties from the company, access to critical systems are revoked within 3 business days

Vendor Risk Assessment

Talentas Technology uses a number of vendors to meet its business objectives. Talentas Technology 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.

Talentas Technology employs several activities to effectively manage its 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, Talentas Technology assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support Talentas Technology's commitments to its customers.

If a critical vendor is unable to provide a third-party security report or assessment, Talentas Technology management meets with such vendors periodically to assess their performance, security concerns, and services. Any vendor risks identified are recorded in the risk assessment matrix, which is reviewed annually by the Senior Management of the company.

Monitoring

Talentas management monitors controls 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 are also monitored. This process is accomplished through ongoing monitoring activities, independent evaluations, or a combination of the two.

Information and Communication Systems

Talentas 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, Talentas 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.

3.4 Principal Service Commitments and System Requirements

Talentas designs its processes to meet security, availability, and confidentiality commitments, aligned with:

- Customer agreements (security obligations).
- Regulatory requirements (ISO 27001, SOC 2, etc.).

Security Commitments

- Role-Based Access Control (RBAC) - Users access only data necessary for their role.
- Network Environment Security - Strict access controls for infrastructure.
- Proactive Monitoring - Real-time alerts on system utilization and anomalies.

Operational Requirements

- Documented in policies, procedures, and contracts.
- Governed by Information Security Policies covering:
 - System design & development
 - Network management
 - Staff hiring & training

3.5 Applicable Trust Services Criteria and Related Controls

TSC Ref#	Criteria	Control#	Control Activity as specified by Talentas Technology
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values	SDC 1	The entity has a documented policy to define behavioral standards and acceptable business conduct.
		SDC 6	The entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.
		SDC 12	The entity has established procedures for staff to acknowledge applicable company policies periodically.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	SDC 24	The entity's Senior Management reviews and approves all company policies annually.
		SDC 25	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.
		SDC 26	The entity's Senior Management reviews and approves the Organizational Chart for all employees annually.
		SDC 27	The entity's Senior Management reviews and approves the "Risk Assessment Report" annually.
		SDC 29	The entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	SDC 2	Entity maintains an organizational structure to define authorities, facilitate information flow, and establish responsibilities.
		SDC 3	The entity has established procedures to communicate with staff about their roles and responsibilities.
		SDC 22	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.
		SDC 25	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

TSC Ref#	Criteria	Control#	Control Activity as specified by Talentas Technology
			ensure their continuing suitability, adequacy, and effectiveness.
		SDC 154	The entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.
		SDC 396	The entity appoints a People Operations Officer to develop and drive all personnel-related security strategies.
		SDC 397	The entity appoints a Compliance Program Manager who has delegated the responsibility of planning and implementing the internal control environment.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	SDC 4	The entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.
		SDC 5	The entity has established procedures to perform security risk screening of individuals prior to authorizing access.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives	SDC 7	The entity provides information security and privacy training to staff that is relevant to their job function.
		SDC 9	Entity requires that all employees in client serving, IT, Engineering, and Information Security roles are periodically evaluated regarding their job responsibilities.
		SDC 12	The entity has established procedures for staff to acknowledge applicable company policies periodically.
		SDC 387	The entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.
		SDC 388	Entity documents, monitors, and retains individual training activities and records.
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control	SDC 11	Entity systems generate information that is reviewed and evaluated to determine impacts on the functioning of internal controls.
		SDC 13	The entity makes all policies and procedures available to all staff members for their perusal.
		SDC 14	Entity displays the most current information about its services on its

TSC Ref#	Criteria	Control#	Control Activity as specified by Talentas Technology
			website, which is accessible to its customers.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control	SDC 1	The entity has a documented policy to define behavioral standards and acceptable business conduct.
		SDC 6	The entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.
		SDC 12	The entity has established procedures for staff to acknowledge applicable company policies periodically.
		SDC 13	The entity makes all policies and procedures available to all staff members for their perusal.
		SDC 15	The 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.
		SDC 387	The entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.
		SDC 388	Entity documents, monitors, and retains individual training activities and records.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control	SDC 14	Entity displays the most current information about its services on its website, which is accessible to its customers.
		SDC 16	The 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.
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives	SDC 18	The 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.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes	SDC 6	The entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

TSC Ref#	Criteria	Control#	Control Activity as specified by Talentas Technology
	risks as a basis for determining how the risks should be managed	SDC 18	The 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.
		SDC 19	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, Confidentiality, Processing Integrity, and Privacy of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.
		SDC 21	The entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives	SDC 20	The entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control	SDC 18	The 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.
		SDC 19	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, Confidentiality, Processing Integrity, and Privacy of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.
		SDC 21	The entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning	SDC 22	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.
		SDC 23	The entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security

TSC Ref#	Criteria	Control#	Control Activity as specified by Talentas Technology
			Officer and other stakeholders.
		SDC 24	The entity's Senior Management reviews and approves all company policies annually.
		SDC 25	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.
		SDC 26	The entity's Senior Management reviews and approves the Organizational Chart for all employees annually.
		SDC 27	The entity's Senior Management reviews and approves the "Risk Assessment Report" annually.
		SDC 29	The entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.
		SDC 30	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.
		SDC 55	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.
		SDC 56	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.
		SDC 154	The entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.
		SDC 389	Entity periodically updates and reviews the inventory of systems as a part of installations, removals and system updates.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate	SDC 15	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.
		SDC 23	The entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security

TSC Ref#	Criteria	Control#	Control Activity as specified by Talentas Technology
			program to the Information Security Officer and other stakeholders.
		SDC 24	The entity's Senior Management reviews and approves all company policies annually.
		SDC 25	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.
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels	SDC 31	The entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.
		SDC 32	Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.
		SDC 105	The entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives	SDC 23	The entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.
		SDC 24	The entity's Senior Management reviews and approves all company policies annually.
		SDC 25	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.
		SDC 26	The entity's Senior Management reviews and approves the Organizational Chart for all employees annually.
		SDC 27	The entity's Senior Management reviews and approves the "Risk Assessment Report" annually.
		SDC 28	The entity's Infosec officer reviews and approves the list of people with access to the production console annually.

TSC Ref#	Criteria	Control#	Control Activity as specified by Talentas Technology
		SDC 29	The entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.
		SDC 30	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.
		SDC 31	The entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action	SDC 6	The entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.
		SDC 12	The entity has established procedures for staff to acknowledge applicable company policies periodically.
		SDC 13	The entity makes all policies and procedures available to all staff members for their perusal.
		SDC 31	The entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.
CC6.1	<i>The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</i>	SDC 33	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.
		SDC 34	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.
		SDC 38	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.
		SDC 42	The 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.
		SDC 43	The entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative

TSC Ref#	Criteria	Control#	Control Activity as specified by Talentas Technology
			access to the critical systems is restricted to only those individuals who require such access to perform their job functions.
		SDC 108	The entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed.
		SDC 135	The entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.
CC6.2	<i>Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.</i>	SDC 33	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.
		SDC 34	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.
		SDC 35	Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.
CC6.3	<i>The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.</i>	SDC 33	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.
		SDC 34	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.
		SDC 35	Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.
		SDC 37	Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.
		SDC 42	The entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those

TSC Ref#	Criteria	Control#	Control Activity as specified by Talentas Technology
			individuals who require such access to perform their job functions.
		SDC 43	The 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.
CC6.4	<i>The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.</i>	N/A	The entity does not have any physical offices or physical data centers. Hence, not applicable.
CC6.5	<i>The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.</i>	SDC 48	The entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.
CC6.6	<i>The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</i>	SDC 38	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.
		SDC 39	Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.
		SDC 44	Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.
		SDC 45	Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.
		SDC 46	The 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.
		SDC 47	Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.

TSC Ref#	Criteria	Control#	Control Activity as specified by Talentas Technology
		SDC 50	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.
		SDC 104	The entity has documented policies and procedures for endpoint security and related controls.
		SDC 141	Entity requires that all critical endpoints be encrypted to protect them from unauthorized access.
		SDC 390	The entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.
CC6.7	<i>The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.</i>	SDC 45	Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.
		SDC 49	The entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.
		SDC 51	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.
		SDC 52	The entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.
		SDC 100	Entity ensures that customer data used in non-production environments requires the same level of protection as the production environment.
		SDC 106	The entity has a documented policy to manage encryption and cryptographic protection controls.
		SDC 141	Entity requires that all critical endpoints be encrypted to protect them from unauthorized access.
CC6.8	<i>The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.</i>	SDC 46	The 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.
		SDC 50	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the

TSC Ref#	Criteria	Control#	Control Activity as specified by Talentas Technology
			Entity's cloud provider.
CC7.1	<i>To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.</i>	SDC 391	The entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.
		SDC 394	The entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.
CC7.2	<i>The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.</i>	SDC 391	The entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.
		SDC 394	The entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.
CC7.3	<i>The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.</i>	SDC 23	The entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.
		SDC 46	The 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.
		SDC 54	The 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.
		SDC 55	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.
		SDC 56	The entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.
		SDC 391	The entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.
		SDC 394	The entity's infrastructure is configured to generate audit events for actions of

TSC Ref#	Criteria	Control#	Control Activity as specified by Talentas Technology
			interest related to security for all critical systems.
CC7.4	<i>The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.</i>	SDC 23	The entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.
		SDC 53	The entity has established a policy and procedure that includes guidelines to be undertaken in response to information security incidents.
		SDC 54	The 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.
		SDC 55	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.
CC7.5	<i>The entity identifies, develops, and implements activities to recover from identified security incidents.</i>	SDC 393	The entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.
CC8.1	<i>The entity authorizes, designs, develops acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.</i>	SDC 52	The entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.
		SDC 56	The entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.
		SDC 64	The entity has documented policies and procedures to manage changes to its operating environment.
		SDC 65	The entity has procedures to govern changes to its operating environment.
		SDC 66	The entity has established procedures for approval when implementing changes to the operating environment.
CC9.1	<i>The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.</i>	SDC 18	The 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.

TSC Ref#	Criteria	Control#	Control Activity as specified by Talentas Technology
		SDC 19	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, Confidentiality, Processing Integrity, and Privacy of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.
		SDC 67	The 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	The entity assesses and manages risks associated with vendors and business partners.	SDC 21	The entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.
		SDC 67	The 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.
		SDC 68	The 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.
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	SDC 59	Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.
A1.2	The entity authorizes, designs, develops acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	SDC 59	Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.
		SDC 393	The entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

TSC Ref#	Criteria	Control#	Control Activity as specified by Talentas Technology
A1.3	<i>The entity tests recovery plan procedures supporting system recovery to meet its objectives.</i>	SDC 97	The entity has procedures to conduct regular tests and exercises that determine the effectiveness and readiness to execute the contingency plan.
		SDC 393	The entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.
C1.1	<i>The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.</i>	SDC 6	The entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.
		SDC 12	The entity has established procedures for staff to acknowledge applicable company policies periodically.
		SDC 45	Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.
		SDC 49	The entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.
		SDC 69	The entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems.
		SDC 70	Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification.
C1.2	<i>The entity disposes of confidential information to meet the entity's objectives related to confidentiality.</i>	SDC 48	The entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.
		SDC 71	The entity has a documented policy outlining guidelines for the disposal and retention of information.

[Space intentionally left blank]



SECTION 4

TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

4. Trust Services Category, Criteria, Related Controls, and Tests of Controls

4.1 Objective of Our Examination

This report is intended to provide interested parties with information about the controls at Talentas Technology that may affect the processing of user organizations' transactions and also to provide users with information about the operating effectiveness of the controls that were tested. This report, when combined with an understanding and assessment of the controls at user organizations, is intended to assist user auditors in (1) planning the audit of user organizations' financial statements and (2) assessing control risk for assertions in user organizations' financial statements that may be affected by controls at Talentas Technology.

Our testing of Talentas Technology controls was restricted to the control objectives and related controls listed in the matrices in this section of the report and was not extended to controls described in the system description but not included in the aforementioned matrices, or to controls that may be in effect at user organizations. It is each user auditor's responsibility to evaluate this information about the controls in place at each user organization. If certain complementary controls are not in place at user organizations, Talentas Technology 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 Talentas Technology our procedures included tests of the following relevant elements of the Talentas Technology control environment:

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

Such tests included inquiry of the appropriate management, supervisory, and staff personnel; observation of Talentas Technology activities and operations, inspection of Talentas Technology documents and records, and re-performance of the application of Talentas Technology 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 Talentas Technology description of the system related to Talentas Technology as well as the suitability of the design effectiveness of controls for a representative number of samples as of April 07, 2025.

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

Testing the accuracy and completeness of the information provided by Talentas Technology 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 Talentas Technology
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. Talentas Technology-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 Talentas Technology.

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 Talentas Technology. Our tests of controls were performed on controls as they existed for the period from as of April 07, 2025, and were applied to those controls relating to the trust services principles and criteria.

Tests performed on 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 reporting 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 reporting period to evidence the application of the specific control activity.
Examination of Documentation/Inspection	If the performance of the control is documented, inspected documents and reports indicate the 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. Compare 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.

4.4 Testing Procedures Performed by Independent Service Auditor

In addition to the tests listed below for each control specified by Talentas Technology, ascertained through inquiry with management and the controlling owner that each control activity listed below operated as described as of April 07, 2025.

TSC Ref	Control#	Control Activities as specified by Talentas Technology	Results of Test
CC1.1 CC2.2	SDC 1	Entity has a documented policy to define behavioral standards and acceptable business conduct.	No Exceptions Noted.
CC1.3	SDC 2	Entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.	No Exceptions Noted.
CC1.3	SDC 3	Entity has established procedures to communicate with staff about their roles and responsibilities.	No Exceptions Noted.
CC1.4	SDC 4	Entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	No Exceptions Noted.
CC1.4	SDC 5	Entity has established procedures to perform security risk screening of individuals prior to authorizing access.	No Exceptions Noted.
C1.1 CC1.1 CC2.2 CC3.2 CC5.3	SDC 6	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	No Exceptions Noted.
CC1.5	SDC 7	Entity provides information security and privacy training to staff that is relevant for their job function.	No Exceptions Noted.
CC1.5	SDC 9	Entity requires that all employees in client serving, IT, Engineering and Information Security roles are periodically evaluated regarding their job responsibilities.	No Exceptions Noted.
CC2.1	SDC 11	Entity systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls.	No Exceptions Noted.
C1.1 CC1.1 CC1.5 CC2.2 CC5.3	SDC 12	Entity has established procedures for staff to acknowledge applicable company policies periodically.	No Exceptions Noted.
CC2.1 CC2.2 CC5.3	SDC 13	Entity makes all policies and procedures available to all staff members for their perusal.	No Exceptions Noted.
CC2.1 CC2.3	SDC 14	Entity displays the most current information about its services on its website, which is accessible to its customers.	No Exceptions Noted.
CC2.2	SDC 15	Entity has provided information to employees, via	No Exceptions

TSC Ref	Control#	Control Activities as specified by Talentas Technology	Results of Test
CC4.2		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.	Noted.
CC2.3	SDC 16	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.
CC3.1 CC3.2 CC3.4 CC9.1	SDC 18	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.
CC3.2 CC3.4 CC9.1	SDC 19	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.
CC3.3	SDC 20	Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.	No Exceptions Noted.
CC3.2 CC3.4 CC9.2	SDC 21	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.
CC1.3 CC4.1	SDC 22	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.
CC4.1 CC4.2 CC5.2 CC7.3 CC7.4	SDC 23	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	No Exceptions Noted.
CC1.2 CC4.1 CC4.2 CC5.2	SDC 24	Entity's Senior Management reviews and approves all company policies annually.	No Exceptions Noted.
CC1.2 CC1.3 CC4.1 CC4.2 CC5.2	SDC 25	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.
CC1.2 CC4.1	SDC 26	Entity's Senior Management reviews and approves the Organizational Chart for all employees	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Talentas Technology	Results of Test
CC5.2		annually.	
CC1.2 CC4.1 CC5.2	SDC 27	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	No Exceptions Noted.
CC5.2	SDC 28	Entity's Infosec officer reviews and approves the list of people with access to production console annually	No Exceptions Noted.
CC1.2 CC4.1 CC5.2	SDC 29	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	No Exceptions Noted.
CC4.1 CC5.2	SDC 30	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.	No Exceptions Noted.
CC5.1 CC5.2 CC5.3	SDC 31	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	No Exceptions Noted.
CC5.1	SDC 32	Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	No Exceptions Noted.
CC6.1 CC6.2 CC6.3	SDC 33	Entity has documented policy 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.
CC6.1 CC6.2 CC6.3	SDC 34	Entity ensures that logical access provisioning to critical systems requires approval from authorised personnel on an individual need or for a predefined role.	No Exceptions Noted.
CC6.2 CC6.3	SDC 35	Entity ensures logical access that is no longer required in the event of a termination is made inaccessible in a timely manner.	No Exceptions Noted.
CC6.3	SDC 37	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.
CC6.1 CC6.6	SDC 38	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	No Exceptions Noted.
CC6.6	SDC 39	Entity requires that all staff members with access to any critical system is protected with a secure login mechanism such as Multifactor-authentication.	No Exceptions Noted.
CC6.1 CC6.3	SDC 42	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Talentas Technology	Results of Test
		only those individuals who require such access to perform their job functions.	
CC6.1 CC6.3	SDC 43	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.
CC6.6	SDC 44	Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.	No Exceptions Noted.
C1.1 CC6.6 CC6.7	SDC 45	Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorised access.	No Exceptions Noted.
CC6.6 CC6.8 CC7.3	SDC 46	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.
CC6.6	SDC 47	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.
C1.2 CC6.5	SDC 48	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	No Exceptions Noted.
C1.1 CC6.7	SDC 49	Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.	No Exceptions Noted.
CC6.6 CC6.8	SDC 50	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.	No Exceptions Noted.
CC6.7	SDC 51	User access to the entity's application is secured using https (TLS algorithm) and industry standard encryption.	No Exceptions Noted.
CC6.7 CC8.1	SDC 52	Entity develop, document, and maintain an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	No Exceptions Noted.
CC7.4	SDC 53	Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.	No Exceptions Noted.
CC7.3 CC7.4	SDC 54	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.	No Exceptions Noted.
CC4.1 CC7.3	SDC 55	Entity identifies vulnerabilities on the Company platform through the execution of regular	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Talentas Technology	Results of Test
CC7.4		vulnerability scans.	
CC4.1 CC7.3 CC8.1	SDC 56	Entity tracks all vulnerabilities, and remediates them as per the policy and procedure defined to manage vulnerabilities.	No Exceptions Noted.
A1.2	SDC 59	Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives, and verifies the integrity of these backups.	No Exceptions Noted.
CC8.1	SDC 64	Entity has documented policies and procedures to manage changes to its operating environment.	No Exceptions Noted.
CC8.1	SDC 65	Entity has procedures to govern changes to its operating environment.	No Exceptions Noted.
CC8.1	SDC 66	Entity has established procedures for approval when implementing changes to the operating environment.	No Exceptions Noted.
CC9.1 CC9.2	SDC 67	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 Entity's service commitments and system requirements	No Exceptions Noted.
CC9.2	SDC 68	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.
C1.1	SDC 69	Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems.	No Exceptions Noted.
C1.1	SDC 70	Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification.	No Exceptions Noted.
C1.2	SDC 71	Entity has a documented policy outlining guidelines for the disposal and retention of information.	No Exceptions Noted.
A1.3	SDC 97	Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.	No Exceptions Noted.
CC6.7	SDC 100	Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.	No Exceptions Noted.
CC6.6	SDC 104	Entity has documented policy and procedures for endpoint security and related controls.	No Exceptions Noted.
CC5.1	SDC 105	Entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Talentas Technology	Results of Test
CC6.7	SDC 106	Entity has a documented policy to manage encryption and cryptographic protection controls.	No Exceptions Noted.
CC6.1	SDC 108	Entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed	No Exceptions Noted.
CC6.1	SDC 135	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.
CC6.6 CC6.7	SDC 141	Entity requires that all critical endpoints are encrypted to protect them from unauthorised access	No Exceptions Noted.
CC1.3 CC4.1	SDC 154	Entity has set up mechanism to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	No Exceptions Noted.
CC1.5 CC2.2	SDC 383	Entity requires that all staff members complete Information Security Awareness training annually.	No Exceptions Noted.
CC1.5 CC2.2	SDC 387	Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	No Exceptions Noted.
CC1.5 CC2.2	SDC 388	Entity documents, monitors and retains individual training activities and records.	No Exceptions Noted.
CC4.1	SDC 389	Entity periodically updates and reviews the inventory of systems as a part of installations, removals and system updates.	No Exceptions Noted.
CC6.6	SDC 390	Entity develop, document, and maintain an inventory of organizational endpoint systems, including all necessary information to achieve accountability.	No Exceptions Noted.
CC7.3 CC7.1 CC7.2	SDC 391	Entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.	No Exceptions Noted.
A1.2 A1.3 CC7.5	SDC 392	Entity has documented guidelines to manage Disaster Recovery that establishes guidelines and procedures for continuing business operations in case of a disruption or a security incident	No Exceptions Noted.
A1.2 A1.3 CC7.5	SDC 393	Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	No Exceptions Noted.
CC7.1 CC7.2 CC7.3	SDC 394	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Talentas Technology	Results of Test
CC1.3	SDC 396	Entity appoints a People Operations Officer to develop and drive all personnel related security strategies.	No Exceptions Noted.
CC1.3	SDC 397	Entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.	No Exceptions Noted.

[End of the report]