GroupMap Technology Pty Ltd
(dba 'TeamRetro')
SOC 3 for Service Organisations Report

1 March 2022 to 28 February 2023

assurancelab

CONTENTS

SECTION I –
ASSERTION OF GROUPMAP TECHNOLOGY PTY LTD MANAGEMENT

ASSERTION OF GROUPMAP TECHNOLOGY PTY LTD MANAGEMENT

14 April 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within GroupMap Technology Pty Ltd's ('GroupMap') TeamRetro (the 'System') throughout the period 1 March 2022 to 28 February 2023, to provide reasonable assurance that ABC's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, and Privacy ('Agreed Criteria') set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria. Our description of the boundaries of the system is presented in 'GroupMap Technology Pty Ltd's Description of its System' (the 'Description') and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the System throughout the period 1 March 2022 to 28 February 2023, to provide reasonable assurance that GroupMap's service commitments and system requirements were achieved based on the Agreed Criteria. GroupMap's objectives for the system in applying the Agreed Criteria are embodied in its service commitments and system requirements relevant to the Agreed Criteria. The principal service commitments and system requirements related to the Agreed Criteria are presented in 'GroupMap Technology Pty Ltd's Description of its System'.

GroupMap uses Amazon Web Services (AWS, 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 GroupMap, to achieve GroupMap's service commitments and system requirements based on the Agreed Criteria. The Description presents GroupMap's controls, the Agreed Criteria, and the types of complementary subservice organization controls assumed in the design of GroupMap'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 GroupMap, to achieve GroupMap's service commitments and system requirements based on the Agreed Criteria. The Description presents GroupMap's controls, the Agreed Criteria, and the complementary user entity controls assumed in the design of GroupMap's controls.

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

We assert that the controls within the system were effective throughout the period 1 March 2022 to 28 February 2023, to provide reasonable assurance that GroupMap's service commitments and system requirements were achieved based on the Agreed Criteria.

Jeremy Lu
Chief Executive Officer
GroupMap Technology Pty Ltd

SECTION II –
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: GroupMap Technology Pty Ltd

Scope

We have examined GroupMap Technology Pty Ltd's ('GroupMap') accompanying description of its TeamRetro ('the Description') which has been prepared for the purposes of the independent assurance report.

GroupMap 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 GroupMap's TeamRetro (the 'System') that may be useful when assessing the risks arising from interactions with GroupMap's system. This includes the controls that GroupMap 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, Confidentiality, and Privacy (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).

GroupMap uses Amazon Web Services (AWS 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 GroupMap, to achieve GroupMap's service commitments and system requirements based on the Agreed Criteria. The complementary subservice organization controls have been reviewed by GroupMap management. The Description does not disclose the actual controls at the subservice organization. Our review 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 GroupMap, to achieve GroupMap's service commitments and system requirements based on the Agreed Criteria. The Description presents GroupMap's controls, the Agreed Criteria, and the complementary user entity controls assumed in the design of GroupMap's controls. The complementary user entity controls have not been assessed by our review and remain the responsibility of those related entities to complete their own review.

Service Organization's Responsibilities

GroupMap 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 GroupMap's service commitments and system requirements were achieved. GroupMap has provided the accompanying assertion titled "Assertion of GroupMap Technology 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. GroupMap 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 GroupMap'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 review. Our review was conducted in accordance with ASAE 3150 (SOC 2), the attestation standards put forth by the Auditing and Assurance Standards Board (AUASB). Those standards require that we plan and perform our review 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 GroupMap'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.

A review of the description of GroupMap's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and GroupMap'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 GroupMap 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 GroupMap 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, management's assertion that the controls within GroupMap's TeamRetro were effective throughout the period 1 March 2022 to 28 February 2023, to provide reasonable assurance that GroupMap's service commitments and system requirements were achieved based on the Agreed Criteria is fairly stated, in all material respects.

Restricted Use

This report is intended solely for the information and use of GroupMap, user entities of GroupMap's TeamRetro, business partners of GroupMap subject to risks arising from interactions with the TeamRetro, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The Agreed Criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

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

Erika Villanueva

Erika Villanueva, CA, CPA
AssuranceLab
Sydney, Australia
14 April 2023

SECTION III –
GROUPMAP TECHNOLOGY PTY LTD'S DESCRIPTION OF ITS SYSTEM

OVERVIEW OF OPERATIONS

Company Background

GroupMap was founded in September 2012 to develop web-based Software as a Service collaboration and group decision making tools. GroupMap focuses on improving the effectiveness of online meetings, return on time investment and productivity.

GroupMap is a distributed company, with primary headquarters based in Perth, Australia.

Industries served by GroupMap include Information Technology and Communications, Financial Services, Telecommunications, Pharmaceutical, Manufacturing, Consumer Goods, Gaming and Entertainment, Health Care, Retail, Educational institutions, and Government agencies.

Description of Services Provided

GroupMap's core application TeamRetro enables online agile retrospectives and team health checks, helping teams realize continuous improvement.

The TeamRetro product enables processing of:

Agile retrospective meetings

- Capturing ideas
- Capturing reactions
- Grouping related / similar ideas
- Capturing user reactions to ideas
- Capturing user votes on ideas worth discussing forward
- Capturing proposed / accepted action items
- Capturing proposed / accepted team agreements
- Publishing retrospective summaries to external systems (such as Confluence, Slack)

Agile health check meetings

- Capturing ratings along user-defined health dimensions
- Capturing comments related to health dimensions
- Capturing discussion along health dimensions
- Capturing proposed / accepted action items
- Capturing proposed / accepted team agreements
- Publishing health check summaries to external systems (such as Confluence)

Team action items

- Capturing proposed / accepted action items
- Capturing action status
- Publishing actions to external task management systems (such as Jira, Trello, Azure DevOps)

Team agreements

- Capturing proposed / accepted team agreements

Reporting

- Cross-team health report
- Team activity report
- User activity report
- Action reports
- Exports in multiple data formats

SCIM for team provisioning

API access

Retrospectives

Retrospective templates can be used to capture ideas, comments and reactions from participants against a series of retrospective trigger prompts such as *What went well? What didn't go well?* etc. Ideas are then grouped and voted on to prioritize for deeper discussion. Each group is then discussed in turn enabling additional comments, reactions can be added by participants, and new action items or team agreements can be proposed or added against these groups. Finally, action items and team agreements are reviewed, assigned, and then shared with meeting participants.

Health Checks

Health check templates can be used to capture participant ratings and comments along key health dimensions such as *Codebase Complexity, Communication, Team Work* etc. Health dimensions are then sorted based on aggregate rating to prioritize for deeper discussion. Each dimension is then discussed in turn where participants can add further comments or propose or add new action items or team agreements. Finally, action items and team agreements are reviewed, assigned, and then shared with meeting participants.

Both retrospective and health check activities can be run synchronously (with all participants online at the same time) or asynchronously (with each participant contributing at their leisure). Both activities can be run fully anonymously, partially anonymously, or non-anonymously.

Principal Service Commitments and System Requirements

GroupMap designs its processes and procedures related to its TeamRetro system to address the service commitments made to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that GroupMap has established for the services.

Security commitments to user entities are documented and communicated in Data Processing Agreements, enterprise agreements and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include security principles within the fundamental designs of the TeamRetro system that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

GroupMap establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in GroupMap's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required for the operation and development of the TeamRetro product.

Components of the System

Infrastructure

GroupMap's primary infrastructure used to provide the TeamRetro product includes the following:

System	Type	Description
Amazon Web Services (AWS)	Managed application servers (AWS ECS)	Server infrastructure for business logic and database binding and mapping to logic
	Managed Postgres databases (AWS Aurora Postgres)	Storage of dynamic customer data
	Managed Backups (AWS Backup)	Backups of customer data
	Managed Redis databases (AWS Elasticache)	User session management, rate limiting and caching
	Content delivery network (AWS CloudFront)	Low-latency, global delivery of static content
	Cloud object storage (AWS S3)	Storage of static application and customer assets
	Web Application Firewall (AWS WAF)	Application security and web application firewall
	Networking infrastructure / logging (AWS VPC, AWS Route53, AWS Application Load Balancer, AWS Systems Manager, AWS ECR, AWS CloudFormation, AWS CloudWatch, AWS CloudTrail), AWS SSO, AWS VPN	Core networking infrastructure, operational monitoring, and alerts
DataDog	Infrastructure dashboards	Operational insights and alerts

System	Type	Description
Solarwinds	Logging (Papertrail)	Operational insights and alerts
	Monitoring (Pingdom)	Operational insights and alerts
GitHub	Source code management, CI/CD, deployment pipeline	Change release testing through production deployment
Pusher	Scalable websocket broadcasting (Channels)	Real-time websocket based data synchronization
SendGrid	Email delivery	Transactional and marketing emails
PayPal	Payment Gateway (Braintree)	Online subscription payments

Software

Primary software is used to support GroupMap's system.

Software	Purpose
Google Workspace	User authentication, documents, spreadsheets, and file storage
Linear	Task management
HelpScout	Service desk
OneTrust	SOC2 compliance management
Slack	Internal communications
HelloNext	Product roadmap, customer feedback
LastPass	Password management
Hexanode	Device management

People

GroupMap has approximately 12 employees that are organized into the following functional areas:

Area	Purpose
Corporate	Including Executives, Finance, Talent, Human Resources
Customer Experience	Including Customer Support, Customer Success, Customer Delivery and CX Operations teams. They provide day to day support to customers, whether dealing with issues from existing customers, to onboarding new customers, as well as how the company can uplift the overall customer experience.
Product Development	Including product management, UX design, as well as analysis, development and quality activities focusing on development and verification of the product.

Area	Purpose
Operations	Including infrastructure, development and quality activities focus on maintenance, security and reliability of the product, platform, and infrastructure.
Sales	Sales is driven by growth and its focus is on retaining existing clients and maximizing advocacy in addition to growing existing customers and new customer acquisition
Marketing	Provides company wide, consistent branding, positioning and drives programs to deliver sustainable growth.

Data

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

TeamRetro customer data, including:

- Retrospective data (ideas, reactions, groups, votes, comments, reactions)
- Health check data (ratings, comments)
- Team action items
- Team agreements
- Custom retrospective templates
- Custom health check templates
- User emails, names, avatars and password hashes
- SCIM groups and users
- User requests
- Reports

Logs

- Activity logs
- Admin logs
- API logs
- Error logs
- Integration logs
- System logs

Supporting data

- Quotes
- Invoices
- Contracts
- Payment history
- Customer queries + tickets + feature suggestions

Privacy Commitments

GroupMap collects and processes personal data as part of TeamRetro. This requires adhering to privacy regulations that apply in each country of operation.

Personally identifiable information collected from users includes email address, full name and internet protocol (IP) address. This information is collected through the online signup process, via invitation from an existing user, or via the optional SSO and SCIM integrations.

Users are presented with the governing TeamRetro Privacy Policy and TeamRetro Terms of Service for review while creating a new account. Any additional users invited to join the account are additionally presented the Privacy Policy and Terms of Service within the invitation emails sent by TeamRetro.

The full TeamRetro Privacy Policy is published on the TeamRetro website at https://www.teamretro.com/privacy and addresses how any personal information and intellectual property is collected, used, retained, disclosed, disposed and anonymized.

The Privacy Policy also provides details of the assigned Privacy Officer, assigned EU Representative and contact information including the primary privacy@teamretro.com email.

The following table describes the personal information collected and processed as part of the System of GroupMap:

Private Data	Reporting
Retrospective data Ideas Reactions Groups Votes Comments Custom retrospective templates	Retrospective summary (PDF) Ideas report (CSV, XLSX) Ideas with comments report (CSV, XLSX) Actions report (CSV, XLSX) Retrospective activity report (CSV, XLSX) Team activity report (CSV, XLSX)
Health check data Ratings Comments Votes Custom health check templates	Health check summary (PDF) Latest health report (CSV, XLSX) Historical health report (CSV, XLSX) Actions report (CSV, XLSX) Health check activity report (CSV, XLSX) Team activity report (CSV, XLSX)
Team Team action items Individual team member action items Team agreements	Teams report (CSV, XLSX) Team activity report (CSV, XLSX) Individual action report (CSV, XLSX)
Users Usernames	Users report (CSV, XLSX)

Private Data	Reporting
Email addresses Avatars Password hashes	

GroupMap is committed to attestation reporting for the SOC 2 Trust Services Criteria related to Privacy to demonstrate the governance, accountability and alignment of its privacy commitments.

Processes, Policies and Procedures

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

Physical Security

The in-scope system and supporting infrastructure are hosted by Amazon Web Services (AWS). As such, AWS is responsible for the physical security controls for the in-scope service. AWS accreditations include ISO 27001, ISO 27017, ISO 27018, SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II), PCI Level 1, FISMA Moderate and Sarbanes-Oxley (SOX).

Logical Access

GroupMap uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, GroupMap implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Employees and approved vendor personnel sign on to the GroupMap software using Google Workspace user ID and passwords.

Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Google Workspace. Passwords must conform to defined password standards and are enforced through parameter settings in the Google Workspace. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts,

and mask workstation screens, requiring re-entry of the user ID and password after a period of inactivity.

Employees are required to use a token-based two-factor authentication where available.

Customer employees' access TeamRetro through the Internet using the SSL functionality of their web-browser. These customer employees must supply a valid email address and password to gain access to customer cloud resources. Passwords must conform to minimum password complexity requirements. Alternatively, customers may opt to require Single Sign On via a customer managed SAML Identity Provider.

Upon approved hire, employees are inducted, and an employee onboarding checklist is completed for each Employee. Employees are entered into the company's financial and access management system. A checklist is used to determine the access to be granted and used by the systems provisioning team to create user ID and access rules based on their associated position and required duties. These access rules are reviewed by the Executive Committee on an annual basis, including the CEO and CTO. In evaluating role access, the group considers the job description, duties requiring segregation and risks associated with the access. Completed rules are reviewed and approved by the CTO. As part of this process, the CTO reviews access by privileged roles and requests modifications based on this review.

In the event of change of roles and duties, role lists are generated by security and provided to managers for review. The CTO reviews employees with access to privileged roles and requests modifications as needed through our applications management system.

Upon termination of an employee, the security team reviews the application management system to suspend user ID and immediately deletes all access roles from ID's belonging to the terminated employee.

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 security, availability and integrity of the infrastructure, software and data. Alerts and logs are monitored with incident management processes defined for handling and resolving adverse events.

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

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

GroupMap monitors the capacity utilization of server infrastructure to ensure that service delivery matches service level agreements. GroupMap evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following:

- Application server utilization (memory, CPU, network)
- Storage utilization (memory, CPU, network)
- Websocket capacity utilization

GroupMap maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers. Management approves changes prior to migration to the production environment and documents those approvals within the version control software.

GroupMap has implemented a patch management process to ensure infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and GroupMap system owners review proposed operating system patches to determine whether the patches are applied. Customers and GroupMap systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. GroupMap staff validate that all patches have been installed and if applicable that reboots have been completed.

Data Governance

GroupMap 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 security, availability and integrity commitments of GroupMap.

Established processes, policies, 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.

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data centre services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

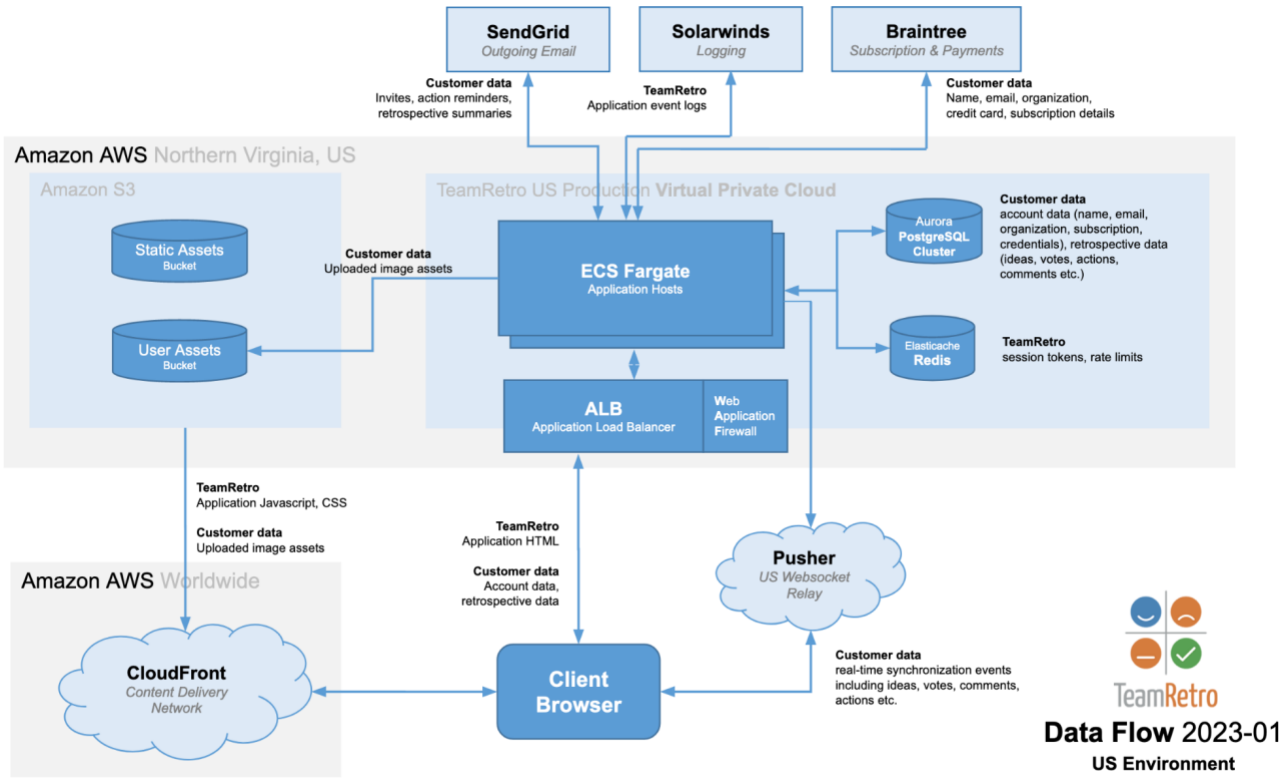
Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by GroupMap. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed on a monthly basis in accordance with GroupMap policy. The scanning solution uses industry standard technologies and a formal methodology specified by GroupMap. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the GroupMap system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system from the Internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes the TeamRetro software as a service system (the "System"). This report does not cover the infrastructure services provided by Amazon Web Services. AWS accreditations include ISO 27001, ISO 27017, ISO 27018, SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II), PCI Level 1, FISMA Moderate and Sarbanes-Oxley (SOX).



Changes to the System in the Last 12 Months

In the last 12 months the TeamRetro platform has migrated from Salesforce Heroku (PaaS) to being directly hosted on AWS infrastructure for improved performance and availability.

A running log of application improvements and updates can be found at https://help.teamretro.com/article/308-whats-new

Incidents in the Last 12 Months

Three high-severity outage incidents affecting multiple customers occurred to the services in the 12 months preceding the end of the review period listed below:

Date	Title	Summary
2022-08-24	Heroku DNS Outage	A Heroku DNS routing issue resulted in both EU and US environments going offline for customers starting at 07.17 AWST. A mitigation was deployed at 08.05 AWST (after 48 minutes) restoring TeamRetro access. A permanent fix was deployed by Heroku at 11.00 AWST.
2022-11-08	Pusher Outage	An expired certificate with MessageBird (Pusher) caused real-time synchronization to fail in US-hosted environments (EU environments unaffected) for 34 minutes.
2023-01-13	Degraded Performance	A performance degradation starting at 23:00 AWST resulted in request timeouts for some users when traffic ramped faster than the implemented auto-scaling rules were anticipating. The incident was resolved at 23:40 AWST after 40 minutes as new application hosts were brought online.

Criteria Not Applicable to the System

All Common Criteria/Security, Availability, Confidentiality, Privacy Trust Services Criteria was applicable to GroupMap's TeamRetro System.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

Subservice Description of Services

Amazon Web Services - AWS provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses around the world. TeamRetro utilizes AWS datacentres in Northern Virginia, United States (us-east-1) and Frankfurt, Germany (eu-central-1).

Complementary Subservice Organization Controls

GroupMap'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 GroupMap's services to be solely achieved by GroupMap control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of GroupMap.

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

Subservice Organization – Amazon Web Service (AWS)		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	Physical access to data centres is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centres is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television cameras ('CCTV'). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
	CC2.1, CC6.1, CC6.6, CC6.8,	Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics

Subservice Organization – Amazon Web Service (AWS)		
Category	**Criteria**	**Control**
	CC7.2, CC7.3, CC7.4	Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution
	CC6.1, CC6.6, CC.7.1, CC8.1	Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters.
		Firewall policies (configuration files) are automatically pushed to production firewall devices
		Firewall policy updates are reviewed and approved
Availability	A1.2	Amazon-owned data centres are protected by fire detection and suppression systems.
		Amazon-owned data centres are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply ('UPS') units provide backup power in the event of an electrical failure in Amazon-owned data centres.
		Amazon-owned data centres have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.

GroupMap 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, GroupMap performs monitoring of the subservice organization controls by reviewing attestation reports and monitoring the performance of the subservice organization controls in relation to security, availability and system integrity.

COMPLEMENTARY USER ENTITY CONTROLS

GroupMap'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 GroupMap's services to be solely achieved by GroupMap control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of GroupMap'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.

1. User entities are responsible for understanding and complying with their contractual obligations to GroupMap.
2. User entities are responsible for notifying GroupMap of changes made to technical or administrative contact information.
3. User entities are responsible for ensuring TeamRetro user login additions and changes are authorized prior to being enacted.
4. User entities are responsible for ensuring TeamRetro user logins are removed in a timely manner upon termination.
5. User entities are responsible for reviewing TeamRetro user logins on a periodic basis to ensure access is restricted to authorized and appropriate individuals.
6. User entities are responsible for ensuring privileged roles on their TeamRetro account, administrator and owner roles, are approved by appropriate personnel prior to being enacted.
7. User entities are responsible for ensuring the supervision, management, and control of the use of TeamRetro by their personnel.
8. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize TeamRetro.
9. User entities are responsible for immediately notifying GroupMap of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
10. User entities are responsible for configuring Single Sign On via their own identity provider (where available) and require SSO login for their TeamRetro account.
11. User entities are responsible for configuring API and/or SCIM automated provisioning (where available) for their TeamRetro account.

assurancelab