Independent Assurance Report on Go1 Pty. Ltd.'s Description of its System and on the Suitability of the Design of its Controls Relevant to Security, Availability, and Confidentiality Trust Services Criteria (SOC 2)

Prepared in accordance with the following:
AT-C section 105: Concepts Common to All Attestation Engagements
AT-C section 205: Assertion-Based Examination Engagements

assurancelab

CONTENTS

SECTION I –
ASSERTION OF GO1 PTY. LTD. MANAGEMENT

ASSERTION OF GO1 PTY. LTD. MANAGEMENT

30 January 2024

We have prepared the accompanying description of Go1 Pty. Ltd.'s ('Go1') Software as a Service System (the 'Description') for the purposes of the independent assurance report. We have prepared the Description in accordance with the following description criteria ('Description Criteria'):

- SOC 2: the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) with regards to the Description.

The Description is intended to provide report users with information about the Go1 Software as a Service System (the 'System') that may be useful when assessing the risks arising from interactions with Go1's system. This includes the controls that Go1 has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the following agreed criteria ('Agreed Criteria'):

- SOC 2: the trust services criteria relevant to Common Criteria/Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Go1 uses Microsoft Azure ('Azure' or 'subservice organization') 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 Go1, to achieve Go1's service commitments and system requirements based on the Agreed Criteria. The Description presents Go1's controls, the Agreed Criteria, and the types of complementary subservice organization controls assumed in the design of Go1'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 are necessary, along with controls at Go1, to achieve Go1's service commitments and system requirements based on the Agreed Criteria. The Description presents Go1's controls, the Agreed Criteria, and the complementary user entity controls assumed in the design of Go1's controls.

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

a. the Description presents Go1's Software as a Service System that was designed and implemented as of 12 January 2024 in accordance with the Description Criteria; and
b. the controls stated in the Description were suitably designed as of 12 January 2024 to provide reasonable assurance that Go1's service commitments and system requirements would be achieved based on the Agreed Criteria, if the controls operated effectively as of that date, and if complementary subservice organization controls and complementary user entity controls assumed in the design of Go1's controls operated effectively as of that date.

Kyle Jackson

Kyle Jackson
Director, Information Security
Go1 Pty. Ltd.

SECTION II –
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Go1 Pty. Ltd.

Scope

We have examined Go1 Pty. Ltd.'s ('Go1') accompanying description of its Software as a Service System (the 'Description') which has been prepared for the purposes of the independent assurance report.

Go1 prepared the Description based on the following description criteria ('Description Criteria'):

- SOC 2: the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) with regards to the Description.

The Description is intended to provide report users with information about the Go1 Software as a Service System (the 'System') that may be useful when assessing the risks arising from interactions with Go1's system. This includes the controls that Go1 has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the following agreed criteria ('Agreed Criteria'):

- SOC 2: the trust services criteria relevant to Common Criteria/Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Go1 uses Microsoft Azure ('Azure' or 'subservice organization') 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 Go1, to achieve Go1's service commitments and system requirements based on the Agreed Criteria. The complementary subservice organization controls have been reviewed by Go1 management. 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 includes complementary user entity controls that are necessary, along with controls at Go1, to achieve Go1's service commitments and system requirements based on the Agreed Criteria. The Description presents Go1's controls, the Agreed Criteria, and the complementary user entity controls assumed in the design of Go1's controls. The complementary user entity controls have not been assessed by our examination and remain the responsibility of those related entities to complete their own review.

Service Organization's Responsibilities

Go1 is responsible for its service commitments and system requirements and for designing and implementing effective controls within the system to provide reasonable assurance that Go1's service commitments and system requirements were achieved. Go1 has provided the accompanying assertion titled "Assertion of Go1 Pty. Ltd. Management" (the 'Assertion') about the Description and the suitability of the design of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the Agreed Criteria. Go1 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 Agreed Criteria and stating the related controls in the Description; and identifying the risks that threaten the achievement of the Go1's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of the design of controls stated in the Description based on our examination. Our examination was conducted in accordance with AT-C 105 and AT-C 205 put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects:

- The Description is presented in accordance with the Description Criteria.
- The controls stated in the Description were suitably designed.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the Description of Go1's system and the suitability of the design of controls involves the following:

- Obtaining an understanding of the system and Go1'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 Go1 achieved its service commitments and system requirements based on Agreed Criteria.
- Evaluating the overall presentation of the Description.

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. 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.

Opinion

In our opinion, in all material respects,

1) the Description presents Go1's Software as a Service System that was designed and implemented as of 12 January 2024, in accordance with the Description Criteria; and
2) the controls stated in the Description were suitably designed as of 12 January 2024, to provide reasonable assurance that Go1's service commitments and system requirements would be achieved based on the Agreed 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 Go1's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Go1, user entities of Go1's System, business partners of Go1 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 Agreed Criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

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

Erika Villanueva

Erika Villanueva, CA, CPA
AssuranceLab Pty Ltd
Sydney, Australia
30 January 2024

SECTION III –
GO1 PTY. LTD.'S DESCRIPTION OF ITS SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Go1 Pty. Ltd. ('Go1') was founded in 2015 by Andrew Barnes, Vu Tran, Chris Eigeland, and Chris Hood and is headquartered in Brisbane, Australia. Go1's objective is to develop a platform for business education and training, including a digital learning library that provides professional development, well-being, and compliance courses for learners to help encourage positive potential.

Go1's core product is a Software as a Service offering called Go1 Premium, which brings content and digital learning together into a single subscription. Industries served by Go1 include all industries with HR training requirements, and supports customers across the world.

Description of Services Provided

Go1's core product, Go1 Premium, is a Software as a Service System that includes the following services offerings:

- Go1 Content Library
  Aggregated learning content from over 250 industry-known eLearning providers.

- Go1 Platform
  A lightweight learning management system (LMS) for administrators and learners to access Go1 content. The Go1 platform allows customers to upload their content instead of consuming Go1 content.

- Go1 Content Hub
  A tool for administrators to access Go1 content and import it to the businesses' learning platform.

Principal Service Commitments and System Requirements

Go1 has established processes, policies, and procedures to meet its objectives related to its Go1 Software as a Service System (the 'System'). Those objectives are based on the purpose, vision, and values of Go1 as well as commitments that Go1 makes to user entities, the requirements of laws and regulations that apply to Go1's activities, and the operational requirements that Go1 has established.

Commitments are documented and communicated in customer agreements, as well as in public descriptions of the System. The operational requirements are communicated in Go1's processes, policies and procedures, system design documentation, and customer agreements. This includes policies around how the System is designed and developed, how the System is operated, how the system components are managed, and how employees are hired, developed, and managed to support the System.

Components of the System

Infrastructure

Go1's primary infrastructure used to provide the System includes the cloud-hosted networking, compute, and database components of Microsoft Azure (Azure).

System	Type	Description
Cloudflare	Network Services	DNS, load balancing, DDOS protection, web firewall, and encryption.
Azure Kubernetes Service (AKS)	Cloud Compute	Deploy and scale containers on managed Kubernetes.
Azure Functions	Cloud Compute	Application services using an event-driven, serverless architecture.
Azure SQL Database	Data Storage	Storage of client data.
Azure Blob Storage	Data Storage	Storage of client documents.
Amazon Simple Storage Service (S3)	Data Storage	Storage of non-critical content hosting functions.
Azure Load Balancer	Networking	Distributes incoming traffic among virtual machines.
Azure Key Vault	Encryption	A cloud service to securely store keys, passwords, certificates, and other secrets.

Software

Primary software is used to support Go1's system.

Software	Purpose
Go1 Premium	The Software as a Service product provided to Go1 customers.
Azure Defender	Cloud security posture management (CSPM) and cloud workload protection (CWP) that finds weak spots across cloud configurations.
Azure Security Center	Monitoring and managing the security of virtual machines and other cloud computing resources within the Microsoft Azure public cloud.
Microsoft Sentinel	A cloud-native security information and event manager (SIEM).
Okta, Auth0	Authentication software used to identify and authenticate users for access control to the systems.
GitLab	Source code repository used to manage the software code and version control.

Software	Purpose
GitLab CI/CD	Continuous integration / continuous delivery software used to manage the pipeline of change release testing and deployment.
1Password	Enterprise password manager used to store authentication secrets and strengthen password security.
Jamf, Microsoft Intune	Mobile device management software used to track and manage security policies on endpoint devices.
Palo Alto Cortex XDR	Anti-virus software used to protect endpoint devices from malware.
Datadog	System monitoring software used to log events and raise alerts to support system security and availability.
OWASP ZAP	Vulnerability scanning software to identify, log and resolve technical vulnerabilities.
JIRA, Zendesk	Ticketing software used to log events and requirements to support the internal controls.
Opsgenie	Incident management platform used to alert incidents from monitoring systems and custom applications.
HiBob	Human resources information system used to manage employee processes like onboarding, offboarding and performance.
Vanta	Security and compliance software used to monitor and manage the security, risk, and control activities to support compliance.
Microsoft Office 365	Microsoft's suite of enterprise productivity, collaboration, and communication tools.

People

Go1 has 650 people that are organized into the following functional areas:

- Senior Leadership: Responsible for the overall governance of Go1; including overseeing company-wide activities, goals and objectives.
- Product: Responsible for understanding customer requirements, collecting, refining, and clarifying feature requests and development efforts, managing feature rollouts and related communications either internally and/or with customers.
- Engineering: Responsible for building, testing, and deploying Go1 code and feature changes in coordination with the product team. Engineering is also responsible for service availability, performance and scale monitoring and incident response.
- Security: Responsible for ensuring the confidentiality, integrity and availability of data handled and system security for Go1. The security team manages security incident detection and response, annual penetration testing and vulnerability management, and risk and compliance oversight.
- IT: Responsible for IT services and support functions across Go1 including onsite and remote

support, access requests, software licenses and supporting People Operations with employee onboarding and offboarding.

- People Operations: Responsible for strategic partnering, talent acquisition, people experience, culture & community, communications, and payroll.
- Legal: Responsible for negotiating contractual obligations with third parties and partners/suppliers, legal terms and conditions and legal aspects of privacy.
- Sales: Responsible for aligning requirements and onboarding new customers, product branding, market positioning and attracting customers.
- Customer Success: Responsible for the success of existing customers leveraging Go1 Premium features.
- Finance: Responsible for the financial performance of Go1.

Data

The data collected and processed by Go1 includes the following types:

- First name and last name
- Postal address
- Contact information (including email and/or phone number)
- IP address
- User activity within Go1 Premium

Processes, Policies and Procedures

Processes, policies, and procedures are established that set the standards and requirements of the System. All personnel are expected to comply with Go1's policies and procedures that define how the System should be managed. The documented policies and procedures are shared with all Go1's employees and can be referred to as needed.

Compliance Management Platform

Go1 uses compliance automation software, Vanta, to support the design, implementation, operation, monitoring, and documentation of internal controls. Vanta leverages APIs to centralize the monitoring of Go1's information assets across their infrastructure provider, identity manager, code repository, and endpoint devices. These APIs in combination with compliance automation functions in Vanta support the continuous monitoring of control activities for Go1's people, devices, policies, procedures and plans, risk assessments, third-party vendor assessments, system monitoring and the security configurations of these critical systems.

Using Vanta does not reduce management's responsibility for designing, implementing and operating an effective system of internal control. Go1 evaluates the accuracy and completeness of the information stored in Vanta and conducts annual vendor risk assessments including review of Vanta's SOC 2 Type 2 reports that includes the trust services criteria related to processing integrity.

Physical Security

The critical infrastructure and data of the System are hosted by Microsoft Azure. There are no trusted local office networks. As such, Microsoft Azure is responsible for the key physical security controls that support the System.

Logical Access

Go1's logical access processes restrict access to the infrastructure, software, and data to only those that are authorized for access. Access is based on the concept of least privilege that limits the system components and access privileges to the minimum level required to fulfil job responsibilities.

The in-scope systems require approval and individual authentication practices prior to gaining access. Okta authentication software is used for identity management and single-sign on. Access management processes are followed to ensure new and modified access is approved, terminated users access is removed, and access rights are reviewed quarterly and adjusted when no longer required. Additional information security policies and procedures require Go1 employees to use the systems and data in an appropriate and authorized manner.

Automated and manual security practices are used to protect the perimeter security and network to prevent unauthorized access attempts and tampering from third-party actors with malicious intent. Those include applying encryption of data and communications, bi-weekly testing for and remediation of technical vulnerabilities and applying network controls like firewalls and event monitoring to prevent and detect unauthorized activity.

Go1 employee workstations are required to follow defined security practices to mitigate the risks of data leakage and malware that may compromise the devices, system access and sensitive data. Jamf and Microsoft Intune mobile device management software are used to monitor, systematically enforce device requirements, and provide remote management capabilities for the workstations.

System Operations

Backup and restoration procedures for the System are defined and followed. The System is monitored through a combination of automated and manual processes to prevent and detect any issues with the infrastructure, software, and data. Alerts and logs are monitored with incident management processes defined for handling and resolving adverse events.

Go1's critical infrastructure and data are hosted by Microsoft Azure with multiple availability zones to provide failover capability in the event of an outage of one of the data centers. Redundancy and disaster recovery in continuity considerations are built into the system design of Microsoft Azure to support Go1's availability objectives. These are supported by the system monitoring, incident management processes and defined recovery and continuity plans.

Change Control

Go1 operates a defined process for software development with supporting policies and procedures. Change requests and requirements are logged and prioritized for development. Changes include those related to functionality improvements, bug fixes, security and reliability-related enhancements, and other updates to the Go1 software to support Go1's System and objectives.

Separate environments are used to support development and testing activities in isolation from the production environment. GitLab version control software is used for the code repository that tracks all changes to the Go1 software, including managing versions and roll-back capability in the event of a failed change release. A continuous integration / continuous deployment (CI/CD) pipeline is configured using GitLab CI/CD to enforce key process steps and checks prior to new versions of the code base being deployed into the production environment. Changes to the infrastructure configurations and settings are managed as code, subject to the same process steps and checks prior to impacting the production environment.

Data Governance

Go1 uses data to support the System objectives and services. An approach to effective data governance has been established to understand and communicate the data that's used in the System, the objectives and requirements of that data, and the commitments of Go1.

Established processes, policies, and procedures define the operational requirements for data governance, including how data is classified, handled, and used by the System in supporting the objectives and services.

Boundaries of the System

The scope of this report includes the Go1 Software as a Service System (the 'System'). This report does not include the cloud hosting services provided by Microsoft Azure.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

The effectiveness of controls is dependent on the integrity and ethical values of the people who implement, manage, and monitor them. Integrity and ethical values are important foundations of Go1's control environment, affecting the design, implementation, and monitoring of the controls. Integrity and ethical behavior are supported by Go1's culture, governance, hiring and onboarding practices, ethical and behavioral standards, the way those are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Commitment to Competence

Go1's competence of employees includes the knowledge and skills necessary to accomplish employees' roles and responsibilities, in support of Go1's objectives and commitments. Management's commitment to competence includes careful consideration of the competence levels required for each role, the requisite skills, knowledge, and experience, and the actual performance of individuals, teams, and the company as a whole.

Management's Philosophy and Operating Style

Go1's management philosophy and operating style is a purpose-driven, risk-based approach to pursuing the company objectives and satisfying Go1's commitments. Risk taking is an essential part of pursuing the objectives. A formal approach is taken to understanding those risks and being deliberate about which risks are acceptable, and where risk mitigation actions are required.

Organizational Structure and Assignment of Authority and Responsibility

Go1's organizational structure provides the framework within which its activities for achieving the objectives are planned, executed, managed, and monitored. An organizational structure has been developed to suit Go1's needs and is revised over time as the company grows and requirements change.

Roles and responsibilities are further established and communicated through documented policies, and job descriptions, as part of individual performance review processes, reviewing and communicating team and functional performance, and the various operational team and governance meetings.

Human Resource Policies and Practices

Go1's employees are the foundation for achieving the objectives and commitments. Go1's hiring, onboarding and human resource practices are designed to attract, develop, and retain high-quality employees. That includes training and development, performance evaluations, compensation, and promotions, providing personal support and perks for individuals, recognizing team and company success, and building a culture of alignment to a shared purpose and vision. It also includes disciplinary processes and business planning to avoid single-person dependencies to ensure the objectives and commitments are not reliant on individuals.

Risk Assessment Process

Risk Assessments

Go1's risk assessment process identifies and manages risks that threaten the achievement of the objectives and commitments. This includes risks that may affect the security, reliability or integrity of the services provided to user organizations and other interested stakeholders.

A formal process is followed to identify, assess, treat, and monitor the risks to ensure the risks are aligned to the risk appetite and objectives of Go1, and mitigated or avoided where appropriate. Risks identified in this process include:

- Operational risk – changes in the environment, staff, or management personnel, reliance on third parties, and threats to security, reliability, and integrity of Go1's operations.
- Strategic risk – new technologies, changing business models, and shifts within the industry.
- Compliance – legal and regulatory obligations and changes.
- Financial – the sustainability of Go1 and resources supporting the objectives.

These risks are identified by Go1 management, employees, and third-party stakeholders, and updated in the risk register as a single source of monitoring the risks. The formal risk assessments ensure the ongoing commitment of management, and support completeness and an evolving view of the risk landscape in Go1's context.

Integration with Risk Assessment

Established internal controls include Go1's policies, procedures, automated system functions and manual activities. The controls are designed and implemented to address the identified risks, and to meet the obligations and criteria set by laws, regulations, customer commitments and other compliance obligations. The controls follow a continual improvement methodology in consideration of the costs and benefits of such control improvements and recognizing the changing landscape and requirement of those controls as Go1 grows and the associated risks change.

Information and Communications Systems

Information and communication are a core part of Go1's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control Go1's operations effectively. The information and communication systems

consider the internal control requirements, operating requirements, and the needs of interested parties including employees, customers, third-party vendors, regulators, and shareholders.

The information and communication systems include central tracking systems that support Go1's established processes, as well as various meetings, and documented policies, procedures, and organizational knowledge.

Monitoring Controls

Management monitors the controls to ensure that they are operating as intended and that controls are modified and continually improved over time. Leadership, culture, and communication of the controls are important enablers to the effectiveness of the controls in practice. This ensures buy-in amongst the employees and empowers Go1's team and individuals to prioritize the performance and continual improvement of the controls. Evaluations are performed during the course of business, in management reviews, and by independent auditors to assess the design and operating effectiveness of the controls. Deficiencies that are identified are communicated to responsible control owners to agree on remediation actions or reinforce the control requirements and importance. Corrective actions are tracked with agreed timelines and ownership for remediation with ownership of management and the Board, to ensure appropriate actions are completed in a timely manner.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the examination date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the examination date.

Criteria Not Applicable to the System

All Common Criteria/Security, Availability, and Confidentiality Trust Services Criteria were applicable to Go1's Software as a Service System.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

This report does not include the cloud hosting services provided by Microsoft Azure (Azure).

Subservice Description of Services

Microsoft Azure, commonly referred to as Azure, is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers.

Complementary Subservice Organization Controls

Go1's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the Agreed Criteria related to Go1's services to be solely achieved by Go1 control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Go1.

The following subservice organization controls should be implemented by Azure to provide additional assurance that the Agreed Criteria described within this report are met.

Subservice Organization – Microsoft Azure		
Category	**Criteria**	**Control**
Common Criteria/ Security	CC6.1-CC6.8	Logical access measures are established and followed to ensure access to systems and data is restricted to authorized personnel with technical safeguards and ongoing assessments to reduce the risk of system and data breaches.
	CC6.4	Procedures have been established to restrict physical access to the data center to authorized employees, vendors, contractors, and visitors.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		Security verification and check-in are required for personnel requiring temporary access to the interior data center facility including tour groups or visitors.
		The data center facility is monitored 24x7 by security personnel.
		Physical access to the data center is reviewed quarterly and verified by the data center management team.

Subservice Organization – Microsoft Azure		
Category	**Criteria**	**Control**
	CC7.1-CC7.5	Incident management and response policies and procedures are established and followed to identify, analyze, classify, respond to, and resolve adverse events.
	CC8.1	Formal processes are established and followed to ensure system changes are documented, tracked, prioritized, developed, tested, and approved prior to deployment into production.
Availability	A1.2	Azure has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements.
		The BCP team conducts testing of the business continuity and disaster recovery plans established for Azure services, per the defined testing schedule for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly.
		Backups of key Azure service components and secrets are performed regularly and stored in fault-tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately.
		Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
		Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.
		Customer data is automatically replicated within Azure to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups.
		Azure services are configured to automatically restore customer services upon detection of hardware and system failures.
		Data center Management team maintains and tests data center-managed environmental equipment within the facility according to documented policy and maintenance procedures.

Subservice Organization – Microsoft Azure		
Category	**Criteria**	**Control**
		Environmental controls have been implemented to protect systems inside data center facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.

Go1 management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Agreed Criteria through written contracts and published terms of service. In addition, Go1 performs monitoring of the subservice organization controls by reviewing attestation reports and monitoring the performance of the subservice organization controls.

COMPLEMENTARY USER ENTITY CONTROLS

Go1's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Agreed Criteria related to Go1's services to be solely achieved by Go1 control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Go1's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Agreed Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

- Enabling Security Assertion Markup Language (SAML) or Microsoft OpenID Connect (OIDC) for their Go1 portal.
  Managing their Go1 portal, including the proper assignment of access permissions to the portal, and user access to the Go1 content library.
- Ensuring authorized users are provided administrator privileges in their Go1 portal.
- Reviewing, properly configuring, and securing access to their own data when accessing it using their own applications via Go1's Application Programming Interface (API)
- Administrating and configuring learning content not provided in Go1's content library

SOC 2 TRUST SERVICES CRITERIA

Trust Services Categories Selected by Go1

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

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality
Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

SECTION IV –
CRITERIA AND RELATED CONTROLS

SOC 2 TRUST SERVICES CRITERIA

Trust Services Criteria for the Security Category

Common Criteria 1: Control Environment

CC1.0	Criteria	Control Activity
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The code of conduct is documented to communicate conduct standards and enforcement procedures.
		The code of conduct is signed off by new hires upon commencement of their role.
		Disciplinary procedures define the consequences and method of handling misconduct.
		Defined processes are in place for employees to report unethical behavior in a confidential manner.
		Background checks are completed for candidates prior to employment.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Go1 operates independent layers of management between the board of directors, senior management, and operational management.
		Board of directors meetings are held at least annually for organizational oversight and governance.
		The board charter sets out the responsibilities and scope of the board of directors.
		The board is responsible for oversight of the systems and data security of Go1 with review at least annually.
		Management reviews are conducted at least annually for oversight and governance of the company and team performance.
		The risks and control effectiveness are reported to the board at least annually.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Management meetings are held at least quarterly to review the company operations.
		The organization chart documents the reporting lines, accountable executives, and team and individual roles and is updated whenever there are changes in personnel.

CC1.0	Criteria	Control Activity
		Job descriptions are documented for employees and management setting out the responsibilities, role requirements and any key accountabilities.
		Management considers interactions with, and the need to monitor the activities of third parties when documenting the organizational chart and defining job descriptions.
		Business planning is performed at least annually to establish business requirements and objectives.
		The entity's third-party agreements outline and communicate: the scope of services, roles and responsibilities, terms of the business relationship, communication protocols, compliance requirements, service levels, and just cause for terminating the relationship.
		Upon hire, employees are required to read and acknowledge the acceptable use policy.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The People Operations team is responsible for attracting individuals with competencies and experience that align with the company goals and objectives.
		An employee hiring and onboarding process is defined including approval of the new role, vetting of candidates, and ensuring role requirements are met.
		New hire candidates are independently approved prior to selection and onboarding.
		Background checks are completed for candidates prior to employment.
		Go1 operates independent layers of management between the Board of Directors, senior management, and operational management.
		Management meetings are held at least quarterly to review the company operations.
		Employee performance reviews are conducted at least annually.
		Security awareness training is provided to Go1 employees.

CC1.0	Criteria	Control Activity
		Training of employees follows defined processes of the training requirements and plans to align to the objectives and employee requirements.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Disciplinary procedures define the consequences and method of handling misconduct.
		Defined processes are in place for employees to report unethical behavior in a confidential manner.
		The organization chart documents the reporting lines, accountable executives, and team and individual roles and is updated whenever there are changes in personnel.
		Company all-hands meetings are held to communicate significant updates and raise awareness of the security and compliance objectives.
		Job descriptions are documented for employees and management setting out the responsibilities, role requirements and any key accountabilities.
		The documented policies and procedures establish roles, responsibilities, and area accountabilities.
		Employment contracts are formed with employees.
		Employee performance reviews are conducted at least annually.
		Performance measures are defined for each team or functional area to support the company objectives.
		Executive management has established performance measures, including the incentives and rewards for exceeding expectations, as it relates to teams and functional areas.

Common Criteria 2: Information and Communication

CC2.0	Criteria	Control Activity
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Company all-hands meetings are held to communicate significant updates and raise awareness of the security and compliance objectives.
		Organizational and information policies and procedures are made available to employees through the intranet.
		Information logs are maintained to track events metrics and indicators to support the processes and internal control requirements.
		Go1 has documented the systems and data flows to identify and document the relevant internal and external information sources of the system.
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.	The code of conduct is signed off by new hires upon commencement of their role.
		Management meetings are held at least quarterly to review the company operations.
		The responsibilities for information security and privacy are established documented and communicated to Go1employees.
		Security awareness training is provided to Go1employees.
		The requirements for managing data are established in the data classification, handling, retention, and disposal policies.
		The defined company objectives include a mix of strategic, financial, and operational level objectives to guide functional areas and teams on how they support the company objectives and identify the risks that threaten achievement of the objectives.
		The company objectives are communicated to employees for awareness.
		Changes are assessed to determine whether communications to users of the system are required and are performed accordingly.

CC2.0	Criteria	Control Activity
		Release notes for changes are sent to internal and external stakeholders.
		The acceptable use policy sets out the roles responsibilities and requirements to maintain the security of systems, data, and endpoint devices.
		On at least an annual basis or when changes are made employees are required to read and acknowledge the information security policies and procedures.
		Organizational and information policies and procedures are made available to employees through the intranet.
		On at least an annual basis security awareness updates are communicated to employees including the handling of incidents and security related matters.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The entity's third-party agreements outline and communicate: the scope of services, roles and responsibilities, terms of the business relationship, communication protocols, compliance requirements, service levels, and just cause for terminating the relationship.
		Management has assigned responsibility and accountability for the management of risks and governance associated with third parties to appropriate personnel.
		Changes are assessed to determine whether communications to users of the system are required and are performed accordingly.
		Release notes for changes are sent to internal and external stakeholders.
		Users of the system are provided mechanisms for reporting any requests incidents, failures, or security-related matters.
		Changes to commitments requirements and responsibilities are communicated to third parties by the appointed account manager.

CC2.0	Criteria	Control Activity
		Awareness of how to report incidents, failures, and any security related matters is supported through user communications.
		Documentation is provided to users to guide them on the operation of the system.
		Customer administrators are provided with training on how to administer the system and perform their responsibilities.
		Customer commitments, requirements, and responsibilities are outlined and communicated through formal service terms.

Common Criteria 3: Risk Assessment

CC3.0	Criteria	Control Activity
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Performance measures are defined for each team or functional area to support the company objectives.
		The defined company objectives include a mix of strategic, financial, and operational level objectives to guide functional areas and teams on how they support the company objectives and identify the risks that threaten achievement of the objectives.
		The company objectives are communicated to employees for awareness.
		The company objectives are used as a basis for identifying and assessing risks.
		Business planning is performed at least annually to establish business requirements and objectives.
		The control framework is based on a recognized industry standard.
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.	The risk register is used to track and monitor the identified risks, ratings, mitigation practices and planned actions.
		The company objectives are used as a basis for identifying and assessing risks.
		Documented policies and procedures are in place to guide personnel when performing a risk assessment.
		Management has defined risk assessment criteria with scales and guidance on how to measure and classify risks and provide a common language for comparing and prioritizing risks.
		Risk assessments are completed at least annually to identify and analyze the risks and identify any required mitigation actions.
		The risk assessments include consideration of risks related to information security, compliance requirements and third-party dependencies.
		Identified risks are rated using a risk evaluation process and ratings are approved by management.

CC3.0	Criteria	Control Activity
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.
		Management has defined a third-party vendor risk management approach for evaluating third-party risks.
		A formal risk assessment is completed for each new vendor prior to commencing the services provided.
		An annual vendor risk assessment is completed to ensure the identification and treatment of risks remains accurate and appropriate.
		Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.
		Risk assessments are conducted at least annually for the inventory of system assets to identify risks and actions required to mitigate those risks.
		As part of the risk assessment process controls within the environment are modified and implemented to mitigate the identified risks.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The risk register is used to track and monitor the identified risks, ratings, mitigation practices and planned actions.
		The risk assessments include consideration of risks related to information security compliance requirements and third-party dependencies.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The risk register is used to track and monitor the identified risks, ratings, mitigation practices and planned actions.
		The risk assessments include consideration of risks related to information security, compliance requirements and third-party dependencies.

CC3.0	Criteria	Control Activity
		The risk assessment process identifies and assesses changes that could significantly impact the system of internal control.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.
		Management has assigned responsibility and accountability for the management of risks and governance associated with third parties to appropriate personnel.

Common Criteria 4: Monitoring Activities

CC4.0	Criteria	Control Activity
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.	The risk register is used to track and monitor the identified risks, ratings, mitigation practices and planned actions.
		Management is assigned ownership of ongoing monitoring of the effectiveness of controls and that key policy and process requirements are being adhered to.
		Key policies and processes are reviewed and updated at least annually to confirm their effectiveness accuracy and compliance.
		An annual vendor risk assessment is completed to ensure the identification and treatment of risks remains accurate and appropriate.
		Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.
		Backup and restoration tests are performed on at least an annual basis to ensure the recovery controls are effective.
		The control framework is based on a recognized industry standard.
		The key control activities are individually assigned to owners responsible for ensuring effective and consistent performance of the controls.
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.	Board of directors meetings are held at least annually for organizational oversight and governance.
		The board charter sets out the responsibilities and scope of the board of directors.
		Management is assigned ownership of ongoing monitoring of the effectiveness of controls and that key policy and process requirements are being adhered to.
		Key policies and processes are reviewed and updated at least annually to confirm their effectiveness accuracy and compliance.

CC4.0	Criteria	Control Activity
		Management tracks whether control failures, breaches of policies and procedures, customer complaints, and other issues are assessed, tracked, and monitored through to resolution, as applicable.
		The third-party vendor register includes a listing of material vendors for tracking and monitoring.
		Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.
		Management has assigned responsibility and accountability for the management of risks and governance associated with third parties to appropriate personnel.
		Security related change requirements based on vulnerabilities, security, risk mitigation requirements or other ongoing improvements have defined criteria to determine their relative priority or timeline for remediation.
		The control framework is based on a recognized industry standard.
		The key control activities are individually assigned to owners responsible for ensuring effective and consistent performance of the controls.
		The control framework is reviewed at least annually by the control owners to ensure the control descriptions and owners are accurate and that the controls are operating effectively as described.
		As part of the risk assessment process controls within the environment are modified and implemented to mitigate the identified risks.
		The risks and control effectiveness are reported to the board at least annually.

Common Criteria 5: Control Activities

CC5.0	Criteria	Control Activity
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.	The risk register is used to track and monitor the identified risks, ratings, mitigation practices and planned actions.
		Risk assessments are completed at least annually to identify and analyze the risks and identify any required mitigation actions.
		The risk assessments include consideration of risks related to information security, compliance requirements and third-party dependencies.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.
		The control framework identifies and documents the key control activities to support the defined objectives, regulations, and compliance requirements.
		The control framework is based on a recognized industry standard.
		An assessment of functional roles and system access privileges has been completed to identify the requirements for segregation of duties.
		The key control activities are individually assigned to owners responsible for ensuring effective and consistent performance of the controls.
		The control framework is reviewed at least annually by the control owners to ensure the control descriptions and owners are accurate and that the controls are operating effectively as described.
		As part of the risk assessment process controls within the environment are modified and implemented to mitigate the identified risks.
		The business continuity plans document the disruptive scenarios, response plans, roles and responsibilities, key internal and external stakeholders, escalation procedures, communication channels to effectively manage critical events.

CC5.0	Criteria	Control Activity
		The business continuity plan is tested at least annually to ensure the response plans to critical events are effective.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The disaster recovery plan is tested at least annually to confirm that recovery procedures are effective.
		The disaster recovery plan includes defined procedures to recover from significant events and is reviewed and updated at least annually.
		Backup and restoration tests are performed on at least an annual basis to ensure the recovery controls are effective.
		The control framework identifies and documents the key control activities to support the defined objectives, regulations, and compliance requirements.
		The control framework is based on a recognized industry standard.
		The key control activities are individually assigned to owners responsible for ensuring effective and consistent performance of the controls.
		The control framework is reviewed at least annually by the control owners to ensure the control descriptions and owners are accurate and that the controls are operating effectively as described.
		The business continuity plans document the disruptive scenarios, response plans, roles and responsibilities, key internal and external stakeholders, escalation procedures, communication channels to effectively manage critical events.
		The business continuity plan is tested at least annually to ensure the response plans to critical events are effective.
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.	Job descriptions are documented for employees and management setting out the responsibilities, role requirements and any key accountabilities.
		The documented policies and procedures establish roles, responsibilities, and area accountabilities.

CC5.0	Criteria	Control Activity
		Documented policies and procedures are in place to guide personnel when performing a risk assessment.
		Key policies and processes are reviewed and updated at least annually to confirm their effectiveness, accuracy, and compliance.
		Management has defined a third-party vendor risk management approach for evaluating third-party risks.
		The control framework identifies and documents the key control activities to support the defined objectives, regulations, and compliance requirements.
		The control framework is reviewed at least annually by the control owners to ensure the control descriptions and owners are accurate and that the controls are operating effectively as described.
		The risks and control effectiveness are reported to the board at least annually.

Common Criteria 6: Logical and Physical Access Controls

CC6.0	Criteria	Control Activity
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.	A password management system is used to ensure quality passwords are applied for user access.
		The security policies set out the requirements for managing information security across Go1's operations.
		The access control policy sets out the required system access controls for secure authentication and account use.
		An inventory of system assets and components is maintained to classify and manage the information assets.
		Access to the network and infrastructure for Go1employees requires strong authentication mechanisms.
		Access to Go1 software for Go1 employees requires strong authentication mechanisms.
		Access to Go1 software for external users requires strong authentication mechanisms.
		User access accounts to the network infrastructure and systems holding customer data are assigned to individual users.
		Privileged access to sensitive resources is restricted to authorized administrators.
		HTTPS is used to encrypt network traffic between Azure Kubernetes and secure company devices.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
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	The security policies set out the requirements for managing information security across Go1's operations.
		An assessment of functional roles and system access privileges has been completed to identify the requirements for segregation of duties.

CC6.0	Criteria	Control Activity
	administered by the entity, user system credentials are removed when user access is no longer authorized.	New user access privileges to critical systems are approved by management prior to provisioning.
		A defined terminations process is followed including revocation of user access from systems in a timely manner.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
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, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Segregation of duties is maintained between the development and operations teams.
		The security policies set out the requirements for managing information security across Go1's operations.
		Privileged access to sensitive resources is restricted to authorized administrators.
		An assessment of functional roles and system access privileges has been completed to identify the requirements for segregation of duties.
		A defined terminations process is followed including revocation of user access from systems in a timely manner.
		User access reviews are performed at least quarterly to confirm Go1user access to critical systems is appropriate.
		User access is based on the concept of least privilege to restrict access to only where there is a legitimate business need.
		Administrator account use is logged for retrospective investigation if required.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.

CC6.0	Criteria	Control Activity
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.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
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.	Defined processes are in place to ensure terminated employees have returned or otherwise destroyed any confidential data.
		The security policies set out the requirements for managing information security across Go1's operations.
		The defined data disposal guidelines and requirements set out the process for ensuring data is erased prior to disposal of system assets.
		A defined terminations process is followed including revocation of user access from systems in a timely manner.
		User access reviews are performed at least quarterly to confirm Go1user access to critical systems is appropriate.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The security policies set out the requirements for managing information security across Go1's operations.
		A vulnerability management program is defined and documented to assess and manage the technical security of Go1's systems including identification, prioritization, and resolution of vulnerabilities.
		Go1 end user devices hard disks are encrypted to prevent unauthorized access to sensitive information.
		Azure Kubernetes encryption process is followed to ensure HTTPS was used to encrypt network traffic and secure company devices.

CC6.0	Criteria	Control Activity
		The authorized WI-FI networks are encrypted, and password protected to prevent unauthorized access.
		Vulnerability scans are performed at least bi-weekly. Vulnerabilities identified are addressed in line with the identified severity ratings.
		Independent penetration testing is conducted annually. Vulnerabilities identified are addressed in line with the identified severity ratings.
		Firewalls are used at external points of connectivity to the infrastructure and network.
		Web application firewalls are used to protect Go1's web applications from unauthorized activity.
		Azure managed platform keys are used to deploy and rotate encryption keys automatically for encryption at rest.
		Encryption keys are secured to limit access to authorized administrators with access logging.
		Systematically applied security restrictions are used to protect against malicious software and data leakage.
		The acceptable use policies include device hardening and data loss prevention requirements.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
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.	The security policies set out the requirements for managing information security across Go1's operations.
		Firewalls are used at external points of connectivity to the infrastructure and network.
		Data at rest in the production database(s) is automatically encrypted.
		Data in transit to the infrastructure is automatically encrypted.
		Systematically applied security restrictions are used to protect against malicious software and data leakage.

CC6.0	Criteria	Control Activity
		The acceptable use policies include device hardening and data loss prevention requirements.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
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.	Incidents reported by external and internal users are logged in a central repository for monitoring through to closure.
		Server hardening and security patching are performed by the cloud provider for Go1's serverless architecture.
		The security policies set out the requirements for managing information security across Go1's operations.
		A vulnerability management program is defined and documented to assess and manage the technical security of Go1's systems including identification, prioritization, and resolution of vulnerabilities.
		Server hardening standards are defined and followed to ensure Go1 managed systems meet good practice security standards.
		Vulnerability scans are performed at least bi-weekly. Vulnerabilities identified are addressed in line with the identified severity ratings.
		Independent penetration testing is conducted annually. Vulnerabilities identified are addressed in line with the identified severity ratings.
		Monitoring of end-point devices is performed to confirm compliance with anti-virus requirements.
		Network security monitoring is performed using network monitoring and threat detection software.
		Anti-virus software is installed to protect Go1 company devices.
		Automatic updates are applied to ensure anti-virus definitions are kept current.

CC6.0	Criteria	Control Activity
		Systematically applied security restrictions are used to protect against malicious software and data leakage.
		The acceptable use policies include device hardening and data loss prevention requirements.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.

Common Criteria 7: System Operations

CC7.0	Criteria	Control Activity
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.	Monitoring tools are used to identify and evaluate system performance capacity, availability, and security-related indicators.
		Incident management processes are defined and followed for identification, assessment, classification, response communications to interested parties and resolution.
		A vulnerability management program is defined and documented to assess and manage the technical security of Go1's systems including identification, prioritization, and resolution of vulnerabilities.
		Risk assessments are conducted at least annually for the inventory of system assets to identify risks and actions required to mitigate those risks.
		Vulnerability scans are performed at least bi-weekly. Vulnerabilities identified are addressed in line with the identified severity ratings.
		Independent penetration testing is conducted annually. Vulnerabilities identified are addressed in line with the identified severity ratings.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
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.	Incidents reported by external and internal users are logged in a central repository for monitoring through to closure.
		The incident management policies and procedures document the approach to identifying, reporting, evaluating, classifying, and handling incidents.
		Incident management processes are defined and followed for identification assessment, classification, response communications to interested parties and resolution.

CC7.0	Criteria	Control Activity
		Risk assessments are conducted at least annually for the inventory of system assets to identify risks and actions required to mitigate those risks.
		Network security monitoring is performed using network monitoring and threat detection software.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
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.	The risk assessments include consideration of risks related to information security, compliance requirements and third-party dependencies.
		Security related change requirements based on vulnerabilities, security, risk mitigation requirements or other ongoing improvements have defined criteria to determine their relative priority or timeline for remediation.
		Incidents reported by external and internal users are logged in a central repository for monitoring through to closure.
		The incident management policies and procedures document the approach to identifying, reporting, evaluating, classifying, and handling incidents.
		Incident response plans are defined to provide guidelines for responding to major incidents including security breaches.
		Root cause analysis is conducted on high severity incidents to determine lessons learned and updates required to the incident response plans, as well as raise change requests for permanent fixes to prevent recurrence.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program	Incidents reported by external and internal users are logged in a central repository for monitoring through to closure.

CC7.0	Criteria	Control Activity
	to understand, contain, remediate, and communicate security incidents, as appropriate.	The incident management policies and procedures document the approach to identifying, reporting, evaluating, classifying, and handling incidents.
		Incident response plans are defined to provide guidelines for responding to major incidents including security breaches.
		The established emergency response team is defined to respond to major adverse events in a timely manner.
		The incident response plans are reviewed and updated at least annually to ensure they remain current and effective.
		Root cause analysis is conducted on high severity incidents to determine lessons learned and updates required to the incident response plans, as well as raise change requests for permanent fixes to prevent recurrence.
		The business continuity plans document the disruptive scenarios, response plans, roles and responsibilities, key internal and external stakeholders, escalation procedures, communication channels to effectively manage critical events.
		The business continuity plan is tested at least annually to ensure the response plans to critical events are effective.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Incidents reported by external and internal users are logged in a central repository for monitoring through to closure.
		The incident management policies and procedures document the approach to identifying, reporting, evaluating, classifying, and handling incidents.
		The established emergency response team is defined to respond to major adverse events in a timely manner.

CC7.0	Criteria	Control Activity
		The incident response plans are reviewed and updated at least annually to ensure they remain current and effective.
		The disaster recovery plan is tested at least annually to confirm that recovery procedures are effective.
		The disaster recovery plan includes defined procedures to recover from significant events and is reviewed and updated at least annually.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.

Common Criteria 8: Change Management

CC8.0	Criteria	Control Activity
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.	Version control software is used to track changes to the source code and provide rollback capability if required.
		Continuous integration continuous deployment (CI/CD) solution is used to configure key checks and conditions to be met prior to change release.
		System change requests are documented and tracked in a ticketing system.
		Documented change control policies and procedures are in place to guide personnel in the change management process.
		Development and test environments are logically separated from the production environment.
		Access to the source code is restricted to authorized developers.
		Changes to the infrastructure configurations are managed as code to ensure the changes follow the formal change management process.
		Code developments require a system enforced peer review prior to merging with the master code branch.
		Change releases require a system enforced review and approval prior to deployment.
		Impact assessments are performed prior to deployment of changes to ensure users of the system are not adversely impacted.
		Segregation of duties is maintained between the development and operations teams.
		System changes are tested based on the type of change prior to implementation.
		Static code analysis tools are used to scan and identify vulnerabilities in the source code.

CC8.0	Criteria	Control Activity
		Security related change requirements based on vulnerabilities, security, risk mitigation requirements or other ongoing improvements have defined criteria to determine their relative priority or timeline for remediation.
		Changes are assessed to determine whether communications to users of the system are required and are performed accordingly.
		Release notes for changes are sent to internal and external stakeholders.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.

Common Criteria 9: Risk Mitigation

CC9.0	Criteria	Control Activity
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Management considers interactions with, and the need to monitor the activities of third parties when documenting the organizational chart and defining job descriptions.
		Go1 has purchased insurance to offset or compensate for the financial loss of an adverse event with the services.
		The business continuity plans document the disruptive scenarios, response plans, roles and responsibilities, key internal and external stakeholders, escalation procedures, communication channels to effectively manage critical events.
		The business continuity plan is tested at least annually to ensure the response plans to critical events are effective.
		The disaster recovery plan is tested at least annually to confirm that recovery procedures are effective.
		The disaster recovery plan includes defined procedures to recover from significant events and is reviewed and updated at least annually.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The risk assessments include consideration of risks related to information security, compliance requirements and third-party dependencies.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.
		Management has defined a third-party vendor risk management approach for evaluating third-party risks.
		A formal risk assessment is completed for each new vendor prior to commencing the services provided.
		The third-party vendor register includes a listing of material vendors for tracking and monitoring.
		New third-party vendors are approved by management prior to selection and onboarding.

CC9.0	Criteria	Control Activity
		The entity's third-party agreements outline and communicate: the scope of services, roles and responsibilities, terms of the business relationship, communication protocols, compliance requirements, service levels, and just cause for terminating the relationship.
		An annual vendor risk assessment is completed to ensure the identification and treatment of risks remains accurate and appropriate.
		Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.
		Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.
		Management has assigned responsibility and accountability for the management of risks and governance associated with third parties to appropriate personnel.
		The entity has documented procedures for terminating third-party relationships.

Trust Services Criteria for the Availability Category

A1.0	Criteria	Control Activity
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Monitoring tools are used to identify and evaluate system performance capacity, availability, and security-related indicators.
		A load balancer is used to automatically distribute traffic across multiple availability zones.
		Preventive services are used to prepare for and protect against attacks that may compromise availability of the service.
		Processing capacity is configured to auto-scale to meet processing demand.
		The system is designed with multiple availability zones and redundancy to support continued availability in the event of a failure.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	A load balancer is used to automatically distribute traffic across multiple availability zones.
		The operations security policy establishes the requirements for backups and recoverability.
		Backups of the application and database are performed daily.
		The system is designed with multiple availability zones and redundancy to support continued availability in the event of a failure.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The disaster recovery plan is tested at least annually to confirm that recovery procedures are effective.
		The disaster recovery plan includes defined procedures to recover from significant events and is reviewed and updated at least annually.
		Backup and restoration tests are performed on at least an annual basis to ensure the recovery controls are effective.

A1.0	Criteria	Control Activity
		When a backup job fails the backup tool sends an alert to the backup administrators who investigate and resolve the failure.

Trust Services Criteria for the Confidentiality Category

C1.0	Criteria	Control Activity
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Defined processes are in place to ensure terminated employees have returned or otherwise destroyed any confidential data.
		The requirements for managing data are established in the data classification, handling, retention, and disposal policies.
		The entities third-party agreements include requirements for protecting confidential data.
		The acceptable use policy sets out the requirements of employees to ensure confidential data is handled appropriately.
		Documented confidential policies and procedures are in place that consider and set the requirements for how data is managed effectively to protect confidentiality.
		Guidance is provided to end users of the system in relation to the requirements for protecting confidential data while using the system.
		The types of confidential data collected and processed have been identified and classified.
		A register of the types and sources of confidential data collected and processed is maintained to track assets and storage locations of confidential data.
		Confidential data is maintained within the system boundaries at times where security controls are applied to restrict access to authorized individuals.
		The risk assessment has identified how confidential data may be leaked outside the boundaries of the system to ensure appropriate protections are in place.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	The defined data disposal guidelines and requirements set out the process for ensuring data is erased prior to disposal of system assets.
		The retention period of confidential data is classified based on the purpose and type of data and location the data is stored.

C1.0	Criteria	Control Activity
		Confidential information is protected from erasure or destruction during the specified retention period by following defined processes.

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

AssuranceLab's examination of the controls of Go1 was limited to the related Agreed Criteria and control activities specified by the management of Go1 and did not encompass all aspects of Go1's operations or operations at user entities. Our examination was performed in accordance with AT-C section 105: Concepts Common to All Attestation Engagements and AT-C section 205: Assertion-Based Examination Engagements.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the Agreed Criteria
- Understand the infrastructure, software, procedures, and data that are designed, implemented, and operated by the service organization
- Determine whether the Agreed Criteria are relevant to the user entity's assertions
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the Agreed Criteria

assurancelab