SOC 3 Report

Glooko Inc. and Glooko AB
August 1, 2024 to August 2, 2025

An Independent Service Auditor's Report
on Controls Relevant to Security, Confidentiality, and Availability

AUDIT AND ATTESTATION BY

PRESCIENT
ASSURANCE

Prescient Assurance LLC
1900 Church Street, Suite 300
Nashville, TN 37203

www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319

Table of Contents

SECTION 1

Management's Assertion

Management's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Glooko Inc. and Glooko AB's system (the system) throughout the period August 1, 2024 to August 2, 2025, to provide reasonable assurance that Glooko Inc. and Glooko AB's service commitments and system requirements relevant to Security, Confidentiality, and Availability were achieved. Our description of the boundaries of the system is presented in Attachment A [A] and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of controls within the system throughout the period August 1, 2024 to August 2, 2025, to provide reasonable assurance that Glooko Inc. and Glooko AB's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, and Availability (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Glooko Inc. and Glooko AB's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment A [A].

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

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

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period August 1, 2024 to August 2, 2025, to provide reasonable assurance that Glooko Inc. and Glooko AB's service commitments and system requirements were achieved based on the applicable trust services criteria.

DocuSigned by:

Benjamin Chang

1B7DE4DC38D4464...

Benjamin Chang
VP, Security and IT Operations
Glooko Inc. and Glooko AB

PRESCIENT
ASSURANCE

SECTION 2

Independent Service Auditor’s Report

Independent Service Auditor's Report

To Glooko Inc. and Glooko AB

Scope

We have examined Glooko Inc. and Glooko AB's accompanying assertion in Section I, titled "Management's Assertion" (the assertion) that the controls within Glooko Inc. and Glooko AB's system (the system) were effective throughout the period August 1, 2024 to August 2, 2025, to provide reasonable assurance that Glooko Inc. and Glooko AB's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, and Availability (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

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

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

Service Organization's Responsibilities

Glooko Inc. and Glooko AB 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 Glooko Inc. and Glooko AB's service commitments and system requirements were achieved. In Section I, Glooko Inc. and Glooko AB has provided the accompanying assertion about the effectiveness of the controls within the system. When preparing its assertion, Glooko Inc. and Glooko AB is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the controls are not effective to achieve Glooko Inc. and Glooko AB's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Glooko Inc. and Glooko AB's service commitments and system requirements based on the applicable trust services criteria

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

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Glooko Inc. and Glooko AB's system were effective throughout the period August 1, 2024 to August 2, 2025, to provide reasonable assurance that Glooko Inc. and Glooko AB's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

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

Signed by:

Prescient Assurance

03DD05F2B23143B...

Prescient Assurance LLC
Nashville, TN
March 9, 2026

glooko®
BETTER TOGETHER

SECTION 3

Attachment A

Company Overview and Types of Products and Services Provided

Glooko Inc. and Glooko AB (Glooko or the Company) was founded in 2010 to help patients track and manage their diabetes-related glucose and insulin dosage information using its mobile and web applications. In 2016, Glooko merged with Swedish company Diasend to enhance and build a more modern platform based on the strengths of each other's works in the blood glucose sector. The US headquarters are located in Palo Alto, California. The European headquarters are in Gothenburg, Sweden. Glooko currently employs over 175 people.

The Glooko Core Platform empowers the management of diabetes and other chronic conditions by collecting and unlocking the power of data from blood-glucose (BG) meters, continuous glucose monitors (CGMs), insulin pumps, connected insulin pens, wearables, connected scales, blood pressure cuffs, and activity trackers – bringing insights together in one place. Data is easily uploaded – remotely via app or in-clinic, securely shared, and visualized in actionable charts and graphs. This creates a solid foundation enabling collaboration and confident treatment decisions. The platform is compatible with over 95% of diabetes devices along with biometric devices, giving people with diabetes and chronic conditions and their care teams the freedom of choice.

The Glooko Core Platform's key functions are:

- Diabetes dosage, tracking, and management for consumers via the web portal and mobile application
- Diabetes treatment management for providers via the web portal
- Third-party partner integration for diabetes treatment and management via the Application Programming Interface (API)

The Principal Service Commitments and System Requirements

Glooko provides customer access and use of its software subscription services as specified in the Master Services Agreement (MSA) and Software-as-a-Service (SaaS) Agreement. The overarching service commitment is to provide and secure Glooko's cloud-based enterprise software, designed for personalized remote patient monitoring for diabetes and other related conditions.

Glooko follows the principle of security to safeguard all protected information, which includes Personally Identifiable Information (PII), as well as the Glooko system as a whole. Glooko is committed to preventing unauthorized access and the potential abuse of information in order to meet contractual customer agreements, as well as statutory requirements. Glooko also maintains the service agreements and contracts with users and vendors to ensure that confidential information is not improperly disclosed.

In order to meet customer obligations, as well as abide by applicable laws and regulations for its services, Glooko is responsible for ensuring that the system is available to meet those requirements. With a commitment to availability in mind, Glooko maintains documented processes and employs redundancies as necessary to ensure that it meets its service level objective of system uptime. The Glooko identifies potential threats to the accessibility of the Glooko system and follows industry best practices to reduce the amount of downtime that would affect availability.

Glooko maintains confidentiality as it is required to ensure that the Company meets customer contractual obligations and applicable laws and regulations for information deemed confidential. Access to confidential data is limited to persons and users based on roles, needs, and permissions. Glooko's system logically protects data to prevent unauthorized access to its confidential data. The Company also maintains the service agreements and contracts with users and vendors in order to make sure that confidential information is not improperly disclosed.

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

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit

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

- The use of encryption technologies to protect system data both at rest and in transit
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties
- Confidential information must be used only for the purposes explicitly stated in agreements between The Company and user entities

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

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components
- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities
- Operational procedures supporting the achievement of availability commitments to user entities

Glooko's service commitments are documented in its contracts with customers. Among other items, they include:

- Security principles within the fundamental designs of the Glooko applications are designed to permit users access to the information they need based on their role as defined in the system while restricting them from accessing information not needed for their role. Roles are defined by each customer and are assigned a list of permissions accordingly.
- Glooko's service automatically locks up if left unattended for a specific period of time. Correct user credentials must be provided to re-access the application.
- Passwords are created by the customer and are required to be at least eight characters long and maintain a certain level of complexity. The password expiration term and reuse limit are configurable by the customer.

- The Glooko service communicates with secure Glooko-hosted and controlled servers and networks with the use of encryption technologies that protect user entities' information both in transit and at rest. Glooko disallows the use of low cipher strength in its Production service.
- Glooko ensures physical and technical security protections of customer data, as it uses servers located in highly secured hosting provider facilities that are subject to SOC 2 Type 2 examinations.
- Glooko employs redundant, next-generation firewalls, intrusion detection, and prevention services that are monitored twenty-four hours a day, seven days a week. Glooko uses internal and external threat prevention, delivering timely and accurate reports of its Production services.
- In addition to these controls, Glooko deploys up-to-date advanced threat protection services that help to identify, block, and track hacking attempts, scams, data breaches, adware, malware, spyware, trojans, phishing attempts, and other equally malicious requests.

Glooko system requirements are documented and communicated to employees through internal policies, standards, and procedures. These materials are available to all team members, and they agree to abide by them at the point of hire. The requirements include:

- System access is implemented according to need-to-know, least privilege, and separation of duties.
- System changes are managed according to change control procedures.
- System components are hardened consistent with internal standards.
- Confidential data is encrypted in transit and at rest.
- System components are monitored for security performance.
- Risks are managed and acknowledged by executive leadership.

Glooko's operational requirements that support the achievement of service commitments are communicated in its policies, procedures, and agreements with user entities. Glooko's policies and procedures define an organization-wide approach to how the system and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Glooko system.

The Components of the System Used to Provide the Services

People

A Board of Directors is in place and oversees management activities. Reporting to the Board of Directors, the Chief Executive Officer (CEO) is responsible for the overall operation of Glooko. Glooko's senior management team reports directly to the CEO. In addition, Glooko has established a Security Working Board to oversee management's information security activities.

Reporting to the CEO, each member of the senior management team has a distinct, separate responsibility within the organization. Roles and responsibilities have been segregated to the extent possible, and a formal organization chart has been developed. The CEO is responsible for the overall operation of Glooko. Glooko's senior management, listed below, report directly to the CEO:

- Chief Operations Officer
- Chief Medical Officer
- Vice President, Quality and Regulatory Management
- Chief Technical Officer
- Chief Financial Officer
- Chief Commercial Officer

Glooko's organizational structure is reflective of its Glooko culture, nature, and scope of its operations. It also provides a framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. An interactive organizational chart is available for all employees on the Company's Human Resources (HR) system. The organizational chart presents the executive team, key areas of authority and responsibility, reporting relationships, and Glooko's overall organizational hierarchy. The executive team and other stakeholders of management review the reporting relationships and organizational structures on a periodic basis as part of organizational planning, as well as to respond timely to changing entity commitments and requirements.

Processes and Procedures

Glooko's procedures are reviewed at least annually and updated as necessary to remain consistent with the system commitments and requirements.

Glooko's Code of Conduct, security, confidentiality, and disciplinary policies are communicated to employees upon hire. The policies are also available on an internal system for employees to reference, and any changes are communicated to employees via email. Additionally, with the acceptance of the employment offer, the employee acknowledges abiding by the policies communicated by HR.

Glooko's managed services and related support processes/procedures include but are not limited to:

- Onboarding procedures for new personnel and contractors to evaluate competency.
- Implementation support for new customers to ensure they have been provided with information on how to report failures, incidents, concerns, and other complaints to appropriate Glooko personnel.
- Access management procedures that ensure access to data, software, functions, and other IT resources are authorized, modified, or removed based on roles, responsibilities, or the system design.
- System development and maintenance procedures, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.
- Change management procedures to ensure changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet Glooko's commitments and system requirements.
- Health and performance monitoring procedures to manage capacity demand and to enable the implementation of additional capacity to help meet Glooko availability commitments and system requirements.
- Incident response procedures that address incidents to ensure logical and physical security incidents, failures, and vulnerabilities are identified and reported to appropriate Glooko personnel and acted upon in a timely manner.

- Disaster recovery procedures that ensure environmental protection, software, data backup process, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet Glooko's commitments and system requirements.

The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved

Personnel Management

Glooko has established appropriate lines of reporting, which facilitate the flow of information to appropriate people in a timely manner. Roles and responsibilities are segregated based on functional requirements. Glooko has an organizational chart that defines the organizational structure and reporting lines.

Glooko maintains a diverse, talented, high-performing organization and ensures that new hires have the appropriate knowledge, tools, and system access to perform successfully in their roles as soon as possible after joining the team. Glooko maintains and follows vetting, onboarding, and performance review procedures.

Prior to publishing a new job requisition, the hiring manager, in coordination with HR and any other relevant stakeholders, meets to discuss the business need for the new role, as well as other relevant attributes. The official role and responsibilities are then defined in the agreed-upon job description and published. Job descriptions are included with offers of employment to ensure the new hire has a clear understanding of the job duties and responsibilities, as well as Glooko expectations of the new hire.

Each candidate must meet minimum educational and/or experience requirements. The candidate's submitted credentials are verified during the interview process. The process is role and department-specific to ensure the candidate's skills and knowledge set are accurately assessed.

Each candidate to whom a conditional offer of employment has been extended undergoes and must pass an employment background check prior to being hired and starting work. This check may include a credit check and federal and state criminal records check. While the background

screening results for each applicant are individually assessed, Glooko operates in a highly regulated industry. As such, individuals convicted of crimes related to insurance fraud, theft, embezzlement, and moral turpitude may be automatically disqualified from employment.

After an offer of employment has been accepted, an HR team member informs IT of the new hire's start date and authorizes them to provision access to only three systems, each in an end-user capacity that is unable to administer any organizational functions. Any access request beyond these systems must be approved by HR, the hiring manager, and IT. All subsequent system access requests or modifications are approved by the individual's manager and/or the system owner. In addition, a company badge is provisioned by HR on the employee's first day of work. The access rights granted are set to coincide with the individual's role.

Within 30 days of their start date, each new hire must successfully complete Information Security Training.

Each employee undergoes at least one performance review on an annual basis consisting of a manager's review. These reviews, in addition to regularly scheduled one-on-one meetings, serve to recognize successful work, identify and respond to areas of improvement, and ensure the employee is sustaining the degree of professionalism, work productivity, and customer care that Glooko standards require.

Each employee who telecommutes has the same responsibilities as personnel situated within an office, such as the use of complex passwords, information security training, virus protection, lock screen, data backup, and encryption for any communication, including email and file sharing.

Policies and Procedures

HR has defined formal hiring policies and guidelines that assist in selecting qualified applicants for specific job responsibilities. Hiring policies require that certain levels of education and experience are met based on position and job requirements. Recruitment and termination duties and actions are defined in Glooko's HR Policies and Procedures. Appropriate levels of management and the Director of Human Resources concurrently approve all hires.

Glooko maintains specific job descriptions, which are available to personnel and intended to assist with employee development while also communicating job responsibilities. These job descriptions are drafted by HR and the hiring managers and include relevant requirements that Glooko looks for in potential candidates when filling the positions.

Training

Glooko conducts two types of information security awareness training: annual company-wide information security awareness training, which informs employees on how to detect and report security incidents, and periodic specialized security training for technical departments, such as secure coding practices.

Separation Procedures

HR creates a Jira ticket for the termination request and assigns IT to revoke all access. Employee and contractor access is revoked within two business days upon the termination of employment.

Vendor and Third-Party Management

When vendors or third-party providers have access to sensitive data or could impact the security, availability, and confidentiality of data within the environment, Glooko ensures that the agreements are in place and reviews their compliance status at least annually.

Security Management

The Glooko security process is described in the Glooko Information Security Policy, which consists of the following:

- Physical access security
- Electronic access security
- Definition of data, privacy, and how to transfer information when required
- Instructions to manage IT and digital assets such as virtual machines, servers, workstations, workspaces, application servers, web servers, database servers, and mail servers
- Instructions on how to proceed under emergency or disaster events
- Instructions related to IP and the way employees keep it safe

Glooko keeps customer information confidential and data up-to-date and error-free. Glooko also keeps the internal systems well-managed, replete with operating system updates, security patches, and limited access to licensed customers, authorized employees, and consultants.

As part of the security efforts, Glooko uses several strategies to detect issues including:

- Static and dynamic code analysis
- Logging user access to any activity on AWS accounts
- Logging of work performed on servers
- Tracking unusual network activity
- Tracking vulnerabilities and updates related to the server's operating system and applications
- Managing desktops and applying needed updates to antivirus, security patches, etc.
- Machine image update notification alerts when the next version is ready for use
- Security Content Automation Protocol (SCAP) scanning and monitoring that helps to identify any operating system/network vulnerability
- Uptime tracking related to the Service Level Agreement (SLA) or other services to the customers

In addition, Glooko performs third-party manual penetration testing on the Production infrastructure, allowing the opportunity to detect more complex security issues within products.

Security Policies

Glooko has designed several policies to protect the security of the systems, the privacy of customer data, and internal confidential information related to the ability to calculate applicable plans and rates for quotes and proposals. These security policies include:

- Security Working Board – This team is responsible for performing the Continuous Risk Analysis. The Security Working Board meets bi-monthly to discuss security issues and review concerns that have come up during prior months. The Security Working Board identifies areas that should be addressed during annual training and reviews and updates security policies as necessary.
- Employee Responsibilities – Glooko trains team members to implement proper security practices, including writing secure code, keeping a "clean desk," challenging unrecognized personnel, using anti-virus and anti-malware on Glooko computers, defining protected data, and restricting access to customer data.

Hard drive encryption and manual password entry after screen lock-out is the default for all Glooko devices.

- Report Security Incidents – All personnel are instructed to report any security issues such as a lost laptop, phone, or any issue that is perceived as suspect.
- Transfer of Sensitive Data – Glooko employs procedures about who, how, and what data can be shared with customers, contractors, developers, and/or all relevant stakeholders.
- Definition of PII/PHI – All personnel have a clear understanding of what constitutes PII, PHI, and the process the Customer Success team is required to follow to de-identify or anonymize it.
- Agreements – Non-Disclosure Agreement, Confidential Agreement (data management), Intellectual Property Agreements, background checks, and other legal processes are in place to protect customers from security and data breaches.
- Timeout/Disable Accounts – Glooko has several policies in place such as forced timeout from systems, disabling accounts after several failed password connection attempts, disabling accounts after receiving a report of a lost or stolen device, and providing automatic warnings if connections from unknown external IP addresses should occur. Accounts can also be disabled in the case of an emergency.
- Network Security, Firewalls – Glooko only allows approved devices to connect to the office network and a limited number of users from the DevOps team to connect to servers via special keys. Workstations, servers, database servers, load balancers, and workspaces all have a firewall that blocks almost all activity except for those expressly approved.
- Encryption – Glooko uses encryption in several processes, such as data on transit (SSL v1.2, HTTPS/SFTP), data on rest (AES-256 encryption, at field level in databases, and in all hard drives for any server), and in workstations/workspaces.

Software Development Lifecycle

Glooko's development framework emphasizes trustworthy computing with continuous development, deployment, and testing phases. Each environment has unit testing, automated QA testing, and manual QA testing. In addition, Glooko performs static code analysis, dynamic code analysis, and manual penetration testing over the deployed code.

Development Environment

Engineers start the Multi-Tenant Environment Development Cycle in the Development environment. Branches are created off of the primary development branch for each Jira ticket. When an Engineer is ready to introduce the code into the Development branch, they verify the work in their local environments and perform unit tests against the application. When all unit tests pass, a pull request (PR) is initiated in GitHub for the work to be pulled into the Development environment. All Engineers review the PR for code quality and accuracy. Once at least another Engineer approves the PR, the work is pulled into the Development branch and deployed for verification. The Engineer who performed the work is not allowed to approve their own work. The QA team tests the Development environment against the acceptance criteria of the Jira ticket to ensure the work that was pulled is correct in appearance and function through automated and manual testing. Once the environment has passed these tests, the code is merged and deployed into the Testing environment.

Testing Environment

The Testing environment is the first environment where multi-tenant customers may have access to the application. This environment is used for customers to test their integrations and file any issues against the application, as needed. The QA team runs automated and manual tests against this environment as new code is merged in. Regression testing also occurs to ensure that the end-to-end workflows perform as designed. Automated and performance testing are run against the environment, and reports are generated for QA team review. When the QA team has verified that the environment is stable, no regressions are found, and the customer (if applicable) has also verified the environment is working as expected, then the code base is merged into the Staging environment.

Staging Environment

The Staging environment is the final location for the QA team to perform environment verification. This is the final environment for deployment verification before moving the code to Production.

Production Environment

The Production environment is the final location of the Multi-Tenant Environment Development Cycle. The relevant stakeholders approve the release to Production with a Go/No-go decision. Production deployment playbooks are created for each Production deployment. The playbook outlines the dates and times each step of the deployment happens and the on-call staff who support the deployment.

New Features

The executive, Sales, Product, Customer Success, and Engineering teams routinely collaborate with ideas and suggestions in order to make a better product. The Sales team continually interviews prospective customers to discover their needs. Feature requests are handled by the Product team, who work with the customers to understand the business requirements, which are translated into Jira stories for Engineering so they can calculate the time and resources needed to accomplish such enhancements into the platform. The Product team updates the list of features with time and resource capacity, then members of the executive, Product, Engineering, and Customer Success teams decide which ones should be implemented and by when. The new desired features are proposed and accommodated in an upcoming sprint according to engineering capacity.

Change Management, Approval, And Tracking

All code changes require Engineering review from at least another developer other than the author of the code. These changes are tracked in Jira. Scans are run on the Testing environment. Glooko has strict control of changes such as:

- To add a change to the code, a PR must be created, which requires another developer to approve the change.
- Once the change is approved, the team lead merges it into the code branch; the system automates the deployment of the latest code for the Development environment.
- When the code is in the Development environment, the QA team performs automated and manual testing; if approved by QA, the process continues to Testing, then Staging.

- The process is different for the Production environment: changes must pass through all lower environments first. Once approved, the team lead merges the change into the code branch for Production deployment and a member of the DevOps team deploys it. A member of the QA team performs smoke testing to confirm that code has been properly deployed.
- In the instance of a bug, Glooko employs an expedited process that puts a hotfix into Production. The team creates a fix, tests the fix in Development, Testing, Staging, and finally deploys it to Production.

Service Monitoring

Glooko validates and monitors the functionality of its services (and dependencies) on a continuous basis aligned to SLA guarantees. Glooko keeps an uptime monitor for the Glooko Core Platform and its components. For each of these components, New Relic and CloudWatch monitor and alert for quality of service and failure in the components. The Production environment monitors and performs self-healing; servers are automatically replaced, or the number of machines is increased to improve the quality of service to the end user.

Incident Management And Response

It is the responsibility of each Glooko employee and contractor to immediately report perceived security incidents to the appropriate supervisor or security personnel.

A user is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the Security Policy immediately to security@glooko.com or the Global Security Head.

Users should report any perceived security incident to either their immediate supervisor, department head, security@glooko.com, or the Global Security Head. Reports of security incidents are escalated as quickly as possible.

Each incident is analyzed to determine if changes to the existing security structure are necessary. All reported incidents are logged and remedial action is indicated. It is the responsibility of the Global Security Head to prompt training on any procedural change that may be required as a result of the investigation of an incident.

Security incidents are promptly investigated. If criminal action is suspected, the Global Legal Head contacts the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the Federal Bureau of Investigations.

Customer incidents are documented and tracked by the Customer Success team until resolution using a combination of various tracking systems. Customer Success follows SLA severity levels which can be different per organization, but follow these standards:

- P1 – Major Business Impact; Service Down
- P2 – Significant Business Impact; No Workaround Available
- P3 – Minor Business Impact; Workaround Available
- P4 – No Business Impact; Workaround Available

Customer support for these incidents is comprised of two levels:

- Tier 1 – Tier 1 representatives engage with ultimate end-user issues. This is accessible via phone, chat, and email support for users with their hands directly on the product. Bugs, data incidents, and feature enhancements are tracked in Jira for proper assignment with Engineering and QA.
- Tier 2 – Tier 2 representatives handle escalated cases that Tier 1 is not able to resolve. Tier 1 issues should be resolved in the first user interaction via phone, chat, or with a simple email response. Complex issues requiring research and/or reproduction for the Engineering team are escalated to Tier 2 support.

Risk Assessment Process

A risk assessment is completed annually to review mission-critical aspects of the business, including technology, environment, market, compliance, regulation, fraud, and risk mitigation. The risk assessment is used to define and maintain a current set of controls based on the Trust Services Criteria. A vulnerability self-assessment, including external dynamic security testing, is performed quarterly, and manual penetration testing is conducted annually in order to identify any technical service vulnerabilities.

Management performs a vendor assessment for new vendors, business partners, and subservice organizations and reviews the SOC 2 Type 2 examination reports to assess potential risks, including security, availability, confidentiality, environmental, and technological changes that impact Glooko’s risk management strategy.

Information and Communication Systems

Glooko has implemented methods of communication to ensure that all employees understand their individual roles and responsibilities for its controls and to ensure that significant events are communicated in a timely manner. These methods include:

- Orientation for newly hired employees
- Ongoing training programs
- Annual re-confirmation of understanding of and compliance with the Information Security Policy
- Publishing diagrams, standards, and procedures regarding the design and operations of the system

Glooko provides customers with a description of the system in the MSA. The MSA has documented procedures for the identification and escalation of any issues or incidents.

Release notes for application changes are made available to employees and contractors (internal users) in Jira and are published and made available for external parties for each release.

Complementary Subservice Organization Controls (CSOCs)

The Company utilizes a subservice organization, AWS, to support the scope of services covered in this report. The controls represented by the subservice organization are not subject to this organization or included in this SOC 2 Type II report.

Subservice Organization	Functions Performed
Amazon Web Services, Inc. (AWS)	Hosting Services

This description presents the Company’s system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organization to meet certain applicable trust services criteria. The following table identifies the impacted criteria and the controls expected to be implemented at the subservice organization:

Complementary Subservice Organization Controls Related Criteria	Related Criteria
Hosted systems are scanned for vulnerabilities, and any identified vulnerabilities are tracked to resolution.	CC 3.2, CC 4.1, CC 5.1, CC 6.8, CC 7.1, CC 7.2
Antivirus or anti-malware solutions detect or prevent unauthorized or malicious software on hosted systems.	CC 4.1 and CC 6.8
Access to hosted systems requires strong authentication mechanisms.	CC 6.1
Data at rest on hosted systems is stored in an encrypted format.	CC 6.1
New and existing user access and permissions to hosted systems are approved by appropriate personnel prior to being granted.	CC 6.2, CC 6.3
Terminated user access permissions to hosted systems are removed in a timely manner.	CC 6.2, CC 6.3
User access permissions to hosted systems are reviewed by appropriate personnel on a regular basis.	CC 6.2, CC 6.3
Privileged access to hosted systems and the underlying data is restricted to appropriate users.	CC 6.3, CC 6.7
Access to the physical facilities housing hosted systems is restricted to authorized users.	CC 6.4
Production media is securely decommissioned and physically destroyed prior to being removed from the data center.	CC 6.5

Network security mechanisms restrict external access to the Production environment to authorized ports and protocols.	CC 6.6
Connections to the Production environment require encrypted communications.	CC 6.6, CC 6.7
System configuration changes are enforced, logged, and monitored.	CC 6.8, CC 7.1
System activities on hosted systems are logged, monitored, and evaluated for security events. Any identified incidents are contained, remediated, and communicated according to defined protocols.	CC 7.2, CC 7.3, CC 7.4
Access to make changes to hosted systems is restricted to appropriate personnel.	CC 8.1
Changes to hosted systems are documented, tested, and approved prior to migration to Production.	CC 8.1

Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant

All Common Criteria/Security, Availability and Confidentiality criteria were applicable to Glooko's system.