armanino

System and Organization Controls (SOC) 2

Type 1 Report on Controls Relevant to the Security Trust Services Category

As of November 30, 2023

REPORT PREPARED FOR

tembo

TABLE OF CONTENTS

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of

Tembo Data Systems, Inc.

Cincinnati, Ohio

Scope

We have examined Tembo Data Systems, Inc.'s ("Tembo" or the "Company") accompanying description of its Tembo cloud system found in Section III titled "Description of the System" as of November 30, 2023 (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* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design of controls stated in the description as of November 30, 2023 to provide reasonable assurance that Tembo's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

Tembo uses a subservice organization, Amazon Web Services ("AWS"), to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Tembo, to achieve Tembo's service commitments and system requirements based on the applicable trust services criteria. The description presents Tembo's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Tembo'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.

Service Organization's Responsibilities

Tembo 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 Tembo's service commitments and system requirements were achieved.

In Section II, Tembo has provided the accompanying assertion titled "Management's Assertion" (assertion) about the description and the suitability of design of controls stated therein. Tembo 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.

Section I – Independent Service Auditor Report

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 American Institute of Certified Public Accountants. 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 that the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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 achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

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

Inherent Limitations

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

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 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.

Service Auditor's Independence

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

Section I – Independent Service Auditor Report

Opinion

In our opinion, in all material respects—

a. The description presents the Tembo cloud system that was designed and implemented as of November 30, 2023, in accordance with the description criteria.

b. The controls stated in the description were suitably designed as of November 30, 2023, to provide reasonable assurance that Tembo'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 organizations and user entities applied the complementary controls assumed in the design of Tembo's controls as of that date.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Tembo; user entities of the Tembo cloud system as of November 30, 2023, business partners of Tembo subject to risks arising from interactions with the 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 user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Armanino LLP

Armanino LLP

San Ramon, California

January 31, 2024

Section II – Management's Assertion

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Tembo Data Systems, Inc.'s ("Tembo" or the "Company") Tembo cloud system titled "Description of the System" as of November 30, 2023 (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* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with Tembo's system, particularly information about system controls that Tembo 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 (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Tembo, to achieve Tembo'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.

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

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

1) The description presents the Tembo cloud system that was designed and implemented as of November 30, 2023, in accordance with the description criteria.
2) The controls stated in the description were suitably designed as of November 30, 2023, to provide reasonable assurance that Tembo'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 and user entities applied the complementary controls assumed in the design of Tembo's controls as of that date.

Section III – Description of the System

DESCRIPTION OF THE TEMBO CLOUD SYSTEM

Overview of Operations

Company Overview

Founded in 2022 and headquartered in Cincinnati, Ohio, (the "Company") is a commercial open-source database company intended to offer one database with infinite capabilities.

Services Provided

Tembo is a Postgres developer platform for building every data service. The Tembo cloud system collapses the database sprawl and empowers users with a high-performance, fully-extensible managed Postgres service. With Tembo, developers can quickly create specialized data services using Stacks, pre-built Postgres configurations, and deploy without complex builds or additional data teams.

Principal Service Commitments and System Requirements

Principal Service Commitments

Tembo's security commitments to customers are documented and communicated to customers in both the master service agreement (MSA) and accompanying sales orders. The MSA is provided to, and accepted by, customers when they first sign onto the platform and includes the following provisions:

- Security: Tembo shall implement and maintain reasonable administrative, physical, and technical safeguards and measures, including without limitation encrypting customer data in transit and at rest, and disaster recovery procedures that are reasonably designed to protect the security and integrity of customer data and protect against unauthorized access to such customer data.

System Requirements

System requirements are specifications regarding how Tembo should function in order to meet their commitments to clients and end users. Requirements are specified in Tembo's policies and procedures and define key roles and responsibilities, risk management governing principles, and design principles to protect systems and data.

RELEVANT ASPECTS OF INTERNAL CONTROL

As defined by the American Institute of Certified Public Accountants (AICPA), internal control is a process affected by an entity's board of directors, management, and other personnel and consists of five interrelated components:

- Control Environment
- Risk Management
- Information and Communication
- Monitoring
- Control Activities

This section briefly describes the essential characteristics and other interrelated components over the trust services criteria of Security as they pertain to the Company.

Section III – Description of the System

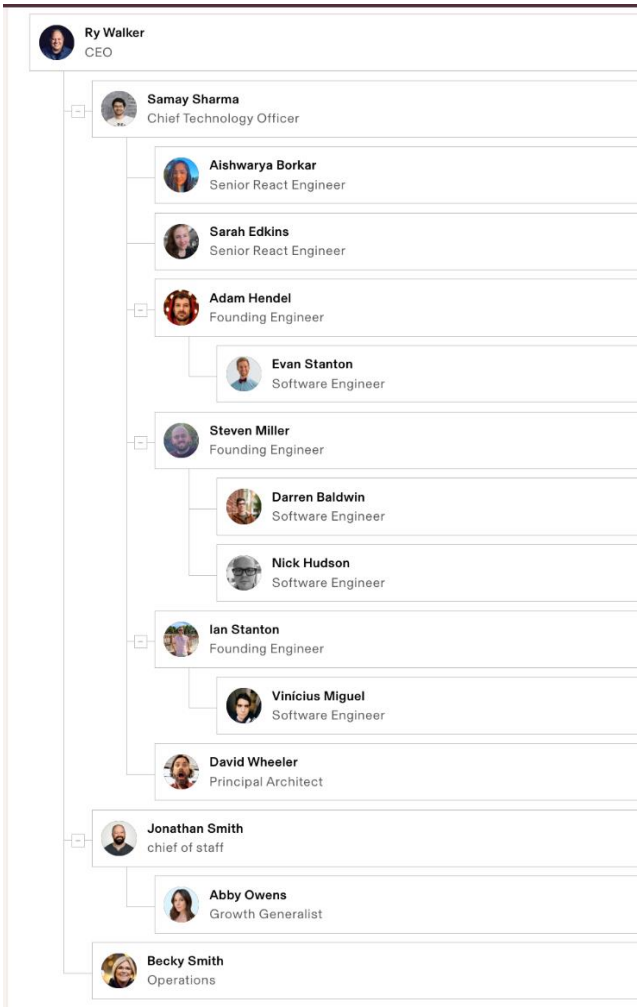
Control Environment

Management and the board of directors take their role in overseeing internal controls seriously. The Company has a code of conduct and a procedure for reporting violations. This information is posted on the Company internal file server. The Company distributes the code of conduct as part of the employee manual to all new employees and requires each employee to acknowledge in digital form that they have read and understand the code of conduct. The Company believes it has the proper incentives in place that would tend to discourage conflicts of interest and/or improper behavior. Company exercises significant diligence in hiring competent, qualified professionals, and to then provide employees with the appropriate on-the-job training. Company employees receive safety training, new hire orientation training, and most employees receive continuing education through online industry-related trainings and periodic industry conferences. The board of directors has sufficient independence to effectively oversee management.

The Company management team meets at least weekly. The members of the management team are the:

- Chief Executive Officer
- Chief Technology Officer
- Chief of Staff

Company Organizational Chart



Control Environment (continued)

The Tembo strategic plan, which is captured in the Tembo vision and mission statement, was enacted by the CEO and founder with contributions from the entire management team. The strategic plan focuses on corporate strategy for developing the core business, improving the current product offering, expanding solutions, and responding to market challenges. Annually, management reviews and develops plans and resources to meet strategic goals. Relevant segments of the strategic plan are shared with members of the management team, who disseminate the strategic goals to personnel, and monitor progress and adherence to the strategic plan.

Tembo has a defined organizational structure. The Company organizational chart is made available to all employees, and reporting relationships are kept current on that chart. Roles and responsibilities are defined in written job descriptions and communicated to employees, as well as supervisors and managers. Management periodically reviews reporting relationships and the organizational structure as part of planning and adjusts the reporting structures, as needed, based on changing commitments, requirements and goals.

Human Resources

The Tembo office manager, as well as upper management, oversee other human resources (HR) functions, including employee search, recruiting, orientation and industry-related training.

The Tembo HR function is guided by established policies and procedures for hiring, promoting and compensating, training, and termination of employees. Relevant Tembo information and security policies and procedures are provided to all employees and available to them internally. Employees are required to electronically acknowledge the receipt and their understanding of the policies and procedures.

Polices include, but are not limited to:

- Code of conduct
- Acceptable use policy
- Information security policy
- Responsible disclosure policy
- Data protection policy

Employee compliance with behavioral expectations is evaluated as part of their job performance. Candidates for promotion must have demonstrated a commitment to ethical standards through their own actions, and by setting an example for other employees.

Information is accumulated primarily through the performance evaluation process, and less formally through emails or comments submitted by supervisors or peers. Complaints indicating departure from behavioral standards are investigated by managers and are documented, as necessary.

As part of Tembo's performance management process, all managers are required to establish expectations and evaluate performance for the employees they manage. At least annually, managers meet with their employees on an individual basis to discuss performance and set expectations for the future. These evaluations are facilitated through management meetings where results of employee performance are discussed. Performance is documented within a performance management tool.

Control Environment (continued)

Human Resources (continued)

A critical part of providing a work environment with strong ethics and controls starts with the hiring and training processes. Management takes an active role in recruitment, including screening applicants, checking references, completing background checks, and providing the orientation of new team members.

Potential employees must pass a criminal background check before beginning work at Tembo.

New Hire Onboarding

Before an individual joins the Tembo team, management must first identify the need for additional personnel. A job requisition is drafted and approved by management. If the job requisition does not have a corresponding job description, one is created and reviewed by the appropriate manager. Once the requisition has been completed, a job description is drafted. This is then posted internally and to various online job boards and career sites.

The Tembo management team reviews resumes to identify qualified candidates. Then a qualified candidate is identified he or she is further evaluated through a screening process. If the candidate passes the screening they are scheduled for an interview with the individuals in the respective team in which they will work.

When interviews are completed, a hiring decision is made. If management chooses to issue an offer letter to the prospective hire, Tembo management will issue an offer letter and communicate the decision with prospective employee. If the prospective employee formally accepts the offer letter, a background check is conducted. The formal background check and hiring steps must be complete before the prospective Tembo employee is allowed access to Tembo's premises or systems to begin work.

When the new employee arrives on his or her first day, they meet with a member of the management team to review necessary paperwork. They are required to electronically acknowledge the code of conduct. The new employee then attends a new employee orientation (NEO) seminar. After orientation is complete, the individual continues training through on the job training.

Throughout the hiring process, progress and completion of tasks are recorded within a digital checklist. This checklist is maintained by the Tembo management team and is included in the employee's file.

Policy for Training

All new employees are required to attend orientation training that introduces them to the Tembo culture, business operations, policies and procedures, and Tembo's applications and software.

Ongoing employee training consists principally of on-the-job training. When external training for an employee will contribute to Tembo's business goals, Tembo will pay for pre-approved, job-related courses and related travel expenses. Employees are also provided access to industry publications and resources for continued self-education on industry trends, regulatory requirements, etc. Management monitors compliance with corporate-wide training requirements and tracks adherence within Drata.

Code of Conduct

The code of conduct is available to all employees within Tembo's compliance software, Drata, and includes sections that address business conduct, conflicts of interest, financial reporting, safeguarding of company assets and other information related to corporate conduct and culture. This document makes Tembo's position clear that violations of the code of conduct will not be tolerated and will lead to disciplinary action, including possible termination.

Control Environment (continued)

Employment Termination

Employment can be terminated by Tembo at any time as it operates as an at-will employer. Employee terminations can be voluntary or involuntary. Involuntary terminations require prior documentation of issues and performance coaching with the individual in question to resolve those issues.

Risk Assessment

As part of Tembo's risk management activities, Tembo conducts an annual enterprise risk assessment. The assessment is a collaborative, face-to-face whereby the management team draws on collective industry, enterprise, technical, and regulatory knowledge to identify key risks to business operations. As part of the management team meeting, a formal risk assessment report is created to memorialize identified risks, risk rankings and mitigation strategies. The risk assessment report guides internal risk management and monitoring activities for the forthcoming year. The risk assessment report is revisited and revised for marked changes or developments in market, industry, regulatory or legal risks.

As part of the annual risk assessment and formal risk assessment report, management identifies information technology risks, ranks those risks, and develops mitigation strategies which are monitored by management for successful mitigation. In addition to the annual risk assessment, risk is evaluated daily through defined and repeatable IT and business processes. These processes consider a multitude of risks, including security, logical access, availability of application services, and confidentiality of customer data at the heart of the Tembo's system. Mitigations strategies are developed by management iteratively to respond in a nimble fashion to ever-changing risk landscapes.

To support IT risk management activities, management conducts annual penetration testing. Each item identified on the penetration tests is reviewed and prioritized for mitigation. Mitigations may include a change in policy as well as monitoring or periodic evaluation. Controls may be evaluated daily, weekly, monthly, or quarterly, per the risks and business needs.

Information and Communication

Information Systems

Tembo's information systems have been engineered on the principles of high availability, security and confidentiality. To assist in achieving the desired level of consistency of these principles, Tembo has located its production environment within the US-East-1 (N. Virginia) region of the Amazon Web Services (AWS) Elastic Compute Cloud (EC2). Customer facing applications run on servers which participate in an active disaster recovery protocol. These systems are physically and logically secured from other components of the Tembo corporate infrastructure.

Through methodology which is documented and tested within the Tembo's business continuity and disaster recovery plan, a portion of Tembo's critical information systems are replicated to the Amazon Simple Storage Service (S3). This increases system availability in the event of a disaster within the AWS US-East-1 (N. Virginia) region as Tembo can fail over to a set of replicated backup servers located in secondary AWS regions.

Communication

Tembo endeavors to inform internal and external users of the structure of the system so they may understand their role in the system and the results of system operation.

Information and Communication (continued)

Communication (continued)

System descriptions are available to authorized external users that describe relevant system components as well as the purpose and design of the system. Additionally, system architectural information and user guides can be found on Tembo's publicly facing website.

Internal users learn about Tembo systems beginning with their orientation and continuing as needed with on-the-job training and/or specific training courses. Tembo's compliance platform, Drata, holds both written documentation as well as links to specific documents on Tembo's cloud drives such as product and system information.

Tembo typically conducts a quarterly all-hands meeting. The meeting is led by the CEO who along with the management team discusses the status of products and projects and any unusual items or events. The meetings also include an employee Q&A session to address specific concerns. These meetings allow senior management to communicate with employees about the strategy, results, and values of the company.

During business development presentations, the business development team provides documentation to prospective clients that describes the relationship between Tembo and the client. As the business development team moves forward in the sales process, they review the standard contract terms and conditions with the prospective client to ensure a clear understanding of the anticipated roles of each party, including those related to system security, system availability, and confidentiality commitments.

Some clients may request deviations from the standard terms of service. Deviations must be approved by the CEO. The CEO evaluates all such deviations for their potential impact on Tembo's system security commitments.

The finalized customer agreements, service level agreement (SLA), SOW, and any other contract documents are stored within Tembo's cloud drive and access is restricted to personnel with a need to know.

Policies and procedures are a key tool for process standardization and communication of key control elements. Relevant policies and procedures are updated by their respective owners, with input and approval from management, and made available to Tembo employees through Drata. Changes in policies and procedures that impact internal users (employees) responsibilities regarding security commitments are communicated via email and in-person meetings.

Monitoring systems assist Tembo in meeting SLA requirements. Technical processes are monitored by automated systems such as automated logging and monitoring tools. Staff members receive automated alerts via Slack, a communication and messaging application, when there is a substantial decrease in system performance or a significant security event so they can respond to the issue.

Clients' responsibilities are defined in the contractual agreements. Changes in contractual responsibilities relevant to security, availability, confidentiality and/or other responsibilities are communicated to customers by management and memorialized in a new or amended MSA.

Monitoring

Monitoring activities are intended to identify and remediate areas of risk including strategic risk, financial risk, operational risk and legal/regulatory risk.

Management and supervisory personnel monitor the quality of internal control performance via frequent observation, interaction and performance of their assigned duties. Additionally, Tembo uses the Drata compliance platform to continuously monitor the operation of controls. Control issues are investigated and remediated, as necessary.

Monitoring (continued)

Critical job functions have been designed and implemented to provide inherent monitoring through separation of job functions, management oversight and systematic controls. Management reviews the functionality of software products and application configurations before they move through the development process and into production.

Drata and AWS Cloud Trail are used to collect data from system infrastructure components and from endpoint systems. The logging and monitoring software is used to monitor system performance, potential security threats and vulnerabilities, and resource utilization, and to detect unusual system activity or service requests.

Throughout each of the above processes, identified deficiencies are communicated to the relevant management personnel and appropriate follow up actions are initiated.

Use and Monitoring of Sub-Service Providers

Tembo's production systems are hosted within the US-East-1 (N. Virginia) region of the Amazon Web Services (AWS) Elastic Compute Cloud (EC2). AWS hosts the Software as a Service ("SaaS") versions of the Tembo cloud system.

Tembo's production AWS environment is designed with fault tolerance protection for all layers of the platform and infrastructure, including network traffic and firewalls, as well as the web and application services and backend database connections. The Tembo infrastructure is designed to scale substantially to accommodate foreseeable growth in the number of end-users and transaction volume for their products and services.

Tembo monitors the performance of these activities with monitoring tools as described above. Issues or relevant exceptions are investigated further for impact to the Tembo suite of applications.

Production data is replicated to all AWS EC2 instance volumes to the highly redundant AWS Simple Storage Service (S2). These replicated instance volumes are on standby and are ready to deploy in the event of a primary virtual server failure.

The Tembo internal data center, also stored in the US-East-1 region of the AWS EC2, replicates the business-critical internal AWS instances to the AWS S3. In the event of a disaster, Tembo will be able to restore these instances within a secondary region.

CONTROL ACTIVITIES

Policies and Procedures

Policies and procedures are a key tool for process standardization and communication of key control elements. Relevant policies and procedures are updated by their respective owners and made available to Tembo employees through the Drata compliance platform. Information security policies include, but are not limited to:

- Acceptable use policy
- Asset management policy
- Backup policy
- Business continuity/ disaster recovery plan
- Code of conduct
- Data classification, retention, and protection policies
- Encryption and password policies
- Incident response plan

CONTROL ACTIVITIES (continued)

Policies and Procedures (continued)

- Physical security policy
- Responsible disclosure policy
- Risk assessment policy
- Software development life cycle policy
- System access management policy
- Vendor management policy
- Vulnerability management policy

Security Awareness Training

Tembo maintains a security awareness program through various mechanisms including:

- Employee orientation program,
- Annual security awareness training,
- Periodic email communications from the solutions architect/compliance manager and other management, and
- Role-specific security training

Access Provisioning

A role-based access model is leveraged to grant system access commensurate with employee's job responsibilities. The security officer is responsible for assigning and maintaining access rights to the Tembo internal and production environments and related devices and applications.

Access requests are documented within the ticketing system and require the security officer's approval prior to the provisioning of access privileges. System administrators review the requests and validate that the request was provided by an authorized individual. Once access has been properly authorized, access is granted in accordance with the request.

Access Deprovisioning

Account terminations are initiated by the HR department. The HR department is responsible for notifying the security officer when employees are terminated. Accounts are disabled or deleted by system administrators within one business day of the termination. Termination activities are documented and tracked within the termination checklist. The termination process includes:

- User access to all applications will typically be revoked or disabled within one business day that the termination takes effect.
- Access to the network, production systems, and critical network devices will typically be revoked or disabled in accordance with the information provided in the termination checklist.
- Physical assets such as laptops, key cards, and IT equipment are collected.

Under certain conditions, network accounts may need to remain accessible after the termination date. In these cases, the account password is changed and the account is marked as locked. Any necessary data is migrated from the terminated account to an active account. When management determines that all necessary data has been preserved, the account is fully closed. Account termination requests are documented within a checklist. Completion dates are logged with within the checklist.

Section III – Description of the System

Network Security Overview

All sensitive data transmitted and processed within the Tembo network is encrypted to protect sensitive data against third-party disclosure in transit. Servers and network components are secured with access control mechanisms and protected by hardened firewalls and intrusion detection systems. All security services are monitored and updated in a timely manner to address emerging vulnerabilities.

Remote Access

Tembo employees access internal and production systems through secure virtual private network (VPN) tunnels. These connections utilize AES 256-Bit encryption. Users are required to authenticate to the VPN using a username, password, and one-time-password (MFA).

Antivirus and Firewalls

Tembo controls the introduction of software by restricting the ability to install software on workstations and laptops to user support personnel and to users with admin privileges over their own workstation or laptop.

Antivirus is installed on all workstations. Daily scans are scheduled for each machine. The antivirus software is configured to receive an updated virus signature at least daily. User support receives a report via email when any machine has not received an update in the required timeframe.

Tembo utilizes several firewalls and AWS lines of defense to protect external points of connectivity and intrusion/extrusion detection systems to alert staff regarding unusual or unauthorized activity.

External access to sensitive data is restricted by user authentication and message encryption systems including VPN and TLS.

Intrusion Detection

Suspicious activity triggers alerts that are sent to responsible information security staff via Slack notifications. The responding individuals investigate the alerts and if necessary escalate the issue following the defined incident response policy.

Vulnerability Assessment and Penetration Testing

The Tembo production environment is monitored on an ongoing basis for known vulnerabilities. Every twelve months, both internal and external penetration tests and vulnerability assessments are conducted and results are reported to the network administrator, with an action plan on correcting any identified vulnerabilities. The Tembo vulnerability scan is active in nature and reports what vulnerabilities exist.

Administrator Access

A root account (also called an admin account or super-user account) is an account that is used to perform high-level tasks. Root accounts are common in all technology domains and acceptable in the corporate computing environment.

Root account privileges within Tembo core systems are designated by the network administrator on an individual basis.

Access Reviews

User access lists for applications, secured folders, root accounts and databases are reviewed by the Information security team leads on a regular basis. If any unnecessary access accounts (orphans) are found, appropriate remediation action is taken.

Network Security Overview (continued)

System Passwords

Users are required to enter a user ID and password to access any Tembo network or application. Complexity standards for passwords have been established to enforce control. The following password policy settings are in place as system-based preventive controls for production systems:

- Complex passwords are required where possible. Complex passwords have at least 10 characters, 1+ uppercase letter(s), 1+ lowercase letter(s), 1+ non-alphanumeric character(s), Maximum age 90 days
- Previously used passwords are not allowed
- Multi-factor authentication must be enabled

Device Build and Hardening

New AWS EC2 instances are periodically deployed to Tembo's production environment to support growth and management of the existing environment. Tembo does not deploy physical servers or hardware. Before an EC2 instance can be deployed, it must be assigned to the appropriate AWS network ACL(s) and security group(s).

System and Performance Monitoring

Tembo leverages various tools and techniques to proactively monitor the production environment. These tools are designed to identify issues and alert responsible staff of the issue before it impacts Tembo end users or customers. Tools that are currently leveraged include:

Tool	Description
Prometheus	Open source systems monitoring and alerting toolkit.
AWS Cloud Trail	Logging tool used to monitor AWS resources.
Drata	Drata is the compliance platform used to monitor the status of controls in real-time and is configured to ingest logs from the production AWS environment and provide alerts via a dashboard within the platform.

Security & Incident Management

Operations personnel follow defined protocols for evaluating and reporting events. Security related events are reported to the engineering team.

If a security event is determined to be an incident, the network administrator directs the incident response team in following defined protocols for responding to the incident. These protocols are contained in the incident response policy manual. Resolution of security events are reviewed periodically at incident response team meetings. Changes in protocol or systems to improve response are addressed in these meetings. Changes are documented and signed off by the network administrator.

Internal and external users are informed of incidents in a timely manner and they are advised of any measures to be taken on their part. Governing entities are notified as required. Tembo policies include probation, suspension or termination as potential sanctions for employee misconduct.

Network Security Overview (continued)

Change Management Policy

The Company maintains release teams comprised of product owners, release managers, and quality Assurance (QA) personnel, who are responsible for authorizing the development of changes to the Tembo cloud system. This authorization process includes evaluating the impact of the change on the Company's security and confidentiality commitments and occurs as part of a daily scrum meeting.

The Company maintains separate development, test, and production environments. The Company uses GitHub for version control.

Change procedures are documented in a ticketing system. Once development has been completed, appropriate testing is performed. Test results are documented in a change ticket. Upon successful completion of testing procedures, engineering, or QA, approves each change for implementation into the production environment.

Once approved, changes are moved into the production environment by engineering personnel. The implementation of changes into the production environment are performed using administrative accounts to the production servers on which the application resides. This server access is limited to authorized engineering personnel.

Data Backup

The Company maintains backups of the production version of the Tembo cloud application code in GitHub. Backups of production databases are performed daily within the AWS environment. Backups are encrypted at rest. Backups are stored in an AWS S3 bucket. Annually, the Company restores a subset of files from backup, and the results are verified as successful.

Disaster Recovery

Planning for the business continuity of Tembo in the aftermath of a disaster is an essential part of an organization risk management program. Preparation for, response to, and recovery from a disaster affecting the administrative functions of the company require the cooperative efforts of many functional areas and supporting organizations.

Because the Tembo infrastructure is 100% cloud-hosted via AWS, a disaster event occurring at the Tembo headquarters would not impact production systems. If there was a major disaster that destroyed or severely compromised the infrastructure within the AWS US-East-1 (N. Virginia) region, Tembo has a disaster recovery policy in place. This policy provides the instructions regarding the transfer of production infrastructure and applications to a secondary AWS region. The detailed procedure for failing-over are outlined in Tembo's disaster recovery plan.

Complementary Subservice Organization Controls

Subservice Organization Controls

The Company utilizes a subservice organization to perform the functions described below to improve operating and administrative effectiveness. Third party personnel are not granted access to Company or User Entity data or the Company systems themselves. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

AWS provides cloud hosting services. The cloud hosting services provided by AWS are ISO 27001:2013 certified and undergo periodic SOC 2 Type 2 examinations. Certification status and the results of the examinations are reviewed annually as part of Company's monitoring controls and the vendor management process. Formal documentation of third-party vendor assessments is preserved for compliance purposes within Drata.

The facilities used during the reporting period and the data center hosting services relied upon by Company are listed in Table 1 and Table 2, respectively.

Table 1 - Subservice organization used by Tembo

Entity	Facility Location	Services Hosted
AWS	Use-East (N. Virginia)	Tembo cloud system

Table 2 - Service Categories

Criteria	Complementary Subservice Organization Controls
CC6.4	• AWS is responsible for restricting data center access to authorized personnel. • AWS is responsible for the 24x7 monitoring of data centers by closed circuit cameras and security personnel.
CC7.2	• AWS is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers. • AWS is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

Complementary User Entity Controls

Tembo's controls related to the Tembo cloud system cover only a portion of overall internal control for each user entity of Tembo. It is not feasible for the control objectives related to the Tembo cloud system to be achieved solely by Tembo. Therefore, each user entity's internal controls should be evaluated in conjunction with Tembo's controls and the related tests and results described in Section IV of this report, taking into account the related complementary user entity controls, where applicable. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal controls to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

This section highlights those internal control responsibilities that the Company believes should be present at each user entity and has considered in developing the Company's controls described in this report. Furthermore, the following list of controls is intended to address only those controls surrounding the interface and communication between the user entity and the Company. Accordingly, this list does not purport to be, and is not, a complete listing of the controls that a user entity should maintain. User entities are responsible for:

- Ensuring that the service agreement or quote with the Company properly describes the services to be provided.
- Communicating service level issues as they arise, including requesting reports of uptime for production servers if this becomes an issue.
- Communicating changes to the Company's services as required.
- Providing written notification of changes to individuals authorized to instruct the Company's activities on behalf of the client.
- Reporting operational failures, incidents, system problems/concerns, and complaints to appropriate Company personnel as client support requests on a timely basis (including resolution thereof).
- Requesting changes to the Tembo cloud system application and communicating issues with these changes after they have been implemented.
- Managing access provided to client personnel to its versions of the Tembo cloud system application.
- Reviewing release notes for changes to the Tembo cloud system application and evaluating the impact of changes to client control environments.

TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS

The following tests of design and implementation were completed to determine if controls necessary to meet the applicable trust services categories and associated criteria have been achieved as of the examination date. Applicable Trust Services Categories for which controls were evaluated are:

- ***Security*** - The system is protected against unauthorized access (both physical and logical)

No other Trust Services Categories are included in the scope of this report.

Section IV – Trust Services Category, Criteria, and Related Controls

CC1.0 Common Criteria Related to Control Environment

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC1.1 – COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	CC1.1.1	Tembo management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.
	CC1.1.2	Tembo has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the acceptable use policy upon hire.
	CC1.1.3	Tembo's new hires are required to pass a background check as a condition of their employment.
	CC1.1.4	Tembo requires its contractors to read and accept the code of conduct, read and accept the acceptable use policy, and pass a background check.
	CC1.1.5	Tembo has a formal code of conduct approved by management and accessible to all employees. All employees must accept the code of conduct upon hire.
	CC1.1.6	Tembo has established a data protection policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.
CC1.2 – COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	CC1.2.1	The Company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the Company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.
	CC1.2.2	The Company's board of directors has a documented charter that outlines its oversight responsibilities for internal control. The Company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.
	CC1.2.3	The Company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.
	CC1.2.4	The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the Company.

Section IV – Trust Services Category, Criteria, and Related Controls

CC1.0 Common Criteria Related to Control Environment

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC1.2 – COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	CC1.2.5	Tembo conducts a risk assessment at least annually.
	CC1.2.6	Tembo engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.
	CC1.2.7	Tembo engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.
	CC1.2.8	Management reviews security policies on an annual basis.
	CC1.2.9	Tembo has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.
	CC1.2.10	At least one members of the board of directors is independent of management.
	CC1.2.11	Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.
CC1.3: - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	CC1.3.1	Tembo reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.
	CC1.2.9	Tembo has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.
CC1.4: - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CC1.4.1	Tembo evaluates the performance of all employees through a formal, annual performance evaluation.

Section IV – Trust Services Category, Criteria, and Related Controls

CC1.0 Common Criteria Related to Control Environment

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC1.4: - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CC1.4.2	Tembo's new hires and/or internal transfers are required to go through an official recruiting process during which their qualifications and experience are screened to ensure that they are competent and capable of fulfilling their responsibilities.
	CC1.4.3	All Tembo positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Tembo.
	CC1.4.4	Tembo has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Tembo's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.
	CC1.4.5	Tembo has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.
	CC1.1.3	Tembo's new hires are required to pass a background check as a condition of their employment.
	CC1.1.4	Tembo requires its contractors to read and accept the code of conduct, read and accept the acceptable use policy, and pass a background check.
	CC1.1.5	Tembo has a formal code of conduct approved by management and accessible to all employees. All employees must accept the code of conduct upon hire.
CC1.5: - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CC1.1.2	Tembo has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the acceptable use policy upon hire.
	CC1.1.5	Tembo has a formal code of conduct approved by management and accessible to all employees. All employees must accept the code of conduct upon hire.
	CC1.4.1	Tembo evaluates the performance of all employees through a formal, annual performance evaluation.

Section IV – Trust Services Category, Criteria, and Related Controls

CC1.0 Common Criteria Related to Control Environment

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC1.5: - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CC1.4.5	Tembo has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.

Section IV – Trust Services Category, Criteria, and Related Controls

CC2.0 Common Criteria Related to Communication and Information

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC2.1 – COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	CC2.1.1	Tembo maintains an accurate architectural diagram to document system boundaries to support the functioning of internal control.
	CC2.1.2	Tembo has a defined policy that establishes requirements for the proper management and tracking of organizational assets.
	CC2.1.3	Tembo performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.
	CC2.1.4	Tembo conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
	CC2.1.5	Tembo has an established policy and procedures that governs the use of cryptographic controls.
	CC2.1.6	Tembo management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.
	CC2.1.7	Tembo has a defined information security policy that covers policies and procedures to support the functioning of internal control.
	CC2.1.8	Tembo authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.
	CC2.1.9	Tembo identifies, inventories, classifies, and assigns owners to IT assets.
	CC1.2.5	Tembo conducts a risk assessment at least annually.

Section IV – Trust Services Category, Criteria, and Related Controls

CC2.0 Common Criteria Related to Communication and Information

Trust Services Criteria	Control Ref #	Tembo's Control Description
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.	CC2.2.1	Tembo provides a process to employees for reporting security features, incidents, and concerns, and other complaints to company management.
	CC2.2.2	Tembo has implemented an incident response plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to business continuity/disaster recovery.
	CC2.2.3	Tembo has an established incident response plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.
	CC2.2.4	Tembo has identified an incident response team that quantifies and monitors incidents involving security at the company.
	CC2.2.5	Tembo has implemented an incident response plan that includes documenting lessons learned and a root cause analysis after incidents and sharing them with the broader engineering team to support business continuity/disaster recovery.
	CC2.2.6	The security team communicates important information security events to company management in a timely manner.
	CC1.1.1	Tembo management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.
	CC1.1.2	Tembo has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the acceptable use policy upon hire.
	CC1.1.5	Tembo has a formal code of conduct approved by management and accessible to all employees. All employees must accept the code of conduct upon hire.
	CC1.1.6	Tembo has established a data protection policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.

Section IV – Trust Services Category, Criteria, and Related Controls

CC2.0 Common Criteria Related to Communication and Information

Trust Services Criteria	Control Ref #	Tembo's Control Description
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.	CC1.4.5	Tembo has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.
	CC2.1.4	Tembo conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
CC2.3 – COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	CC2.3.1	Tembo's security commitments are communicated to external users, as appropriate.
	CC2.3.2	Tembo communicates system changes to customers that may affect security, availability, processing integrity, or confidentiality.
	CC2.3.3	Tembo provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.
	CC2.3.4	Tembo maintains a privacy policy that is available to all external users and internal employees, and it details the Company's confidentiality and privacy commitments.
	CC2.3.5	Tembo maintains a terms of service that is available to all external users and internal employees, and the terms detail the Company's security and availability commitments regarding the systems. Client agreements or master service agreements are in place for when the terms of service may not apply.
	CC2.3.6	Tembo tracks security deficiencies through internal tools and closes them within an SLA that management has pre-specified.
	CC2.3.7	Tembo maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.

Section IV – Trust Services Category, Criteria, and Related Controls

CC2.0 Common Criteria Related to Communication and Information

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC2.3 – COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	CC2.3.8	Tembo maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.
	CC2.1.2	Tembo has a defined policy that establishes requirements for the proper management and tracking of organizational assets.
	CC2.1.3	Tembo performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.
	CC2.1.4	Tembo conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
	CC2.1.5	Tembo has an established policy and procedures that governs the use of cryptographic controls.

Section IV – Trust Services Category, Criteria, and Related Controls

CC3.0 Common Criteria Related to Risk Assessment

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC3.1 – COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CC3.1.1	Tembo has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.
CC3.2 – COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	CC3.2.1	Tembo's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.
	CC1.2.5	Tembo conducts a risk assessment at least annually.
	CC1.2.6	Tembo engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.
	CC2.3.7	Tembo maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.
	CC2.3.8	Tembo maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.
	CC3.1.1	Tembo has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.

Section IV – Trust Services Category, Criteria, and Related Controls

CC3.0 Common Criteria Related to Risk Assessment

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC3.3 – COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CC1.2.5	Tembo conducts a risk assessment at least annually.
CC3.4 – COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	CC1.2.5	Tembo conducts a risk assessment at least annually.
	CC3.2.1	Tembo's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.

Section IV – Trust Services Category, Criteria, and Related Controls

CC4.0 Common Criteria Related to Monitoring Activities

Trust Services Criteria	Control Ref #	Tembo's Control Description
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.	CC1.2.6	Tembo engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.
	CC1.2.7	Tembo engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.
	CC2.1.3	Tembo performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.
	CC2.1.4	Tembo conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
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.	CC1.2.6	Tembo engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.
	CC1.2.7	Tembo engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.
	CC2.1.3	Tembo performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.
	CC2.1.4	Tembo conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.

Section IV – Trust Services Category, Criteria, and Related Controls

CC5.0 Common Criteria Related to Control Activities

Trust Services Criteria	Control Ref #	Tembo's Control Description
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.	CC2.1.3	Tembo performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.
	CC2.1.4	Tembo conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	CC2.1.3	Tembo performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.
	CC2.1.4	Tembo conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
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.	CC1.1.1	Tembo management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.
	CC1.1.2	Tembo has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the acceptable use policy upon hire.

Section IV – Trust Services Category, Criteria, and Related Controls

CC6.0 Common Criteria Related to Logical and Physical Access Controls

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	CC6.1.1	Tembo uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.
	CC6.1.2	Hardening standards are in place to ensure that newly deployed server instances are appropriately secured.
	CC6.1.3	Tembo maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.
	CC6.1.4	Tembo ensures that a password manager is installed on all company-issued laptops.
	CC6.1.5	Tembo ensures that company-issued laptops have encrypted hard-disks.
	CC6.1.6	Tembo stores data in databases that is encrypted at rest.
	CC6.1.7	Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for external users, and MFA required for employee users.
	CC6.1.8	Tembo's application user passwords are stored using a salted password hash.
	CC6.1.9	Role-based security is in place for internal and external users, including super admin users.
	CC6.1.10	Tembo requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.
	CC6.1.11	Tembo has established formal guidelines for passwords to govern the management and use of authentication mechanisms.
	CC6.1.12	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.
	CC6.1.13	Access to corporate network, production machines, network devices, and support tools requires a unique ID.

Section IV – Trust Services Category, Criteria, and Related Controls

CC6.0 Common Criteria Related to Logical and Physical Access Controls

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	CC6.1.14	Users can only access the production system remotely through the use of encrypted communication systems.
	CC6.1.15	Tembo has an established key management process in place to support the organization's use of cryptographic techniques.
	CC6.1.16	Tembo has a defined policy that establishes requirements for the use of cryptographic controls.
	CC1.1.6	Tembo has established a data protection policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.
	CC2.1.2	Tembo has a defined policy that establishes requirements for the proper management and tracking of organizational assets.
	CC2.1.9	Tembo identifies, inventories, classifies, and assigns owners to IT assets.
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	CC6.2.1	Tembo has a defined system access control policy that requires annual access control reviews to be conducted and access request forms be filled out for new hires and employee transfers.
	CC6.2.2	Tembo performs annual access control reviews.
	CC6.2.3	Tembo uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned.
	CC6.2.4	External users must accept the terms of service prior to their account being created.
	CC6.2.5	Access to infrastructure and code review tools is removed from terminated employees within one business day.

Section IV – Trust Services Category, Criteria, and Related Controls

CC6.0 Common Criteria Related to Logical and Physical Access Controls

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	CC6.1.12	Tembo has established formal guidelines for passwords to govern the management and use of authentication mechanisms.
	CC6.1.13	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	CC6.1.9	Role-based security is in place for internal and external users, including super admin users.
	CC6.1.12	Tembo has established formal guidelines for passwords to govern the management and use of authentication mechanisms.
	CC6.1.13	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.
	CC6.2.1	Tembo has a defined system access control policy that requires annual access control reviews to be conducted and access request forms be filled out for new hires and employee transfers.
	CC6.2.2	Tembo performs annual access control reviews.

Section IV – Trust Services Category, Criteria, and Related Controls

CC6.0 Common Criteria Related to Logical and Physical Access Controls

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	CC6.2.3	Tembo uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned.
	CC6.2.4	External users must accept the terms of service prior to their account being created.
	CC6.2.5	Access to infrastructure and code review tools is removed from terminated employees within one business day.
CC6.4 - 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.	CC6.4.1	Tembo maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.
	CC6.4.2	Tembo has security policies that have been approved by management and detail how physical security for the company's headquarters is maintained. These policies are accessible to all employees and contractors.
	CC6.4.3	Tembo has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors.
	CC6.2.2	Tembo performs annual access control reviews.

CC6.0 Common Criteria Related to Logical and Physical Access Controls

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC6.4 - 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.	CC6.2.3	Tembo uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned.
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	CC6.5.1	Tembo has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.
	CC6.2.3	Tembo uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned.
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CC6.6.1	Tembo ensures that all company-issued computers use a screensaver lock with a timeout of no more than 15 minutes.
	CC6.2.2	Tembo ensures that all connections to its web application from its users are encrypted.
	CC6.6.3	Tembo automatically logs users out after a predefined inactivity interval and/or closure of the internet browser, and requires users to reauthenticate.

Section IV – Trust Services Category, Criteria, and Related Controls

CC6.0 Common Criteria Related to Logical and Physical Access Controls

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CC6.6.4	SSH users use unique accounts to access production machines. Additionally, the use of the Root account is not allowed.
	CC6.6.5	No public SSH is allowed.
	CC6.6.8	WAF in place to protect Tembo's application from outside threats.
	CC6.6.9	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected.
	CC6.1.3	Tembo maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.
	CC6.1.7	Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for external users, and MFA required for employee users.
	CC6.1.10	Tembo requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.
	CC6.1.11	Tembo has established formal guidelines for passwords to govern the management and use of authentication mechanisms.
	CC6.1.14	Users can only access the production system remotely through the use of encrypted communication systems.

Section IV – Trust Services Category, Criteria, and Related Controls

CC6.0 Common Criteria Related to Logical and Physical Access Controls

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	CC6.7.1	Usage of removable media for members of the Tembo team is restricted to registered devices and requires approval by management. When authorized, only encrypted removeable media is allowed.
	CC6.7.2	Tembo's customer data is segregated from the data of other customers.
	CC6.7.3	Tembo ensures that company-issued removable media devices (USB drives) are encrypted.
	CC1.1.6	Tembo has established a data protection policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.
	CC6.1.5	Tembo ensures that a password manager is installed on all company-issued laptops.
	CC6.1.6	Tembo ensures that company-issued laptops have encrypted hard-disks.
	CC6.6.2	Tembo ensures that all connections to its web application from its users are encrypted.
	CC6.6.4	SSH users use unique accounts to access production machines. Additionally, the use of the root account is not allowed.
	CC6.6.5	No public SSH is allowed.
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	CC6.8.1	Tembo requires antivirus software to be installed on workstations to protect the network against malware.
	CC6.8.2	Tembo's workstations operating system (OS) security patches are applied automatically.
	CC6.8.3	Tembo has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.
	CC6.8.4	Tembo ensures that virtual machine OS patches are applied monthly.

Section IV – Trust Services Category, Criteria, and Related Controls

CC7.0 Common Criteria Related to System Operations

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	CC7.1.1	When Tembo's application code changes, code reviews and tests are performed by someone other than the person who made the code change.
	CC7.1.2	Tembo engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.
	CC7.1.3	Tembo engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.
	CC7.1.4	Tembo conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
	CC7.1.5	Tembo has a defined policy that establishes requirements for vulnerability assessments and reporting.
	CC6.1.1	Tembo uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.
	CC6.8.3	Tembo has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.
	CC6.6.9	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected.

Section IV – Trust Services Category, Criteria, and Related Controls

CC7.0 Common Criteria Related to System Operations

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	CC7.2.1	Tembo tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.
	CC7.2.2	Tembo uses a system that collects and stores server logs in a central location. The system can be queried in an ad hoc fashion by authorized users.
	CC7.2.3	Tembo uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.
	CC7.2.4	Tembo's cloud infrastructure is monitored through an operational audit system that sends alerts to appropriate personnel.
	CC7.2.5	Tembo is using Drata to monitor the security and compliance of its cloud infrastructure configuration.
	CC7.2.6	Tembo does not use root account on infrastructure provider.
	CC6.6.9	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected.
	CC6.8.3	Tembo has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.
	CC7.1.2	Tembo engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.
	CC7.1.5	Tembo has a defined policy that establishes requirements for vulnerability assessments and reporting.

Section IV – Trust Services Category, Criteria, and Related Controls

CC7.0 Common Criteria Related to System Operations

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	CC7.3.1	Tembo tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.
	CC2.2.2	Tembo has implemented an incident response plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to business continuity/disaster recovery.
	CC2.2.3	Tembo has an established incident response plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.
	CC2.2.4	Tembo has identified an incident response team that quantifies and monitors incidents involving security at the company.
	CC2.2.5	Tembo has implemented an incident response plan that includes documenting lessons learned and a root cause analysis after incidents and sharing them with the broader engineering team to support business continuity/disaster recovery.
	CC2.2.2	Tembo has implemented an incident response plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to business continuity/disaster recovery.
CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	CC2.2.2	Tembo has implemented an incident response plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to business continuity/disaster recovery.
	CC2.2.3	Tembo has an established incident response plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.
	CC2.2.4	Tembo has identified an incident response team that quantifies and monitors incidents involving security at the company.
	CC7.3.1	Tembo tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.

Section IV – Trust Services Category, Criteria, and Related Controls

CC7.0 Common Criteria Related to System Operations

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.	CC7.5.1	Tembo has an established disaster recovery plan that outlines roles and responsibilities and detailed procedures for recovery of systems.
	CC7.5.2	Tembo performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.
	CC7.5.3	Tembo ensures that incident response plan testing is performed on an annual basis.
	CC7.5.4	Tembo has a defined business continuity plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption or significant change.
	CC2.2.2	Tembo has implemented an incident response plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to business continuity/disaster recovery.
	CC2.2.3	Tembo has an established incident response plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.
	CC2.2.4	Tembo has identified an incident response team that quantifies and monitors incidents involving security at the company.
	CC2.2.5	Tembo has implemented an incident response plan that includes documenting lessons learned and a root cause analysis after incidents and sharing them with the broader engineering team to support business continuity/disaster recovery.
	CC7.3.1	Tembo tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.

Section IV – Trust Services Category, Criteria, and Related Controls

CC8.0 Common Criteria Related to Change Management

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CC8.1.1	Only authorized Tembo personnel can push or make changes to production code.
	CC8.1.2	Separate environments are used for testing and production for Tembo's application.
	CC8.1.3	Tembo has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.
	CC8.1.4	Tembo ensures that code changes are tested prior to deployment to ensure quality and security.
	CC8.1.5	Tembo ensures that releases are approved by appropriate members of management prior to production release.
	CC6.1.1	Tembo uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.
	CC7.1.1	When Tembo's application code changes, code reviews and tests are performed by someone other than the person who made the code change.

Section IV – Trust Services Category, Criteria, and Related Controls

CC9.0 Common Criteria Related to Risk Mitigation

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions	CC9.1.1	Tembo conducts annual BCP/DR tests and documents according to the BCDR Plan.
	CC9.1.2	Tembo utilizes multiple availability zones to replicate production data across different zones.
	CC9.1.3	Tembo maintains cybersecurity insurance to mitigate the financial impact of business disruptions.
	CC9.1.4	Tembo maintains cybersecurity insurance to mitigate the financial impact of business disruptions.
	CC2.2.2	Tembo has implemented an incident response plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to business continuity/disaster recovery.
	CC2.2.3	Tembo has an established incident response plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.
	CC2.2.4	Tembo has identified an incident response team that quantifies and monitors incidents involving security at the company.
	CC2.2.5	Tembo has implemented an incident response plan that includes documenting lessons learned and a root cause analysis after incidents and sharing them with the broader engineering team to support business continuity/disaster recovery.
	CC3.1.1	Tembo has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.
	CC7.5.1	Tembo has an established disaster recovery plan that outlines roles and responsibilities and detailed procedures for recovery of systems.
	CC7.5.2	Tembo performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.
	CC7.5.4	Tembo has a defined business continuity plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption or significant change.

Section IV – Trust Services Category, Criteria, and Related Controls

CC9.0 Common Criteria Related to Risk Mitigation

Trust Services Criteria	Control Ref #	Tembo's Control Description
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.	CC9.2.1	Tembo maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.
	CC9.2.2	Tembo has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.
	CC6.4.1	Tembo maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.