



Grazitti Interactive

Independent Practitioner's Trust Services Report for Digital Marketing
Automation Services including SearchUnify

For the Period March 01, 2019 to February 29, 2020

(SOC 3 Report)



SSAE Attestation Services

Independent Practitioner's Trust Services Report

To: Management of Grazitti Interactive (Grazitti)

We have examined Grazitti Interactive's (Grazitti) assertion related to "Description of Its Digital Marketing Automation Services including SearchUnify" system that, during the period March 01, 2019 to February 29, 2020, Grazitti maintained effective controls to provide reasonable assurance that:

- the system was protected against unauthorized access, use or modification;
- the system was available for operation and use as committed or agreed;
- information designated as confidential was protected by the systems as committed or agreed

based on the trust services criteria relevant to 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). This assertion is the responsibility of Grazitti's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Grazitti's relevant controls over security, availability and confidentiality (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, the Company's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct errors or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the systems or controls.

In our opinion, Grazitti management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability and confidentiality.

Manoj Jain, CPA
(Colorado Membership Number - 0023943)



March 25, 2020
Mumbai, India

Grazitti Management's Assertion

DocuSign Envelope ID: E5CA2CE8-B56C-413A-BD9F-85E724455255



March 25, 2020

During the period March 01, 2019 to February 29, 2020, Grazitti Interactive's (Grazitti) maintained effective controls over **Digital Marketing Automation Services and SearchUnify** (the "system"), to provide reasonable assurance that:

- the system was protected against unauthorised access, use or modification;
- the system was available for operation and use as committed or agreed;
- information designated as confidential was protected by the systems as committed or agreed

based on the criteria for security, availability and confidentiality set forth in the Description Criteria DC Section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (description criteria).

The attached system description identifies the aspects of the Description of Grazitti's "Digital Marketing Automation Services and SearchUnify" covered by the assertion.

DocuSigned by:
Alok Ramsisaria

Alok Ramsisaria
CEO
Grazitti Interactive

Plot No. 164, 198 & 271, Industrial Area Phase II, Panchkula-134113, India
Tel: +91 172 5048500, 5057200 Website: www.grazitti.com

Description of Grazitti Interactive’s Digital Marketing Automation Services including SearchUnify including SearchUnify and related processes throughout the period March 01, 2019 to February 29, 2020

Background and Overview of Services

Grazitti Interactive (Grazitti) is engaged in the business of providing marketing automation and cloud innovation services.

As a global consultancy, Grazitti Interactive has strategic partnerships with technology pioneers like Marketo, Salesforce, Google, Alteryx, Microsoft, Adobe, Lithium, Optimizely, Acquia, Shopify and Jive. They combine these platforms with their innovative approaches to provide effective, result-oriented solutions to clients. They have also been helping hundreds of global companies to transform their business technologies and save millions.

Grazitti is certified by ISO 27001:2013, PIMS (BS 10012) and HIPAA compliant.

Overview of SearchUnify

SearchUnify is an AI powered federated search product that lets users search and find relevant information across multiple platforms. It has features such as detailed analytics, granular level configuration and search tuning. SearchUnify is being used by many enterprises to help them leverage machine learning for enterprise search.

Subservice Organizations

Grazitti utilizes the following subservice providers for data center services that are not included in within the scope of this examination. However, Grazitti’s responsibilities for the applications and services run at these cloud services are covered as part of the audit and in scope. Responsibility matrix is defined as part of the SLA and agreements with these sub service organizations.

- **AWS – For Data Center Services**

AWS is a SOC 2 and SOC 3 attested organisation.

The Criteria that relate to controls at the subservice organizations included all criteria related to the control objectives of Security and Availability. The types of controls that are necessary to meet the control objectives and related criteria, either alone or in combination with controls at Grazitti include:

- The system is protected against unauthorized access (both physical and logical).
- The system is available for operation and use and in the capacities as committed or agreed.
- Policies and procedures exist related to security and availability and are implemented and followed.

Boundaries of the System

The specific products and services and locations included in the scope of the report are given below. All other products, services and locations are not included.

Products and Services in Scope

The scope of this report is limited to Grazitti Interactive and related support processes. This covers the following products and services.

Products

- SearchUnify
- M-Clean (MCN)
- M-Hive (MHV)
- ZakCalendar (ZCL)
- Salesforce-Jira Connector (Sinergify)
- Alteryx Connectors (ALC)
- Email to Case Advance (ECA)
- Jive-Salesforce KB Sync Connector (JSK)
- Lithium-Salesforce KB Sync Connector (LSK)
- Ideas Manager (IDM), Lithium Salesforce Case Connector (LSC)
- Marketo Connectors (WordPress Marketo Integration Connector (WMC), Magento Marketo Integration Connector (MMC), Drupal Marketo Integration Connector (DMC))

Services

- Marketing Automation
- Software development for marketing platforms and CRM's
- Development and deployment of connectors and plugins

Geographic Locations in Scope

Panchkula, India	Plot 198, Industrial Area, Phase 2, Panchkula, Haryana - 134113 India
Panchkula, India	Plot 164, Industrial Area, Phase 2, Panchkula, Haryana - 134113 India
Panchkula, India	Plot 271, Industrial Area, Phase 2, Panchkula, Haryana - 134113 India
Mohali, India (Effective From: Jan 2020)	Quark City - SEZ, Landmark Plaza (F-3 tower) A-40A, Phase VIII Extn., Industrial Focal Point, Mohali, Punjab, India (with approximately 25-30 employees)

All material activities and operations in scope are performed from the above four office locations. Unless otherwise mentioned, the description and related controls apply only to the location covered by the report.

Control Environment

Board of Directors

Business activities at Grazitti are under the direction of the Board of Directors. The company is governed by its Board of Directors headed by its promoter director Mr. Alok Ramsisaria as the CEO.

Neeta Ramsisaria is in charge of the company's India operations playing a key role in strategy and client management.

Risk Management and Risk Assessment

Risk assessments are performed annually to identify current risk levels, with recommendations to minimise those risks that are determined to pose an unacceptable level of risk to Grazitti. As part of this process, security threats are identified and the risk from these threats is formally assessed.

Information Security Policies

Grazitti has developed an organization-wide Information Security Policies. Relevant and important Security Policies (IS Policies) are made available to all employees via Google Drive folders. Changes to the Information Security Policies are reviewed by the IS Team and approved by CEO/CISO prior to implementation.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in business conditions. Grazitti management and Information Security personnel monitor the quality of internal control performance as a routine part of their activities.

Information and Communication

Grazitti has documented procedures covering significant functions and operations for each major work group. Policies and procedures are reviewed and updated based upon suggestions from security personnel and approval by management. Departmental managers monitor adherence to Grazitti policies and procedures as part of their daily activities.

Components of the System

Infrastructure

The infrastructure comprises physical and hardware components of the System including facilities, equipment, and networks.

Network Segmentation Overview

Grazitti's office is equipped with the latest hardware, software and networking infrastructure. Office is linked using high speed communication links, backed up by redundant networks.

Physical Access

Grazitti's Office power systems are designed to provide uninterrupted power, regardless of the availability of power from the local public utilities supplying the office premises, UPS units and backup generators supply power to the center in the event of a power failure. All components are covered by maintenance contracts and tested regularly. Generators are tested periodically.

Software

Firewalls

Firewall is configured and in place to protect IT resources. Firewall and switch configuration standards are documented. Firewall and switch configurations are reviewed by management on a quarterly basis.

Network & endpoint protection / monitoring

Access to Internet services from any company computing device (laptop, workstation, server etc.) or from any company address designation should be made through the company's approved perimeter security mechanisms. External connections to company servers is not permitted.

Monitoring

Grazitti has devised and implemented adequate monitoring controls to detect unauthorized information processing activities. Critical servers and systems are configured to log user activities, exceptions and information security events. System administrator and system operator activities are logged and reviewed on a periodic basis. We analyze logs generated by FW, IDS/IPS on a daily basis and figure out for any critical events.

Vulnerability Scans & Intrusion Detection/Intrusion Prevention

As per the Audit calendar, all the network devices and services are audited for vulnerabilities by doing periodic vulnerability scans. These scans are done by the system admin internally. Grazitti uses OpenVas for vulnerability scans. External VAPT is also performed by the third-party vendor every year.

Anti-virus software has been installed on all desktops & laptops within the scope. Updates to the virus definition files are managed and downloaded by the software itself on a daily basis from the vendor website at specific intervals.

People

Organizational Structure

The organizational structure of Grazitti provides the overall framework for planning, directing, and controlling operations. It has segregated personnel and business functions into functional groups according to job responsibilities. This approach helps enable the organization to define responsibilities, lines of reporting, and communication, and helps facilitate employees to focus on the specific business issues impacting Grazitti clients.

New Hire Procedures

New employees are required to read HR corporate policies and procedures and are provided online access to these policies. Hiring procedures require that the proper educational levels have been attained along with required job-related certifications, if applicable, and industry experience. If a candidate is qualified, interviews are conducted with various levels of management and staff.

Code of Conduct and Disciplinary Action

Grazitti has put forward the Code of Conduct and Disciplinary Process in-order to encourage and maintain standards of conduct and ensure consistent and fair treatment for all

Procedures

IT policies and operating instructions are documented. Procedures described cover server management, server hardening, workstation security system, network management, security patch management, user creation, system audit, ID card activation, etc. Additionally, production and training standard operating procedures are available.

Change Management

Grazitti has implemented a well-defined Change management process to ensure that all changes to the information processing facilities, including equipment, supporting facilities and utilities, networks, application software, systems software and security devices are managed and controlled. The Change Management process describes a methodical approach to handle the changes that are to be made. All the changes need to be subjected to a formal Change Management process.

Incident Response and Management

Procedures for the incident response including identification and escalation of security breaches and other incidents are included in the policy. Root-cause analyses of all the incidents are performed and the root cause identified shall remedy and reported. The actions proposed from the root-cause analysis is reviewed and approved by CISO.

Logical Access

Access to resources is granted to an authenticated user based on the user's identity through a unique login ID that is authenticated by an associated password. Assets are assigned owners who are responsible for evaluating the appropriateness of access based on job roles.

Administrative Level Access

Administrative rights and access to administrative accounts are granted to individuals that require that level of access in order to perform their jobs. All developers in the Grazitti application development team have admin rights by default in order to install software required for their day to day job. All administrative level access, other than to the IT team and dev team, must be justified to and approved by the IT team.

Confidentiality

Secure procedures are established to ensure safe and secure disposal of media when no longer required. The level of destruction or disposal of media would depend on the information or data stored in the media and the criticality of the information as per the information classification guideline.

Backup and Recovery of Data

Grazitti has developed formal policies and procedures relating to backup and recovery. Backup policy is defined in the Backup Policy. Suitable backups are taken and maintained.