REPORT ON

GTMHUB'S

OKR MANAGEMENT SAAS SYSTEM RELEVANT TO SECURITY AND AVAILABILITY THROUGHOUT THE PERIOD

AUGUST 1, 2020 TO JULY 31, 2021

MARCUM
ACCOUNTANTS ▲ ADVISORS

Acronym Table

AD	Active Directory
AICPA	American Institute of Certified Public Accountants
BoD	Board of Directors
CEO	Chief Executive Officer
COSO	Committee of Sponsoring Organizations
CRM	Customer Relationship Management
CTO	Chief Technology Officer
DC	Description Criteria
HR	Human Resource
ICPC	Internal Control Project Charter
IP	Internet Protocol
ISMS	Information Security Management System
IT	Information Technology
MFA	Multi-Factor Authentication
NDA	Non-Disclosure Agreement
OKR	Objectives and Key Results
QA	Quality Assurance
RDP	Remote Desktop Protocol
SaaS	Software as a Service
SSO	Single Sign-On
SOC	Standard Operating Controls
TSC	Trust Service Categories
TSP	Trust Service Principles
VPN	Virtual Private Network
WAF	Web Application Firewall

Assertion of the Management of Gtmhub

We are responsible for designing, implementing, operating, and maintaining effective controls within Gtmhub's OKR Management Saas System throughout the period August 1, 2020 to July 31, 2021, to provide reasonable assurance that Gtmhub's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the OKR Management Saas System throughout the period August 1, 2020 to July 31, 2021, to provide reasonable assurance that Gtmhub's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria)set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Gtmhub's objectives for the OKR Management Saas System in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

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 OKR Management Saas System were effective throughout the period August 1, 2020 to July 31, 2021, to provide reasonable assurance that Gtmhub's service commitments and system requirements were achieved based on the applicable trust services criteria.

/s/ Radoslav Georgiev

CTO

Gtmhub, Inc.

September 20, 2021

Section 2: Independent Service Auditors' Report

MARCUM
ACCOUNTANTS ▲ ADVISORS

Independent Service Auditors' Report

To: Gtmhub

Scope

We have examined Gtmhub's accompanying assertion, titled "Assertion of the Management of Gtmhub" (assertion) that the controls within Gtmhub's OKR Management Saas System were effective throughout the period August 1, 2020 to July 31, 2021, to provide reasonable assurance that Gtmhub's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Gtmhub is responsible for responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Gtmhub's service commitments and system requirements were achieved. Gtmhub has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Gtmhub is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditors' Responsibilities

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Gtmhub's service commitments and system requirements based on the applicable trust services criteria.

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Gtmhub's service commitments and system requirements based on the applicable trust services criteria.

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

Inherent Limitations

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the 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 Gtmhub's OKR Management Saas System were effective throughout the period August 1, 2020 to July 31, 2021, to provide reasonable assurance that Gtmhub's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Marcum LLP

September 20, 2021
Tampa, FL

Attachment A: Gtmhub's Description of its OKR Management SaaS System

System Description

Company Overview and Services Provided

Founded in Sofia, Bulgaria on July 7, 2015 and with offices in Denver, London and Berlin, Gtmhub helps organizations bridge the gap between strategy and operational execution. Gtmhub's platform enables executives and managers to amplify staff effort and accelerate growth by connecting strategic priorities to daily actions using the OKR methodology. Gtmhub integrates more than 160 CRM, tasking, business intelligence and other commonly used tools directly with key results, enabling real-time progress monitoring and active course corrections. Hundreds of enterprises, not-for-profits and even governments rely on Gtmhub to align and focus their organizations for accelerated growth.

Infrastructure

The production IT infrastructure supporting Gtmhub's OKR Management SaaS system is hosted on Azure with authentication tied in through Azure AD. The infrastructure consists of servers, virtual routers and switches, WAF, and software systems, which are located at the data center locations of the subservice organization. Each region can be used as a failover site in case of an outage. Backups are automatically created and encrypted in Azure Cloud and are then transferred using HTTPS to Amazon S3 buckets for storage.

The production environment is managed only by authorized personnel. Only authorized services and protocols that meet security requirements are permitted access to the network. Security groups are designed to automatically deny any traffic not explicitly authorized. Administrative access to security functions is limited to authorized administrative personnel. Changes to network configurations are reviewed and approved by authorized IT team members prior to deployment.

Software

The following provides a summary of systems used to deliver the OKR Management SaaS System:

- Jira – utilized for help desk ticketing and project management.
- Cloudflare – utilized for WAF and DDOS to protect the Gtmhub platform.
- Auth0 – utilized as identity provider for access to Gtmhub application
- Bitbucket – utilized as a code repository
- Slack – utilized for messaging and alerting
- Terraform – utilized for the deployment of new systems
- Confluence – utilized as a source of information for users of the system
- ElasticSearch – utilized as a logging solution
- Grafana – utilized as alerting solution
- Zappier – utilized for alerting

People

Gtmhub has staff organized in the following functional areas:

- CEO - who is responsible for defining the strategy and leading the company.
- COO - who is responsible for the management of the day-to-day operations of Gtmhub.
- CFO - who is responsible for managing the finance function, including financial accounting and reporting, tax submission and compliance, payroll, treasury and legal affairs.
- CTO - who is responsible for the oversight of all IT related hardware, software, configuration and security.
- VP, Software Engineering - who is responsible for the oversight of the software engineering team, its practices, deliverables, on-growing growth and development.
- Information Security Manager - who is responsible for the oversight of and adherence to the company's information security policies and procedures.
- Director of Product - who is responsible for the coordination of system feature development and enhancements, and ultimately the acceptor for completed work by the engineering team.
- Customer Success Manager - who is responsible for the onboarding of clients, support of clients, and fulfillment of operational processes and services to enable clients to realize the full value of the Gtmhub platform.

Procedures

The following provides a summary of policies maintained and documented by management personnel involved in the operation of the OKR Management SaaS System:

- Acceptable use
- Bring your own device
- Change management
- Data classification
- Data protection
- Data retention
- Encryption
- Incident response
- Information security
- IP rights
- Network security
- Paper and electronic media
- Password management
- Physical security

- Risk assessment
- Software development
- Vendor management

Control activities have been placed into operation to help ensure that actions are carried out properly and efficiently. Control procedures serve as mechanisms for managing the achievement of control activities, and are a part of the process by which Gtmhub strives to achieve its business objectives. Gtmhub has applied a top-down risk management approach to meet internal and regulatory compliance objectives. Gtmhub has an Information Security Manager that performs various risk management activities, including identifying, assessing, implementing and monitoring IT risks and controls for compliance with applicable trust services criteria in this report.

Data

Access to customer data in Gtmhub's OKR Management SaaS System is restricted to authorized IT users, explicitly clients approved Gtmhub Customer Success team members and customer personnel. Data for multiple clients reside within the same database, but is logically restricted by a combination of internal client and user identifiers. Data at rest is encrypted.

Gtmhub designs their backup and storage program to meet necessary business requirements and customer agreements. A comprehensive backup strategy is outlined in their operational policies and procedures and implemented by the IT department. A program has been developed and deployed to ensure that all system settings, production data, and test and development data is backed up, secured, and limited to authorized personnel. A full backup of the encrypted database is performed on a schedule from every 10 minutes to daily and delivered to an Amazon S3 where it is stored for 180 days. The backup schedule depends on the criticality of the database. Critical databases are backed up as often as every 10 minutes. Annual restoration tests are performed to ensure their ability to recover environments and data as needed.

Attachment B - Gtmhub's Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Gtmhub designs its processes and procedures related to its OKR Management SaaS System to meet its objectives. Those objectives are based on the service commitments that Gtmhub makes to user entities and the financial, operational, and compliance requirements that Gtmhub has established for the services provided.

Security commitments to user entities are documented in client agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the OKR Management SaaS System that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Use of encryption protocols to protect client data at rest and in transit.

Availability commitments to user entities are documented in client agreements. Availability commitments are standardized and include, but are not limited to, the following:

- Managing software, servers (including storage), network, internet and infrastructure capacity as is necessary to provide a commercially reasonable level of performance of the OKR Management SaaS System.
- Meeting Company objectives through authorization, design, development, and monitoring of data backup processes and recovery infrastructure.
- Support coverage, hours of availability, response times, and resolution times.

Gtmhub establishes operational requirements that support the achievement of security and availability commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Gtmhub'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 in the operation and development of the OKR Management SaaS System.

MARCUMGROUP

Marcum Group is a family of organizations providing a comprehensive range of professional services including accounting and advisory, technology solutions, wealth management, and executive and professional recruiting.

These organizations include:

- Marcum LLP
  www.marcumllp.com
- Marcum Bernstein & Pinchuk
  www.marcumbp.com
- Marcum Insurance Services
  www.marcumis.com
- Marcum RBK Ireland
  www.marcumrbk.com
- Marcum Search
  www.marcumsearch.com
- Marcum Strategic Marketing
  marketing.marcumllp.com
- Marcum Technology
  www.marcumtechnology.com
- Marcum Wealth
  www.marcumwealth.com

MARCUM
ACCOUNTANTS ▲ ADVISORS

Ben Osbrach, CISSP, CISA, QSA, CICP, National Risk Advisory Leader
813.397.4860 ● ben.osbrach@marcumllp.com

Mark Agulnik, CPA, CISA, CIS LI, JD, Regional Advisory Partner-in-Charge
954.320.8013 ● mark.agulnik@marcumllp.com