

**Independent Assurance Report on
Go1 Pty. Ltd.'s Description of its System and on
the Suitability of the Design and Operating
Effectiveness of its Controls Relevant to the
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

CONTENTS

SECTION I – ASSERTION OF GO1 PTY. LTD. MANAGEMENT	3
SECTION II – INDEPENDENT SERVICE AUDITOR'S REPORT	6
SECTION III – GO1 PTY. LTD.'S DESCRIPTION OF ITS SYSTEM	11
OVERVIEW OF OPERATIONS.....	12
<i>Company Background</i>	12
<i>Description of Services Provided</i>	12
<i>Principal Service Commitments and System Requirements</i>	12
<i>Components of the System</i>	13
<i>Processes, Policies and Procedures</i>	15
<i>Boundaries of the System</i>	17
RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING.....	18
<i>Control Environment</i>	18
<i>Risk Assessment Process</i>	19
<i>Information and Communications Systems</i>	19
<i>Monitoring Controls</i>	20
<i>Changes to the System in the Last 12 Months</i>	20
<i>Incidents in the Last 12 Months</i>	20
<i>Criteria Not Applicable to the System</i>	20
COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS.....	21
<i>Subservice Description of Services</i>	21
<i>Complementary Subservice Organization Controls</i>	21
COMPLEMENTARY USER ENTITY CONTROLS.....	24
SOC 2 TRUST SERVICES CRITERIA.....	25
<i>Trust Services Categories Selected by Go1</i>	25
SECTION IV – CRITERIA AND RELATED CONTROLS	26
SOC 2 TRUST SERVICES CRITERIA.....	27
<i>Trust Services Criteria for the Security Category</i>	27
<i>Trust Services Criteria for the Availability Category</i>	85
<i>Trust Services Criteria for the Confidentiality Category</i>	88
GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR.....	91
SECTION V – OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION	92
MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS.....	93

**SECTION I –
ASSERTION OF GO1 PTY. LTD.
MANAGEMENT**

ASSERTION OF GO1 PTY. LTD. MANAGEMENT

18th June 2024

We have prepared the accompanying description of Go1 Pty. Ltd.'s ('Go1') Go1 Premium 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 Premium 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, implemented, and operated 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 throughout the period 01 February 2024 to 30 April 2024, in accordance with the Description Criteria;
- b. the controls stated in the Description were suitably designed throughout the period 01 February 2024 to 30 April 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 throughout that period, and if complementary subservice

- organization controls and complementary user entity controls assumed in the design of Go1's controls operated effectively throughout that period; and
- c. the controls stated in the Description operated effectively throughout the period 01 February 2024 to 30 April 2024, to provide reasonable assurance that Go1's service commitments and system requirements were achieved based on the Agreed Criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Go1's controls operated effectively throughout that period.

DocuSigned by:
Kyle Jackson
6898F9D36BBE462...

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 Go1 Premium 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 Premium 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, implemented, and operated 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.

The information in the accompanying "Section V - Other Information Provided by the Service Organization" is presented by management of Go1 to provide additional information and is not part of Go1's Description. Such information has not been subjected to the procedures applied in our examination and, accordingly we express no opinion on it.

Service Organization's Responsibilities

Go1 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 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 and operating effectiveness 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 and operating effectiveness 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.
- The controls stated in the Description were operating effectively throughout the period to provide reasonable assurance that Go1's service commitments and system requirements were achieved based on the Agreed Criteria.

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 and operating effectiveness 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.
- Testing the operating effectiveness of controls stated in the Description to provide reasonable assurance that Go1 achieved its service commitments and system requirements based on the 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 throughout the period 01 February 2024 to 30 April 2024 in accordance with the Description Criteria;
- 2) the controls stated in the Description were suitably designed throughout the period 01 February 2024 to 30 April 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 throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Go1's controls throughout that period; and
- 3) the controls stated in the Description operated effectively throughout the period 01 February 2024 to 30 April 2024, to provide reasonable assurance that Go1's service commitments and system requirements were achieved based on the Agreed Criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Go1's controls operated effectively throughout that period.

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.

AssuranceLab CPAs LLC

AssuranceLab CPAs LLC
Austin, Texas
United States
18th June 2024

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

OVERVIEW OF OPERATIONS

Company Background

Go1 Pty. Ltd. ('Go1') was founded in 2015 with the objective of developing 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 Premium 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
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.
Cloudflare	Network Services	DNS, load balancing, DDOS protection, web firewall and TLS encryption.
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.
Microsoft Sentinel	A cloud-native security information and event manager (SIEM).
Okta	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.
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 and Microsoft Intune	Mobile device management software used to track and manage security policies on endpoint devices.

Software	Purpose
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.
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 600 people who 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 supports 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 ('Azure'). There are no trusted local office networks. As such, Microsoft Azure ('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 is 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.

Microsoft Azure hosts Go1's critical infrastructure and data 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 and GitLab CI/CD 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 and 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 Premium 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.

Management's Philosophy and Operating Style

Go1's management philosophy and operating style is purpose-driven, risk-based approaches 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 they 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 the 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 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 re-enforce 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 period.

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 period.

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 can 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.

Subservice Organization – Microsoft Azure		
Category	Criteria	Control
		Data center Management team maintains and tests data center-managed environmental equipment within the facility according to documented policy and maintenance procedures.
		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.

User entities are responsible for:

- Understanding and complying with Go1's terms of service.
- Administering their users' access rights, including approval, removal, and periodic review to ensure access is appropriate.
- Ensuring multi-factor authentication is applied by personnel, if required.
- Performing any required risk assessments and approvals when using pre-built integrations available with Go1's services.
- Performing any required risk assessments and approvals for using Go1's open application programming interface (API) and notifying Go1 of any identified vulnerabilities, security breaches or system failures when using the APIs.
- Ensuring the supervision, management, and control of the use of Go1's services by their personnel.
- Developing their own disaster recovery and business continuity plans that address the inability to access or utilize Go1 services for any critical reliance on these services.

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	Test Applied by the Service Auditor	Test Results
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.	Inspected the code of conduct to determine that the code of conduct was documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Disciplinary procedures define the consequences and method of handling misconduct.	Inspected the disciplinary procedure to determine that disciplinary procedures defined the consequences and method of handling misconduct.	No exceptions noted.
		Defined processes are in place for employees to report unethical behavior in a confidential manner.	Inspected the whistleblower policy to determine that defined processes were in place for employees to report unethical behavior in a confidential manner.	No exceptions noted.
		The code of conduct is signed off by new hires upon commencement of their role.	Inspected the code of conduct acknowledgement for a sample of new hires to determine that the code of conduct was signed off by new hires upon commencement of their role.	No exceptions noted.
		Background checks are completed for candidates prior to employment.	Inquired with the Director of Information Security to determine that background checks were required to be completed for candidates prior to employment.	No exceptions noted.

CC1.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
			Inspected the background checks for a sample of new hires to determine that background checks were completed for candidates prior to employment.	Testing of the control activity disclosed that background checks were not completed prior to employment for 2 out of 5 new hire samples tested.
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.	Inspected the organizational chart to determine that Go1 operated independent layers of management between the board of directors, senior management, and operational management.	No exceptions noted.
		Board of directors meetings are held at least annually for organizational oversight and governance.	Inspected the meeting minutes for a sample board meeting to determine that board of directors' meetings were held at least annually for organizational oversight and governance.	No exceptions noted.
		The board of directors meetings sets out the responsibilities and scope of the board of directors.	Inspected the board of directors meeting minutes to determine that Go1 board of directors meetings were held.	No exceptions noted.
		The board is responsible for oversight of the systems and data security of Go1 with review at least annually.	Inspected the audit committee meeting agenda to determine that the board was responsible for oversight of the systems and data security of Go1 with review at least annually.	No exceptions noted.

CC1.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Management reviews are conducted at least annually for oversight and governance of the company and team performance.	Inspected the management review to determine that on at least an annual basis, management reviews were held for oversight and governance of the company and team performance	No exceptions noted.
		The risks and control effectiveness are reported to the board at least annually.	Inspected the audit committee meeting minutes to determine that the risks and control effectiveness were reported to the board at least annually.	No exceptions noted.
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.	Inspected the meeting minutes for a sample management meeting to determine that management meetings were held at least quarterly to review the company operations.	No exceptions noted.
		The organization chart documents the reporting lines accountable executives, and team and individual roles and is updated whenever there are changes in personnel.	Inspected the organizational chart to determine that the organization chart documented the reporting lines, accountable executives, and team and individual roles, and was updated whenever there were changes in personnel.	No exceptions noted.
		Management considers interactions with, and the need to monitor the activities of third parties when documenting the organizational chart and defining job descriptions.	Inspected the organization chart, job descriptions and documented policies to determine that management considered interactions with, and the need to monitor the activities of third parties when documenting the organizational chart and defining job descriptions.	No exceptions noted.

CC1.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Job descriptions are documented for employees and management setting out the responsibilities, role requirements, and any key accountabilities.	Inspected the job description for a sample of current employees to determine that job descriptions were documented for employees and management setting out the responsibilities, role requirements, and any key accountabilities.	No exceptions noted.
		Business planning is performed at least annually to establish business requirements and objectives.	Inspected the information security objectives roadmap and FY24 OKRs to determine that annual business planning was performed to establish business requirements and objectives.	No exceptions noted.
		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.	Inspected the third-party agreements for a sample vendor to determine that the entity's third-party agreements outlined and communicated: 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.	No exceptions noted.
		Upon hire, employees are required to read and acknowledge the acceptable use policy.	Inspected the acceptance of the acceptable use policy for a sample of new hires to determine that upon hire, employees were required to read and acknowledge the acceptable use policy.	No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain	The recruiting department is responsible for attracting individuals with competencies and experience	Inspected the job descriptions for the recruiting department to determine that the recruiting department was responsible for attracting individuals with	No exceptions noted.

CC1.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
	competent individuals in alignment with objectives.	that align with the company goals and objectives.	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.	Inspected the hiring guide to determine that an employee hiring and onboarding process was defined including approval of the new role, vetting of candidates, and ensuring role requirements were met.	No exceptions noted.
		Go1 operates independent layers of management between the board of directors, senior management, and operational management.	Inspected the organizational chart to determine that Go1 operated independent layers of management between the board of directors, senior management, and operational management.	No exceptions noted.
		Management meetings are held at least quarterly to review the company operations.	Inspected the meeting minutes for a sample management meeting to determine that management meetings were held at least quarterly to review the company operations.	No exceptions noted.
		Training of employees follows defined processes of the training requirements and plans to align to the objectives and employee requirements.	Inspected the learning and development policy to determine that training of employees followed defined processes of training requirements and plans to align to the objectives and employee requirements.	No exceptions noted.
		New hire candidates are independently approved prior to selection and onboarding.	Inspected the approval for a sample of new hires to determine that new hire candidates were independently approved prior to selection and onboarding.	No exceptions noted.

CC1.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Background checks are completed for candidates prior to employment.	Inquired with the Director of Information Security to determine that background checks were required to be completed for candidates prior to employment.	No exceptions noted.
			Inspected the background checks for a sample of new hires to determine that background checks were completed for candidates prior to employment.	Testing of the control activity disclosed that background checks were not completed prior to employment for 2 out of 5 new hire samples tested.
		Employee performance reviews are conducted at least annually.	Inspected the performance reviews for a sample of employees to determine that employee performance reviews were conducted at least annually.	No exceptions noted.
		Security awareness training is provided to Go1 employees.	Inspected the security awareness communications to determine that on at least an annual basis, security awareness updates were communicated to employees including the handling of incidents and security related matters.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control	Disciplinary procedures define the consequences and method of handling misconduct.	Inspected the disciplinary procedure to determine that disciplinary procedures defined the consequences and method of handling misconduct.	No exceptions noted.

CC1.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
	responsibilities in the pursuit of objectives.	Defined processes are in place for employees to report unethical behavior in a confidential manner.	Inspected the whistleblower policy to determine that defined processes were in place for employees to report unethical behavior in a confidential manner.	No exceptions noted.
		The organization chart documents the reporting lines accountable executives, and team and individual roles and is updated whenever there are changes in personnel.	Inspected the organizational chart to determine that the organization chart documented the reporting lines, accountable executives, and team and individual roles, and was updated whenever there were changes in personnel.	No exceptions noted.
		Company all-hands meetings are held to communicate significant updates and raise awareness of the security and compliance objectives.	Inspected the meeting presentation documents for a sample company-wide meetings to determine that company-wide meetings were held to communicate company updates, company performance, and system and service changes.	No exceptions noted.
		The documented policies and procedures establish roles, responsibilities, and area accountabilities.	Inspected the information security roles and responsibilities policy to determine that the documented policies and procedures established roles, responsibilities, and area accountabilities.	No exceptions noted.
		Performance measures are defined for each team or functional area to support the company objectives.	Inspected the performance measures to determine that performance measures were defined for each team or functional area to support the company objectives.	No exceptions noted.

CC1.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Executive management has established performance measures, including the incentives and rewards for exceeding expectations, as it relates to teams and functional areas.	Inspected the bonus policy to determine that executive management established performance measures including the incentives and rewards for exceeding expectations, as it relates to teams and functional areas.	No exceptions noted.
		Job descriptions are documented for employees and management setting out the responsibilities, role requirements, and any key accountabilities.	Inspected the job description for a sample of current employees to determine that job descriptions were documented for employees and management setting out the responsibilities, role requirements, and any key accountabilities.	No exceptions noted.
		Employment contracts are formed with employees.	Inspected the employment contract for a sample of new hire to determine that employment contracts were formed with employees.	No exceptions noted.
		Employee performance reviews are conducted at least annually.	Inspected the performance reviews for a sample of new hires to determine that employee performance reviews were conducted at least annually.	No exceptions noted.

Common Criteria 2: Information and Communication

CC2.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
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.	Inspected the company-wide meetings to determine that company-wide meetings were held to communicate company updates, company performance, and system and service changes.	No exceptions noted.
		Organizational and information policies and procedures are made available to employees through the intranet.	Inspected intranet to determine that organizational and information policies and procedures were made available to employees through the intranet.	No exceptions noted.
		Information logs are maintained to track events metrics and indicators to support the processes and internal control requirements.	Inspected the information logs to determine that central logs were maintained to track events metrics and indicators to support the processes and internal control requirements.	No exceptions noted.
		Go1 have documented the systems and data flows to identify and document the relevant internal and external information sources of the system.	Inspected the data flow documentation to determine that Go1 had a documented data flow diagram to identify and document the relevant internal and external information sources of the system.	No exceptions noted.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and	Management meetings are held at least quarterly to review the company operations.	Inspected the meeting minutes for a sample management meeting to determine that management meetings were held at least quarterly to review the company operations.	No exceptions noted.

CC2.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
	responsibilities for internal control, necessary to support the functioning of internal control.	The responsibilities for information security and privacy are established documented and communicated to Go1 employees.	Inspected the defined responsibilities for information security to determine that the responsibilities for information security and privacy were established, documented and communicated to Go1 employees.	No exceptions noted.
		The requirements for managing data are established in the data management policy.	Inspected the data management policy to determine that the requirements for managing data were established in the data management policy.	No exceptions noted.
		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.	Inspected the company objectives to determine that the defined company objectives included a mix of strategic, financial, and operational level objectives that guided functional areas and teams on how they supported the company objectives and identified the risks that threaten achievement of the objectives.	No exceptions noted.
		The company objectives are communicated to employees for awareness.	Inspected the communication of company objectives to determine that the company objectives were communicated to employees through the intranet.	No exceptions noted.
		The information security policy sets out the roles, responsibilities, and requirements to maintain the security of systems data and endpoint devices.	Inspected the information security policy to determine that the acceptable use section set out the roles, responsibilities, and requirements to maintain the security of systems, data and endpoint devices.	No exceptions noted.

CC2.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Organizational and information policies and procedures are made available to employees through the intranet.	Inspected intranet to determine that organizational and information policies and procedures were made available to employees through the intranet.	No exceptions noted.
		On at least an annual basis security awareness updates are communicated to employees including the handling of incidents and security related matters.	Inspected the security awareness communications to determine that on at least an annual basis, security awareness updates were communicated to employees including the handling of incidents and security related matters.	No exceptions noted.
		The code of conduct is signed off by new hires upon commencement of their role.	Inspected the code of conduct acknowledgement for a sample of new hires to determine that the code of conduct was signed off by new hires upon commencement of their role.	No exceptions noted.
		Security awareness training is provided to Go1 employees.	Inspected the security awareness communications to determine that on at least an annual basis, security awareness updates were communicated to employees including the handling of incidents and security related matters.	No exceptions noted.
		Changes are assessed to determine whether communications to users of the system are required and are performed accordingly.	Inspected the assessment of communication requirements for a sample of changes to determine that changes were assessed to determine whether communications to users of the system were required.	Descoped

CC2.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Release notes for changes are sent to internal and external stakeholders, as applicable.	Inspected the release notes for a sample of change releases to determine that release notes for changes were sent to internal and external stakeholders, as applicable.	No exceptions noted.
		On at least an annual basis, or when changes are made, employees are required to read and acknowledge the information security policies and procedures.	Inspected the documented acceptance of the security policy of current employees to determine that on at least an annual basis, or when changes were made, employees were required to read and acknowledge the information security policies and procedures.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Management has assigned responsibility and accountability for the management of risks and governance associated with third parties to appropriate personnel.	Inspected the assigned responsibilities for third-party vendors to determine that management had assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.	No exceptions noted.
		Users of the system are provided mechanisms for reporting any requests incidents, failures, or security-related matters.	Inspected the Go1 Help Centre to determine that users of the system were provided dedicated customer support for reporting any requests, incidents, failures, or security related matters.	No exceptions noted.
		Changes to commitments, requirements, and responsibilities are communicated to third parties by the appointed account manager(s).	Inspected the appointed account manager(s) for a sample of customers to determine that there were clear responsibilities for communicating any changes to agreements, services or other operating changes that may impact customers.	No exceptions noted.

CC2.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Documentation is provided to users to guide them on the operation of the system.	Inspected the Go1 Help Center to determine that documentation was provided to users to guide them on the operation of the system.	No exceptions noted.
		Customer administrators are provided with training on how to administer the system and perform their responsibilities.	Inspected the Go1 Help Center to determine that customer administrators were provided with training on how to administer the system and perform their responsibilities.	No exceptions noted.
		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.	Inspected the third-party agreements for a sample vendor to determine that the entity's third-party agreements outlined and communicated: 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.	No exceptions noted.
		Changes are assessed to determine whether communications to users of the system are required and are performed accordingly.	Inspected the assessment of communication requirements for a sample of changes to determine whether communications to users of the system were required.	Descoped
		Release notes for changes are sent to internal and external stakeholders, as applicable.	Inspected the release notes for a sample of change releases to determine that release notes for changes were sent to internal and external stakeholders, as applicable.	No exceptions noted.

CC2.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Awareness of how to report incidents, failures, and any security related matters is supported through user communications.	Inspected the Go1 User Terms and Policies to determine that awareness of how to report incidents, failures and any security related matters was supported through how-to guides and dedicated support contacts.	No exceptions noted.
		Customer commitments, requirements, and responsibilities are outlined and communicated through formal service terms.	Inspected the agreements for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.

Common Criteria 3: Risk Assessment

CC3.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
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.	Inspected the performance measures to determine that performance measures were defined for each team or functional area to support the company objectives.	No exceptions noted.
		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.	Inspected the company objectives to determine that the defined company objectives included a mix of strategic, financial, and operational level objectives that guided functional areas and teams on how they supported the company objectives and identified the risks that threaten achievement of the objectives.	No exceptions noted.
		The company objectives are communicated to employees for awareness.	Inspected the communication of company objectives to determine that the company objectives were communicated to employees through the intranet.	No exceptions noted.
		The company objectives are used as a basis for identifying and assessing risks.	Inspected the risk management policy to determine that the company objectives were used as a basis for identifying and assessing risks.	No exceptions noted.
		The control framework is based on a recognized industry standard.	Inspected the control framework to determine that the control framework was based on a recognized industry standard.	No exceptions noted.

CC3.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Business planning is performed at least annually to establish business requirements and objectives.	Inspected the information security objectives roadmap and FY24 OKRs to determine that annual business planning was performed to establish business requirements and objectives.	No exceptions noted.
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.	Inspected the risk register to determine that the risk register was used to track and monitor the identified risks including risk owners, risk ratings, and planned actions and mitigations.	No exceptions noted.
		The company objectives are used as a basis for identifying and assessing risks.	Inspected the risk management policy to determine that the company objectives were used as a basis for identifying and assessing risks.	No exceptions noted.
		Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the risk management policy, risk assessment and risk treatment process to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.
		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.	Inspected the risk assessment criteria to determine that management had defined risk assessment criteria with scales and guidance on how to measure and classify risks and provided a common language for comparing and prioritizing risks.	No exceptions noted.

CC3.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Management has defined a third-party vendor risk management approach for evaluating third-party risks.	Inspected the third-party management policy to determine that management had defined a third-party vendor risk management approach for evaluating third-party risks.	No exceptions noted.
		An annual vendor risk assessment is completed to ensure the identification and treatment of risks remains accurate and appropriate.	Inspected the vendor register to determine that an annual vendor risk assessment was completed to ensure the identification and treatment of risks remains accurate and appropriate.	No exceptions noted.
		Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the vendor security and security review policy to determine that management developed third-party risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		Risk assessments are conducted at least annually for the inventory of system assets to identify risks and actions required to mitigate those risks.	Inspected the cluster security risk assessment to determine that risk assessments were conducted at least annually for the inventory of system assets to identify risks and actions required to mitigate those risks.	No exceptions noted.
		Risk assessments are completed at least annually to identify and analyze the risks and identify any required mitigation actions.	Inspected the risk assessment to determine that risk assessments were completed to identify and analyze the risks and identified any required mitigation actions.	No exceptions noted.

CC3.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		The risk assessments include consideration of risks related to information security compliance requirements and third-party dependencies.	Inspected the risk register to determine that risk assessments included consideration of risks related to compliance requirements and third-party dependencies.	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected risk register to determine that the identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk register to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		A formal risk assessment is completed for each new vendor prior to commencing the services provided.	Inspected the risk assessment for a sample of new vendors to determine that a formal risk assessment was completed for each new vendor prior to commencing the services provided.	No exceptions noted.
		As part of the risk assessment process controls within the environment are modified and implemented to mitigate the identified risks.	Inspected the risk register to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate the identified risks.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the	The risk register is used to track and monitor the identified risks, ratings, mitigation practices and planned actions.	Inspected the risk register to determine that the risk register was used to track and monitor the identified risks including risk owners, risk ratings, and planned actions and mitigations.	No exceptions noted.

CC3.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
	achievement of objectives.	The risk assessment process considers the potential for fraud including malicious acts of employees or other users of the system.	Inspected the risk register to determine that the risk assessment process considered the potential for fraud including malicious acts of employees or other users of the system.	No exceptions noted.
		The risk assessments include consideration of risks related to information security compliance requirements and third-party dependencies.	Inspected the risk register to determine that risk assessments included consideration of risks related to compliance requirements and third-party dependencies.	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk register to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
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.	Inspected the risk register to determine that the risk register was used to track and monitor the identified risks including risk owners, risk ratings, and planned actions and mitigations.	No exceptions noted.
		Management has assigned responsibility and accountability for the management of risks and governance associated with third parties to appropriate personnel.	Inspected the assigned responsibilities for third-party vendors to determine that management had assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.	No exceptions noted.

CC3.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		The risk assessments include consideration of risks related to information security compliance requirements and third-party dependencies.	Inspected the risk register to determine that risk assessments included consideration of risks related to compliance requirements and third-party dependencies.	No exceptions noted.
		The risk assessment process identifies and assesses changes that could significantly impact the system of internal control.	Inspected the risk register to determine that the risk assessment process identified and assessed changes that could significantly impact the system of internal control.	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk register to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.

Common Criteria 4: Monitoring Activities

CC4.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
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.	Inspected the risk register to determine that the risk register was used to track and monitor the identified risks including risk owners, risk ratings, and planned actions and mitigations.	No exceptions noted.
		Management is assigned ownership of ongoing monitoring of the effectiveness of controls and that key policy and process requirements are being adhered to.	Inspected the assigned responsibilities to determine that management were assigned ownership of ongoing monitoring of the effectiveness of controls and that key policy and process requirements were being adhered to.	No exceptions noted.
		Key policies and processes are reviewed and updated at least annually to confirm their effectiveness accuracy and compliance.	Inspected the revision history of policy documents to determine that key policies and processes were reviewed and updated at least annually to confirm their effectiveness and accuracy.	No exceptions noted.
		An annual vendor risk assessment is completed to ensure the identification and treatment of risks remains accurate and appropriate.	Inspected the vendor register to determine that an annual vendor risk assessment was completed to ensure the identification and treatment of risks remains accurate and appropriate.	No exceptions noted.
		Backup and restoration tests are performed on at least an annual basis to ensure the recovery controls are effective.	Inspected the backup restoration test to determine that backup and restoration tests were performed on at least an annual basis to ensure the recovery controls were effective.	No exceptions noted.

CC4.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		The control framework is based on a recognized good practice industry standard.	Inspected the control framework to determine that the control framework was based on a recognized industry standard.	No exceptions noted.
		The key control activities are individually assigned to owners responsible for ensuring effective and consistent performance of the controls.	Inspected the control framework to determine that the key control activities were individually assigned to owners responsible for ensuring effective and consistent performance of the controls.	No exceptions noted.
		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.	Inspected the review of third-party attestation reports for a sample of material third-party vendors to determine that management obtained and reviewed attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
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	Board of directors meetings are held at least annually for organizational oversight and governance.	Inspected the meeting minutes for a sample board meeting to determine that board of directors' meetings were held at least annually for organizational oversight and governance.	No exceptions noted.
		The board of directors meetings sets out the responsibilities and scope of the board of directors.	Inspected the board of directors meeting minutes to determine that Go1 board of directors meetings were held.	No exceptions noted.

CC4.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
	management and the board of directors, as appropriate.	Management is assigned ownership of ongoing monitoring of the effectiveness of controls and that key policy and process requirements are being adhered to.	Inspected the assigned responsibilities to determine that management were assigned ownership of ongoing monitoring of the effectiveness of controls and that key policy and process requirements were being adhered to.	No exceptions noted.
		Key policies and processes are reviewed and updated at least annually to confirm their effectiveness accuracy and compliance.	Inspected the revision history of policy documents to determine that key policies and processes were reviewed and updated at least annually to confirm their effectiveness and accuracy.	No exceptions noted.
		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.	Inspected the tracking of vulnerabilities, deviations, and control gaps to determine that management tracked whether control failures, breaches of policies and procedures, customer complaints and other issues were assessed, tracked, and monitored through to resolution, as applicable.	No exceptions noted.
		The third-party vendor register includes a listing of material vendors for tracking and monitoring.	Inspected the third-party vendor register to determine that the third-party vendor register included a listing of material vendors for tracking and monitoring.	No exceptions noted.
		Management has assigned responsibility and accountability for the management of risks and governance associated with third parties to appropriate personnel.	Inspected the assigned responsibilities for third-party vendors to determine that management had assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.	No exceptions noted.

CC4.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		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.	Inspected the operations security policy to determine that security related change requirements based on vulnerabilities, security risk mitigation requirements, or other ongoing improvements had defined criteria to determine their relative priority or timeline for remediation.	No exceptions noted.
		The control framework is based on a recognized industry standard.	Inspected the control framework to determine that the control framework was based on a recognized industry standard.	No exceptions noted.
		The key control activities are individually assigned to owners responsible for ensuring effective and consistent performance of the controls.	Inspected the control framework to determine that the key control activities were individually assigned to owners responsible for ensuring effective and consistent performance of the controls.	No exceptions noted.
		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.	Inspected the annual review of the control framework to determine that the control framework was reviewed at least annually by the control owners to ensure the control descriptions and owners were accurate, and that the controls were operating effectively as described.	No exceptions noted.
		The risks and control effectiveness are reported to the board at least annually.	Inspected the audit committee meeting minutes to determine that the risks and control effectiveness were reported to the board at least annually.	No exceptions noted.

CC4.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		<p>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.</p>	<p>Inspected the review of third-party attestation reports for a sample of material third-party vendors to determine that management obtained and reviewed attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.</p>	<p>No exceptions noted.</p>
		<p>As part of the risk assessment process controls within the environment are modified and implemented to mitigate the identified risks.</p>	<p>Inspected the risk register to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate the identified risks.</p>	<p>No exceptions noted.</p>

Common Criteria 5: Control Activities

CC5.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
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.	Inspected the risk register to determine that the risk register was used to track and monitor the identified risks including risk owners, risk ratings, and planned actions and mitigations.	No exceptions noted.
		The control framework identifies and documents the key control activities to support the defined objectives, regulations, and compliance requirements.	Inspected the control framework to determine that the control framework identified and documented the key control activities to support the defined objectives, regulations, and compliance requirements.	No exceptions noted.
		The control framework is based on a recognized industry standard.	Inspected the control framework to determine that the control framework was based on a recognized industry standard.	No exceptions noted.
		An assessment of functional roles and system access privileges has been completed to identify the requirements for segregation of duties.	Inspected the assessment of functional roles to determine that an assessment of functional roles and system access privileges was completed to identify the requirements for segregation of duties.	No exceptions noted.
		The key control activities are individually assigned to owners responsible for ensuring effective and consistent performance of the controls.	Inspected the control framework to determine that the key control activities were individually assigned to owners responsible for ensuring effective and consistent performance of the controls.	No exceptions noted.

CC5.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		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.	Inspected the annual review of the control framework to determine that the control framework was reviewed at least annually by the control owners to ensure the control descriptions and owners were accurate, and that the controls were operating effectively as described.	No exceptions noted.
		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.	Inspected the business continuity plans to determine that the business continuity plans documented the disruptive scenarios, response plans, roles and responsibilities, key internal and external stakeholders, escalation procedures, communication channels to effectively manage critical events.	No exceptions noted.
		The business continuity plan is tested at least annually to ensure the response plans to critical events are effective.	Inspected the business continuity plan testing to determine that the business continuity plan was tested at least annually to ensure the response plans to critical events were effective.	No exceptions noted.
		Risk assessments are completed at least annually to identify and analyze the risks and identify any required mitigation actions.	Inspected the risk assessment to determine that risk assessments were completed to identify and analyze the risks and identified any required mitigation actions.	No exceptions noted.
		The risk assessments include consideration of risks related to information security compliance requirements and third-party dependencies.	Inspected the risk register to determine that risk assessments included consideration of risks related to compliance requirements and third-party dependencies.	No exceptions noted.

CC5.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk register to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		As part of the risk assessment process controls within the environment are modified and implemented to mitigate the identified risks.	Inspected the risk register to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate the identified risks.	No exceptions noted.
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.	Inspected the results of the disaster recovery tests to determine that the disaster recovery plan was tested at least annually to confirm that recovery procedures were effective.	No exceptions noted.
		The disaster recovery plan includes defined procedures to recover from significant events and is reviewed and updated at least annually.	Inspected the disaster recovery plan to determine that the disaster recovery plan included defined procedures to recover from significant events and was reviewed and updated at least annually.	No exceptions noted.
		Backup and restoration tests are performed on at least an annual basis to ensure the recovery controls are effective.	Inspected the backup restoration test to determine that backup and restoration tests were performed on at least an annual basis to ensure the recovery controls were effective.	No exceptions noted.

CC5.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		The control framework identifies and documents the key control activities to support the defined objectives, regulations, and compliance requirements.	Inspected the control framework to determine that the control framework identified and documented the key control activities to support the defined objectives, regulations, and compliance requirements.	No exceptions noted.
		The control framework is based on a recognized good practice industry standard.	Inspected the control framework to determine that the control framework was based on a recognized good practice industry standard.	No exceptions noted.
		The key control activities are individually assigned to owners responsible for ensuring effective and consistent performance of the controls.	Inspected the control framework to determine that the key control activities were individually assigned to owners responsible for ensuring effective and consistent performance of the controls.	No exceptions noted.
		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.	Inspected the annual review of the control framework to determine that the control framework was reviewed at least annually by the control owners to ensure the control descriptions and owners were accurate, and that the controls were operating effectively as described.	No exceptions noted.
		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.	Inspected the business continuity plans to determine that the business continuity plans documented the disruptive scenarios, response plans, roles and responsibilities, key internal and external stakeholders, escalation procedures, communication channels to effectively manage critical events.	No exceptions noted.

CC5.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		The business continuity plan is tested at least annually to ensure the response plans to critical events are effective.	Inspected the business continuity plan testing to determine that the business continuity plan was tested at least annually to ensure the response plans to critical events were effective.	No exceptions noted.
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.	The documented policies and procedures establish roles responsibilities and area accountabilities.	Inspected the information security roles and responsibilities policy to determine that the documented policies and procedures established roles, responsibilities, and area accountabilities.	No exceptions noted.
		Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the risk management policy, risk assessment and risk treatment process to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.
		Key policies and processes are reviewed and updated at least annually to confirm their effectiveness accuracy and compliance.	Inspected the revision history of policy documents to determine that key policies and processes were reviewed and updated at least annually to confirm their effectiveness and accuracy.	No exceptions noted.
		Management has defined a third-party vendor risk management approach for evaluating third-party risks.	Inspected the third-party management policy to determine that management had defined a third-party vendor risk management approach for evaluating third-party risks.	No exceptions noted.

CC5.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		The control framework identifies and documents the key control activities to support the defined objectives, regulations, and compliance requirements.	Inspected the control framework to determine that the control framework identified and documented the key control activities to support the defined objectives, regulations, and compliance requirements.	No exceptions noted.
		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.	Inspected the annual review of the control framework to determine that the control framework was reviewed at least annually by the control owners to ensure the control descriptions and owners were accurate, and that the controls were operating effectively as described.	No exceptions noted.
		The risks and control effectiveness are reported to the board at least annually.	Inspected the audit committee meeting minutes to determine that the risks and control effectiveness were reported to the Board at least annually.	No exceptions noted.
		Job descriptions are documented for employees and management setting out the responsibilities, role requirements, and any key accountabilities.	Inspected the job description for a sample of current employees to determine that job descriptions were documented for employees and management setting out the responsibilities, role requirements, and any key accountabilities.	No exceptions noted.

Common Criteria 6: Logical and Physical Access Controls

CC6.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
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.	The security policies set out the requirements for managing information security across Go1's operations.	Inspected the information security policies to determine that the security policies set out the requirements for Go1's operations.	No exceptions noted.
		The access control policy sets out the required system access controls for secure authentication and account use.	Inspected the access control policy to determine that the access control policy set out the required system access controls for secure authentication and account use.	No exceptions noted.
		Access to the network and infrastructure for Go1 employees requires strong authentication mechanisms.	Inspected the authentication requirements to determine that access to the network and infrastructure for Go1 employees required authentication with strong password requirements.	No exceptions noted.
		Access to Go1 software for Go1 employees requires strong authentication mechanisms.	Inspected the authentication requirements to determine that access to the Go1 software for Go1 employees required authentication with strong authentication mechanisms.	No exceptions noted.
		Access to Go1 software for external users requires strong authentication mechanisms.	Inspected the authentication requirements to determine that access to Go1 for external users required authentication with SSO.	No exceptions noted.
		User access accounts to the network infrastructure and systems holding customer data are assigned to individual users.	Inspected the Okta user listings to determine that user access accounts to the network, infrastructure, and systems holding customer data were assigned to individual users.	No exceptions noted.

CC6.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Privileged access to sensitive resources is restricted to authorized administrators.	Inspected the privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Azure Kubernetes encryption process is followed to ensure HTTPS was used to encrypt network traffic and secure company devices.	Inspected the Azure Kubernetes encryption process to determine that HTTPS was used to encrypt network traffic and secure company devices.	No exceptions noted.
		A password management system is used to ensure quality passwords are applied for user access.	Inspected the password manager to determine that the 1Password password management system was used to ensure quality passwords were applied for user access.	No exceptions noted.
		An inventory of system assets and components is maintained to classify and manage the information assets.	Inspected the inventory of system assets and components to determine an inventory of system assets and components was maintained to classify and manage the information assets.	No exceptions noted.
		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	The security policies set out the requirements for managing information security across Go1's operations.	Inspected the information security policies to determine that the security policies set out the requirements for Go1's operations.	No exceptions noted.

CC6.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
	<p>new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.</p>	<p>An assessment of functional roles and system access privileges has been completed to identify the requirements for segregation of duties.</p>	<p>Inspected the assessment of functional roles to determine that an assessment of functional roles and system access privileges was completed to identify the requirements for segregation of duties.</p>	<p>No exceptions noted.</p>
		<p>New user access privileges to critical systems are approved by management prior to provisioning.</p>	<p>Inspected the access approval for a sample of new employees to determine that new user access privileges to critical systems were approved by management prior to provisioning.</p>	<p>No exceptions noted.</p>
		<p>A defined terminations process is followed including revocation of user access from systems in a timely manner.</p>	<p>Inspected the access removal for a sample of terminated employees to determine that a defined terminations process was followed including revocation of user access from systems in a timely manner.</p>	<p>No exceptions noted.</p>
		<p>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.</p>		
CC6.3	<p>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</p>	<p>Segregation of duties is maintained between the development and operations teams.</p>	<p>Inspected the system access for developers and operations personnel to determine that segregation of duties was maintained between the development and operations teams.</p>	<p>No exceptions noted.</p>
		<p>The security policies set out the requirements for managing information security across Go1's operations.</p>	<p>Inspected the information security policies to determine that the security policies set out the requirements for Go1's operations.</p>	<p>No exceptions noted.</p>

CC6.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
	concepts of least privilege and segregation of duties, to meet the entity's objectives.	Privileged access to sensitive resources is restricted to authorized administrators.	Inspected the privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		An assessment of functional roles and system access privileges has been completed to identify the requirements for segregation of duties.	Inspected the assessment of functional roles to determine that an assessment of functional roles and system access privileges was completed to identify the requirements for segregation of duties.	No exceptions noted.
		User access reviews are performed at least quarterly to confirm Go1 user access to critical systems is appropriate.	Inspected the user access reviews for a sample quarter to determine that user access reviews were performed at least quarterly to confirm Go1's user access to the infrastructure and software was appropriate.	No exceptions noted.
		User access is based on the concept of least privilege to restrict access to only where there is a legitimate business need.	Inspected the access control policy to determine that user access was based on the concept of least privilege to restrict access to only where there was a legitimate business need.	No exceptions noted.
		Administrator account use is logged for retrospective investigation if required.	Inspected the logs of administrator access to determine that administrator account use was logged for retrospective investigation if required.	No exceptions noted.
		A defined terminations process is followed including revocation of user access from systems in a timely manner.	Inspected the access removal for a sample of terminated employees to determine that a defined terminations process was followed including revocation of user access from systems in a timely manner.	No exceptions noted.

CC6.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		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.		
CC6.4	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.	The security policies set out the requirements for managing information security across Go1's operations.	Inspected the information security policies to determine that the security policies set out the requirements for Go1's operations.	No exceptions noted.
		The defined data disposal guidelines and requirements set out the process for ensuring data is erased prior to disposal of system assets.	Inspected the guidelines and requirements to determine that the defined data disposal guidelines and requirements set out the process for ensuring data was erased prior to disposal of system assets.	No exceptions noted.
		User access reviews are performed at least quarterly to confirm Go1 user access to critical systems is appropriate.	Inspected the user access reviews for a sample quarter to determine that user access reviews were performed at least quarterly to confirm Go1's user access to the infrastructure and software was appropriate.	No exceptions noted.

CC6.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Defined processes are in place to ensure terminated employees have returned or otherwise destroyed any confidential data.	Inspected a sample of terminated employees to determine that defined processes were in place to ensure terminated employees had returned or otherwise destroyed any confidential data.	No exceptions noted.
		A defined terminations process is followed including revocation of user access from systems in a timely manner.	Inspected the access removal for a sample of terminated employees to determine that a defined terminations process was followed including revocation of user access from systems in a timely manner.	No exceptions noted.
		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.	Inspected the information security policies to determine that the security policies set out the requirements for Go1's operations.	No exceptions noted.
		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.	Inspected the vulnerability management program to determine that a vulnerability management program was defined and documented to assess and manage the technical security of Go1's systems including identification, prioritization and resolution of vulnerabilities.	No exceptions noted.
		Azure Kubernetes encryption process is followed to ensure HTTPS was used to encrypt network traffic and secure company devices.	Inspected the Azure Kubernetes encryption process to determine that HTTPS was used to encrypt network traffic and secure company devices.	No exceptions noted.

CC6.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		The authorized WI-FI networks are encrypted, and password protected to prevent unauthorized access.	Inspected the WI-FI configurations to determine that the authorized WI-FI networks were encrypted, and password protected to prevent unauthorized access.	No exceptions noted.
		Independent penetration testing is conducted annually. Vulnerabilities identified are addressed in line with the identified severity ratings.	Inspected the penetration test report to determine that independent penetration testing was conducted annually. Vulnerabilities identified were addressed in line with the identified severity ratings.	No exceptions noted.
		Firewalls are used at external points of connectivity to the infrastructure and network.	Inspected the network diagram and system firewall documentation to determine that firewalls were used at external connectivity points to the network and infrastructure.	No exceptions noted.
		Web application firewalls are used to protect Go1's web applications from unauthorized activity.	Inspected the system diagram and web application firewall configurations to determine that the web application firewalls used.	No exceptions noted.
		Azure managed platform keys are used to deploy and rotate encryption keys automatically for encryption at rest.	Inspected the Azure managed platform encryption key configuration to determine that Azure managed platform keys were used to deploy and rotate encryption keys automatically for encryption at rest	No exceptions noted.
		Encryption keys are secured to limit access to authorized administrators with access logging.	Inspected the encryption key secure authentication, logging, and storage to determine that encryption keys were secured to limit access to authorized administrators with access logging.	No exceptions noted.

CC6.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Systematically applied security restrictions are used to protect against malicious software and data leakage.	Inspected the Cortex XDR configuration to determine that end user device hardening and data loss prevention configurations systematically applied security restrictions that are used to protect against malicious software and data leakage.	No exceptions noted.
		The information security policy include device hardening and data loss prevention requirements.	Inspected the information security policy terms to determine that the acceptable use section included device hardening and data loss prevention requirements.	No exceptions noted.
		Go1 end users' devices hard disks are encrypted to prevent unauthorized access to sensitive information.	Inspected the hard disk encryption configuration to determine that Go1 end users' devices hard disks were encrypted to prevent unauthorized access to sensitive information.	No exceptions noted.
		Vulnerability scans are performed at least bi-weekly. Vulnerabilities identified are addressed in line with the identified severity ratings.	Inspected the vulnerability scans for a sample of weeks to determine that bi-weekly vulnerability scans were performed. Vulnerabilities identified were addressed in line with the identified severity ratings.	No exceptions noted.
		The firewall settings are maintained through ongoing reviews and monitoring activities.	Inspected the firewall settings and management to determine that the firewall settings were maintained through restricting all access from untrusted networks, denying all traffic aside from necessary protocols, automated alerts for configuration changes, and restricted access to authorized administrators.	Descoped

CC6.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		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.	Inspected the information security policies to determine that the security policies set out the requirements for Go1's operations.	No exceptions noted.
		Firewalls are used at external points of connectivity to the infrastructure and network.	Inspected the network diagram and system firewall documentation to determine that firewalls were used at external connectivity points to the network and infrastructure.	No exceptions noted.
		Data at rest in the production database(s) is automatically encrypted.	Inspected the configuration settings for encryption to determine that data at rest in the production database(s) was automatically encrypted.	No exceptions noted.
		Data in transit to the infrastructure is automatically encrypted.	Inspected the configuration settings for encryption to determine that data in transit to the infrastructure and application was automatically encrypted.	No exceptions noted.
		Systematically applied security restrictions are used to protect against malicious software and data leakage.	Inspected the Palo Alto Cortex XDR configuration to determine that end user device hardening and data loss prevention configurations systematically applied security restrictions that are used to protect against malicious software and data leakage.	No exceptions noted.

CC6.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		The information security policy include device hardening and data loss prevention requirements.	Inspected the information security policy terms to determine that the acceptable use section included device hardening and data loss prevention requirements.	No exceptions noted.
		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.	Inspected the log of incidents and the incident management procedures to determine that incidents reported by external and internal users were centrally logged and monitored through to closure.	No exceptions noted.
		Server hardening and security patching are performed by the cloud provider for Go1's serverless architecture.	Inspected the cloud providers SOC 2 report to determine that server hardening, and security patching were performed by the cloud provider for Go1's serverless architecture.	No exceptions noted.
		The security policies set out the requirements for managing information security across Go1's operations.	Inspected the information security policies to determine that the security policies set out the requirements for Go1's operations.	No exceptions noted.
		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.	Inspected the vulnerability management program to determine that a vulnerability management program was defined and documented to assess and manage the technical security of Go1's systems including identification, prioritization and resolution of vulnerabilities.	No exceptions noted.

CC6.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Server hardening standards are defined and followed to ensure Go1 managed systems meet good practice security standards.	Inspected the shared responsibility model to determine that server hardening standards were defined and followed to ensure Go1 managed systems met good practice security standards.	No exceptions noted.
		Independent penetration testing is conducted annually. Vulnerabilities identified are addressed in line with the identified severity ratings.	inspected the penetration test report to determine that independent penetration testing was conducted annually. Vulnerabilities identified were addressed in line with the identified severity ratings.	No exceptions noted.
		Monitoring of end-point devices is performed to confirm compliance with anti-virus requirements.	Inspected the monitoring of end-point devices to determine that continuous monitoring of end-point devices was performed to confirm compliance with anti-virus requirements.	No exceptions noted.
		Network security monitoring is performed using network monitoring and threat detection software.	Inspected the network monitoring to determine that network security monitoring was performed using network monitoring and threat detection software.	No exceptions noted.
		Anti-virus software is installed to protect Go1 company devices.	Inspected the anti-virus software installation to determine that anti-virus software was installed to protect Go1 company devices.	No exceptions noted.
		Automatic updates are applied to ensure anti-virus definitions are kept current.	Inspected the configuration of automatic updates to determine that automatic updates were applied to ensure anti-virus definitions were kept current.	No exceptions noted.

CC6.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Systematically applied security restrictions are used to protect against malicious software and data leakage.	Inspected the Palo Alto Cortex XDR configuration to determine that end user device hardening and data loss prevention configurations systematically applied security restrictions that are used to protect against malicious software and data leakage.	No exceptions noted.
		The information security policy include device hardening and data loss prevention requirements.	Inspected the information security policy terms to determine that the acceptable use section included device hardening and data loss prevention requirements.	No exceptions noted.
		Vulnerability scans are performed at least bi-weekly. Vulnerabilities identified are addressed in line with the identified severity ratings.	Inspected the vulnerability scans for a sample of weeks to determine that bi-weekly vulnerability scans were performed. Vulnerabilities identified were addressed in line with the identified severity ratings.	No exceptions noted.
		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	Test Applied by the Service Auditor	Test Results
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.	Inspected the monitoring tools to determine that monitoring tools were used to identify and evaluate system performance, capacity, availability, and security-related indicators.	No exceptions noted.
		Incident management processes are defined and followed for identification, assessment, classification, response, communications to interested parties, and resolution.	Inspected the incident handling for a sample incident to determine that incident management processes were defined and followed for identification, assessment, classification, response, communications to interested parties, and resolution.	No exceptions noted.
		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.	Inspected the vulnerability management program to determine that a vulnerability management program was defined and documented to assess and manage the technical security of Go1's systems including identification, prioritization and resolution of vulnerabilities.	No exceptions noted.
		Risk assessments are conducted at least annually for the inventory of system assets to identify risks and actions required to mitigate those risks.	Inspected the cluster security risk assessment to determine that risk assessments were conducted at least annually for the inventory of system assets to identify risks and actions required to mitigate those risks.	No exceptions noted.

CC7.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Independent penetration testing is conducted annually. Vulnerabilities identified are addressed in line with the identified severity ratings.	inspected the penetration test report to determine that independent penetration testing was conducted annually. Vulnerabilities identified were addressed in line with the identified severity ratings.	No exceptions noted.
		Vulnerability scans are performed at least bi-weekly. Vulnerabilities identified are addressed in line with the identified severity ratings.	Inspected the vulnerability scans for a sample of weeks to determine that bi-weekly vulnerability scans were performed. Vulnerabilities identified were addressed in line with the identified severity ratings.	No exceptions noted.
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	Incidents reported by external and internal users are logged in a central repository for monitoring through to closure.	Inspected the log of incidents and the incident management procedures to determine that incidents reported by external and internal users were centrally logged and monitored through to closure.	No exceptions noted.
		The incident management policies and procedures document the approach to identifying reporting, evaluating, classifying and handling incidents.	Inspected the policies and procedures to determine that the incident management policies and procedures documented the approach to identifying, reporting, evaluating, classifying, and handling incidents.	No exceptions noted.

CC7.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
	whether they represent security events.	Incident management processes are defined and followed for identification assessment, classification, response, communications to interested parties and resolution.	Inspected the incident handling for a sample of incidents to determine that incident management processes were defined and followed.	No exceptions noted.
Risk assessments are conducted at least annually for the inventory of system assets to identify risks and actions required to mitigate those risks.		Inspected the cluster security risk assessment to determine that risk assessments were conducted at least annually for the inventory of system assets to identify risks and actions required to mitigate those risks.	No exceptions noted.	
Network security monitoring is performed using network monitoring and threat detection software.		Inspected the network monitoring to determine that network security monitoring was performed using network monitoring and threat detection software.	No exceptions noted.	
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	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.	Inspected the operations security policy to determine that security related change requirements based on vulnerabilities, security risk mitigation requirements, or other ongoing improvements had defined criteria to determine their relative priority or timeline for remediation.	No exceptions noted.

CC7.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
	prevent or address such failures.	Incidents reported by external and internal users are logged in a central repository for monitoring through to closure.	Inspected the log of incidents and the incident management procedures to determine that incidents reported by external and internal users were centrally logged and monitored through to closure.	No exceptions noted.
		The incident management policies and procedures document the approach to identifying, reporting, evaluating, classifying, and handling incidents.	Inspected the policies and procedures to determine that the incident management policies and procedures documented the approach to identifying, reporting, evaluating, classifying, and handling incidents.	No exceptions noted.
		Incident response plans are defined to provide guidelines for responding to major incidents including security breaches.	Inspected the incident response plans to determine that incident response plans were defined to provide guidelines for responding to major incidents including security breaches.	No exceptions noted.
		The risk assessments include consideration of risks related to information security compliance requirements, and third-party dependencies.	Inspected the risk register to determine that risk assessments included consideration of risks related to compliance requirements and third-party dependencies.	No exceptions noted.
		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.	Inspected the root cause analysis for a sample high severity incident to determine that root cause analysis was conducted to determine lessons learned and updates required to the incident response plans, as well as change requests raised for permanent fixes to prevent recurrence.	No exceptions noted.

CC7.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		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 to understand, contain, remediate, and communicate security incidents, as appropriate.	Incidents reported by external and internal users are logged in a central repository for monitoring through to closure.	Inspected the log of incidents and the incident management procedures to determine that incidents reported by external and internal users were centrally logged and monitored through to closure.	No exceptions noted.
		The incident management policies and procedures document the approach to identifying, reporting, evaluating, classifying, and handling incidents.	Inspected the policies and procedures to determine that the incident management policies and procedures documented the approach to identifying, reporting, evaluating, classifying, and handling incidents.	No exceptions noted.
		Incident response plans are defined to provide guidelines for responding to major incidents including security breaches.	Inspected the incident response plans to determine that incident response plans were defined to provide guidelines for responding to major incidents including security breaches.	No exceptions noted.
		The established emergency response team is defined to respond to major adverse events in a timely manner.	Inspected the incident response plan to determine that the established emergency response team was defined to respond to major adverse events in a timely manner.	No exceptions noted.
		The incident response plans are reviewed and updated at least annually to ensure they remain current and effective.	Inspected the incident response plans to determine that the incident response plans were reviewed and updated at least annually to ensure they remained current and effective.	No exceptions noted.

CC7.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		<p>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.</p>	<p>Inspected the business continuity plans to determine that the business continuity plans documented the disruptive scenarios, response plans, roles and responsibilities, key internal and external stakeholders, escalation procedures, communication channels to effectively manage critical events.</p>	<p>No exceptions noted.</p>
		<p>The business continuity plan is tested at least annually to ensure the response plans to critical events are effective.</p>	<p>Inspected the business continuity plan testing to determine that the business continuity plan was tested at least annually to ensure the response plans to critical events were effective.</p>	<p>No exceptions noted.</p>
		<p>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.</p>	<p>Inspected the root cause analysis for a sample high severity incident to determine that root cause analysis was conducted to determine lessons learned and updates required to the incident response plans, as well as change requests raised for permanent fixes to prevent recurrence.</p>	<p>No exceptions noted.</p>
<p>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.</p>				
CC7.5	<p>The entity identifies, develops, and implements activities to recover from identified security incidents.</p>	<p>Incidents reported by external and internal users are logged in a central repository for monitoring through to closure.</p>	<p>Inspected the log of incidents and the incident management procedures to determine that incidents reported by external and internal users were centrally logged and monitored through to closure.</p>	<p>No exceptions noted.</p>

CC7.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		The incident management policies and procedures document the approach to identifying, reporting, evaluating, classifying, and handling incidents.	Inspected the policies and procedures to determine that the incident management policies and procedures documented the approach to identifying, reporting, evaluating, classifying, and handling incidents.	No exceptions noted.
		The established emergency response team is defined to respond to major adverse events in a timely manner.	Inspected the incident response plan to determine that the established emergency response team was defined to respond to major adverse events in a timely manner.	No exceptions noted.
		The incident response plans are reviewed and updated at least annually to ensure they remain current and effective.	Inspected the incident response plans to determine that the incident response plans were reviewed and updated at least annually to ensure they remained current and effective.	No exceptions noted.
		The disaster recovery plan is tested at least annually to confirm that recovery procedures are effective.	Inspected the results of the disaster recovery tests to determine that the disaster recovery plan was tested at least annually to confirm that recovery procedures were effective.	No exceptions noted.
		The disaster recovery plan includes defined procedures to recover from significant events and is reviewed and updated at least annually.	Inspected the disaster recovery plan to determine that the disaster recovery plan included defined procedures to recover from significant events and was reviewed and updated at least annually.	No exceptions noted.
		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	Test Applied by the Service Auditor	Test Results
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.	Inspected the version control software to determine that Gitlab version control software was used to track changes to the source code and provide rollback capability if required.	No exceptions noted.
		Continuous integration continuous deployment (CI/CD) solution is used to configure key checks and conditions to be met prior to change release.	Inspected the CI/CD configuration to determine that Gitlab continuous integration, continuous deployment (CI/CD) solution was used to configure key checks and conditions to be met prior to change release.	No exceptions noted.
		System change requests are documented and tracked in a ticketing system.	Inspected the change log to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the operations security policy to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		Development and test environments are logically separated from the production environment.	Inspected the environments to determine that QA environment was logically separated from the production environment.	No exceptions noted.
		Access to the source code is restricted to authorized developers.	Inspected the developer access to determine that access to the source code was restricted to authorized developers.	No exceptions noted.

CC8.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Changes to the infrastructure configurations are managed as code to ensure the changes follow the formal change management process.	Inspected the system configuration to determine that changes to the infrastructure configurations are managed as code to ensure the changes follow the formal change management process.	No exceptions noted.
		Code developments require a system enforced peer review prior to merging with the master code branch.	Inspected the system configuration to determine that code developments required a system enforced peer review prior to merging with the master code branch.	No exceptions noted.
		Change releases require a system enforced review and approval prior to deployment.	Inspected the system configuration to determine that change releases required a system enforced review and approval prior to deployment.	No exceptions noted.
		Segregation of duties is maintained between the development and operations teams.	Inspected the system access for developers and operations personnel to determine that segregation of duties was maintained between the development and operations teams.	No exceptions noted.
		Static code analysis tools are used to scan and identify vulnerabilities in the source code.	Inspected the static code analysis to determine that static code analysis tools were used to scan and identify vulnerabilities in the source code.	No exceptions noted.

CC8.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		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.	Inspected the operations security policy to determine that security related change requirements based on vulnerabilities, security risk mitigation requirements, or other ongoing improvements had defined criteria to determine their relative priority or timeline for remediation.	No exceptions noted.
		Impact assessments are performed prior to deployment of changes to ensure users of the system are not adversely impacted.	Inspected the switch-on plan for account fields to determine that impact assessments were performed prior to deployment of changes to ensure users of the system were not adversely impacted.	Descoped
		System changes are automatically tested, and approval flows are verified in the configured continuous integration/continuous deployment (CI/CD) software before they can be promoted to production.	Inspected the configured continuous integration/continuous deployment (CI/CD) to determine that system changes were automatically tested, and approval flows were verified in the configured continuous integration/continuous deployment (CI/CD) software before they can be promoted to production.	No exceptions noted.
		Changes are assessed to determine whether communications to users of the system are required and are performed accordingly.	Inspected the assessment of communication requirements for a sample of changes to determine that changes were assessed to determine whether communications to users of the system were required.	Descoped

CC8.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Release notes for changes are sent to internal and external stakeholders, as applicable.	Inspected the release notes for a sample of change releases to determine that release notes for changes were sent to internal and external stakeholders, as applicable.	No exceptions noted.
		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	Test Applied by the Service Auditor	Test Results
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.	Inspected the organization chart, job descriptions and documented policies to determine that management considered interactions with, and the need to monitor the activities of third parties when documenting the organizational chart and defining job descriptions.	No exceptions noted.
		Go1 has purchased insurance to offset or compensate for the financial loss of an adverse event with the services.	Inspected the insurance policy to determine that the entity had purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.
		The disaster recovery plan is tested at least annually to confirm that recovery procedures are effective.	Inspected the results of the disaster recovery tests to determine that the disaster recovery plan was tested at least annually to confirm that recovery procedures were effective.	No exceptions noted.
		The disaster recovery plan includes defined procedures to recover from significant events and is reviewed and updated at least annually.	Inspected the disaster recovery plan to determine that the disaster recovery plan included defined procedures to recover from significant events and was reviewed and updated at least annually.	No exceptions noted.

CC9.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		<p>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.</p>	<p>Inspected the business continuity plans to determine that the business continuity plans documented the disruptive scenarios, response plans, roles and responsibilities, key internal and external stakeholders, escalation procedures, communication channels to effectively manage critical events.</p>	<p>No exceptions noted.</p>
		<p>The business continuity plan is tested at least annually to ensure the response plans to critical events are effective.</p>	<p>Inspected the business continuity plan testing to determine that the business continuity plan was tested at least annually to ensure the response plans to critical events were effective.</p>	<p>No exceptions noted.</p>
CC9.2	<p>The entity assesses and manages risks associated with vendors and business partners.</p>	<p>Management has defined a third-party vendor risk management approach for evaluating third-party risks.</p>	<p>Inspected the third-party management policy to determine that management had defined a third-party vendor risk management approach for evaluating third-party risks.</p>	<p>No exceptions noted.</p>
		<p>The third-party vendor register includes a listing of material vendors for tracking and monitoring.</p>	<p>Inspected the third-party vendor register to determine that the third-party vendor register included a listing of material vendors for tracking and monitoring.</p>	<p>No exceptions noted.</p>
		<p>An annual vendor risk assessment is completed to ensure the identification and treatment of risks remains accurate and appropriate.</p>	<p>Inspected the vendor register to determine that an annual vendor risk assessment was completed to ensure the identification and treatment of risks remains accurate and appropriate.</p>	<p>No exceptions noted.</p>

CC9.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the vendor security and security review policy to determine that management developed third-party risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		Management has assigned responsibility and accountability for the management of risks and governance associated with third parties to appropriate personnel.	Inspected the assigned responsibilities for third-party vendors to determine that management had assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.	No exceptions noted.
		The entity has documented procedures for terminating third-party relationships.	Inspected the termination procedures to determine that the entity had documented procedures for terminating third-party relationships.	No exceptions noted.
		The risk assessments include consideration of risks related to information security compliance requirements, and third-party dependencies.	Inspected the risk register to determine that risk assessments included consideration of risks related to compliance requirements and third-party dependencies.	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk register to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.

CC9.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		A formal risk assessment is completed for each new vendor prior to commencing the services provided.	Inspected the risk assessment for a sample of new vendors to determine that a formal risk assessment was completed for each new vendor prior to commencing the services provided.	No exceptions noted.
		New third-party vendors are approved by management prior to selection and onboarding.	Inspected the approval for a sample new vendor to determine that new third-party vendors were approved by management prior to selection and onboarding.	Descoped
		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.	Inspected the third-party agreements for a sample vendor to determine that the entity's third-party agreements outlined and communicated; 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.	No exceptions noted.
		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.	Inspected the review of third-party attestation reports for a sample of material third-party vendors to determine that management obtained and reviewed attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.

Trust Services Criteria for the Availability Category

A1.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
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.	Inspected the monitoring tools to determine that monitoring tools were used to identify and evaluate system performance, capacity, availability, and security-related indicators.	No exceptions noted.
		A load balancer is used to automatically distribute traffic across multiple availability zones.	Inspected the load balancer configuration to determine that a load balancer was used to automatically distribute traffic across multiple availability zones.	No exceptions noted.
		Preventive services are used to prepare for and protect against attacks that may compromise availability of the service.	Inspected the DDOS tool configuration to determine that a DDOS tool was used to prepare for, and protect against, attacks that may compromise availability of the service.	No exceptions noted.
		Processing capacity is configured to auto-scale to meet processing demand.	Inspected the configurations of capacity scaling to determine that processing capacity was configured to auto-scale to meet processing demand.	No exceptions noted.
		The system is designed with multiple availability zones and redundancy to support continued availability in the event of a failure.	Inspected the system documentation to determine that the system was designed with redundancy to support continued availability in the event of a failure.	No exceptions noted.
A1.2	The entity authorizes, designs, develops, or acquires, implements, operates, approves,	A load balancer is used to automatically distribute traffic across multiple availability zones.	Inspected the load balancer configuration to determine that a load balancer was used to automatically distribute traffic across multiple availability zones.	No exceptions noted.

A1.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
	maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Backups of the application and database are performed daily.	Inspected the backup configuration to determine that daily backups of the application and database were performed.	No exceptions noted.
		The operations security policy establishes the requirements for backups and recoverability.	Inspected the operations security policy to determine that the backup section established the requirements for backups and recoverability.	No exceptions noted.
		The system is designed with multiple availability zones and redundancy to support continued availability in the event of a failure.	Inspected the system documentation to determine that the system was designed with redundancy to support continued availability in the event of a failure.	No exceptions noted.
		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.	Inspected the results of the disaster recovery tests to determine that the disaster recovery plan was tested at least annually to confirm that recovery procedures were effective.	No exceptions noted.
		The disaster recovery plan includes defined procedures to recover from significant events and is reviewed and updated at least annually.	Inspected the disaster recovery plan to determine that the disaster recovery plan included defined procedures to recover from significant events and was reviewed and updated at least annually.	No exceptions noted.
		Backup and restoration tests are performed on at least an annual basis to ensure the recovery controls are effective.	Inspected the backup restoration test to determine that backup and restoration tests were performed on at least an annual basis to ensure the recovery controls were effective.	No exceptions noted.

A1.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		When a backup job fails the backup tool sends an alert to the backup administrators who investigate and resolve the failure.	Inspected the alert configuration to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure.	No exceptions noted.
		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.	Inspected the business continuity plans to determine that the business continuity plans documented the disruptive scenarios, response plans, roles and responsibilities, key internal and external stakeholders, escalation procedures, communication channels to effectively manage critical events.	No exceptions noted.
		The business continuity plan is tested at least annually to ensure the response plans to critical events are effective.	Inspected the business continuity plan testing to determine that the business continuity plan was tested at least annually to ensure the response plans to critical events were effective.	No exceptions noted.

Trust Services Criteria for the Confidentiality Category

C1.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The requirements for managing data are established in the data management policy.	Inspected the data management policy to determine that the requirements for managing data were established in the data management policy.	No exceptions noted.
		The information security policy sets out the requirements of employees to ensure confidential data is handled appropriately.	Inspected the information security policy terms to determine that the acceptable use section set out the requirements of employees to ensure confidential data was handled appropriately.	No exceptions noted.
		Documented confidential policies and procedures are in place that consider and set the requirements for how data is managed effectively to protect confidentiality.	Inspected the data management policy and procedures to determine that documented confidential policies and procedures were in place that considered and set the requirements for identifying, classifying, labelling and retention period of data.	No exceptions noted.
		Guidance is provided to end users of the system in relation to the requirements for protecting confidential data while using the system.	Inspected the data management policy to determine that guidance was provided to end users of the system in relation to the requirements for protecting confidential data while using the system.	No exceptions noted.
		The types of confidential data collected and processed have been identified and classified.	Inspected the data management policy to determine that the types of confidential data collected and processed were identified and classified.	No exceptions noted.

C1.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
		A register of the types and sources of confidential data collected and processed is maintained to track assets and storage locations of confidential data.	Inspected the data register to determine that a register of the types and sources of confidential data collected and processed was maintained to track assets and storage locations of confidential data.	No exceptions noted.
		Confidential data is maintained within the system boundaries at times where security controls are applied to restrict access to authorized individuals.	Inspected the confidential data documentation to determine that confidential data was maintained within the system boundaries where security controls were applied to restrict access to authorized individuals.	No exceptions noted.
		The risk assessment has identified how confidential data may be leaked outside the boundaries of the system to ensure appropriate protections are in place.	Inspected the risk assessment to determine that the risk assessment identified how confidential data may be leaked outside the boundaries of the system to ensure appropriate protections were in place.	No exceptions noted.
		Defined processes are in place to ensure terminated employees have returned or otherwise destroyed any confidential data.	Inspected a sample of terminated employees to determine that defined processes were in place to ensure terminated employees had returned or otherwise destroyed any confidential data.	No exceptions noted.
		The entities third-party agreements include requirements for protecting confidential data.	Inspected the third-party agreement for a sample material vendor to determine that the entities third-party agreements included requirements for protecting confidential data.	No exceptions noted.

C1.0	Criteria	Control Activity	Test Applied by the Service Auditor	Test Results
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.	Inspected the guidelines and requirements to determine that the defined data disposal guidelines and requirements set out the process for ensuring data was erased prior to disposal of system assets.	No exceptions noted.
		The retention period of confidential data is classified based on the purpose and type of data and location the data is stored.	Inspected the confidential data documentation to determine that the retention period of confidential data was classified based on the purpose and type of data and location the data is stored.	No exceptions noted.
		Confidential information is protected from erasure or destruction during the specified retention period by following defined processes.	Inspected the data management policy to determine that confidential information was protected from erasure or destruction during the specified retention period by following defined processes.	No exceptions noted.

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

**SECTION V –
OTHER INFORMATION PROVIDED BY THE
SERVICE ORGANIZATION**

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Ref	Control Activity	Test Applied	Test Results	Management's Response
CC1.1 CC1.4	Background checks are completed for candidates prior to employment.	Inspected the background checks for a sample of new hires to determine that background checks were completed for candidates prior to employment.	Testing of the control activity disclosed that background checks were not completed prior to employment for 2 out of 5 new hire samples tested.	<p>In both instances the employees were hired using third-party recruiters which didn't follow our internal processes for performing background checks prior to the start date of the employee. In both instances the employees had completed background checks within two days of starting their roles.</p> <p>The People Operations team have adjusted processes to ensure background checks are performed prior to the start date.</p>

