A-LIGN

xMatters, Inc.
an Everbridge Company

Type 2 SOC 3

2023

everbridge™
xmatters

A-LIGN.COM

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

October 1, 2021 to March 31, 2023

Table of Contents

SECTION 1

ASSERTION OF XMATTERS, INC. AN EVERBRIDGE COMPANY MANAGEMENT

ASSERTION OF XMATTERS, INC. AN EVERBRIDGE COMPANY MANAGEMENT

May 18, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within xMatters, Inc. an Everbridge Company's ('xMatters' or 'the Company') xMatters Platform throughout the period October 1, 2021 to March 31, 2023, to provide reasonable assurance that xMatters' service commitments and system requirements were achieved 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*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "xMatters, Inc. an Everbridge Company's Description of Its xMatters Platform throughout the period October 1, 2021 to March 31, 2023" 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 October 1, 2021 to March 31, 2023, to provide reasonable assurance that xMatters' service commitments and system requirements were achieved based on the trust services criteria. xMatters' objectives for the 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 "xMatters, Inc. an Everbridge Company's Description of Its xMatters Platform throughout the period October 1, 2021 to March 31, 2023".

xMatters uses Google Cloud Provider ('GCP' 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 xMatters, to achieve xMatters' service commitments and system requirements based on the applicable trust services criteria. The description presents xMatters' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of xMatters' 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 and operating effectively are necessary to achieve xMatters' service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of xMatters' 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 October 1, 2021 to March 31, 2023 to provide reasonable assurance that xMatters' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of xMatters' controls operated effectively throughout that period.

Karen Meohas

Karen Meohas
Senior Director of Global Compliance
xMatters, Inc. an Everbridge Company

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To xMatters, Inc. an Everbridge Company:

Scope

We have examined xMatters' accompanying assertion titled "Assertion of xMatters, Inc. an Everbridge Company Management" (assertion) that the controls within xMatters Platform were effective throughout the period October 1, 2021 to March 31, 2023, to provide reasonable assurance that xMatters' service commitments and system requirements were achieved 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*, in AICPA *Trust Services Criteria*.

xMatters uses GCP 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 xMatters, to achieve xMatters' service commitments and system requirements based on the applicable trust services criteria. The description presents xMatters' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of xMatters' controls. 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 indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at xMatters, to achieve xMatters' service commitments and system requirements based on the applicable trust services criteria. The description presents xMatters' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of xMatters' controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

xMatters 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 xMatters' service commitments and system requirements were achieved. xMatters has also provided the accompanying assertion (xMatters assertion) about the effectiveness of controls within the system. When preparing its assertion, xMatters 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 Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization'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 AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management'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 the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its 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.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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 xMatters Platform were suitably designed and operating effectively throughout the period October 1, 2021 to March 31, 2023, to provide reasonable assurance that xMatters’ service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of xMatters’ controls operated effectively throughout that period.

The SOC logo for Service Organizations on xMatters’ website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of xMatters, user entities of xMatters Platform during some or all of the period October 1, 2021 to March 31, 2023, business partners of xMatters subject to risks arising from interactions with the xMatters Platform, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements.

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

A-LIGN ASSURANCE

Tampa, Florida
May 18, 2023

SECTION 3

XMATTERS, INC. AN EVERBRIDGE COMPANY’S DESCRIPTION OF ITS XMATTERS PLATFORM THROUGHOUT THE PERIOD OCTOBER 1, 2021 TO MARCH 31, 2023

OVERVIEW OF OPERATIONS

Company Background

xMatters, Inc. is an Everbridge Company (“xMatters”). xMatters offers a Software as a Service (SaaS) platform that allows its clients to manage and communicate Information Technology (IT) incidents internally, as well as to support and manage communication as part of business continuity plans.

In May 2021, xMatters was acquired by Everbridge Inc, a global software company that provides enterprise software applications across the critical events space. This acquisition has not only strengthened xMatters and Everbridge’s position in the mass notification arena but also provided a platform for a stronger and more robust security, privacy and compliance posture for their combined customers.

Description of Services Provided

The xMatters system offers the following services:

- Incident Management enables response to service interruptions across teams, cultures, and systems, and includes the following features:
  - Automated Resolution
  - Dynamic Collaboration
  - Data-Driven Process Improvements
  - Scalable, Service-Centric Model
- IT Event Management filters and prioritizes the most important system alerts and includes the following features:
  - Filtering and Suppression
  - Alert Correlation
  - Enriched Notifications
  - Context-Based Routing
  - Prioritization
- Integration Platform enables collaboration between people, data, and tools to resolve issues and includes the following features:
  - Orchestrated Toolchains
  - Hybrid Cloud Support
  - Integration Builder
  - Built-In Integrations
- Flow Designer enables integration, synchronization, and automation of toolchains and includes the following features:
  - IT Ops
  - DevOps & Site Reliability Engineer (SRE)
  - Major Incident Management
- Smart Notifications condense alert information from monitoring and issue-tracking tools in actionable notifications and include the following features:
  - Resolutions Actions
  - Situational Context
  - Stakeholder Alignment
  - Major Incident Coordination
  - Conference Call Engagement
- On-Call Management tracks schedules and shifts to ensure that issues are sent to appropriate personnel and includes the following features:
  - Coverage & Scheduling Calendar
  - Escalations
  - User Self-Service
  - Data Synchronization

- Workflow & Process Automation orchestrates and automates key resolution processes to drive efficiency and includes the following features:
    - Orchestrated Toolchain Resolution
    - Structured Communication Plans
    - Scenario Management
    - Post-Mortem Analysis
- Performance Analytics provide the insights and visibility into customer-facing incidents, digital service downtime, or unmanaged responses to critical issues and include the following features:
    - Incident Timeline
    - Real-Time Event Visibility
    - Instant Replay of Events
    - Team Performance
- Enterprise Grade Architecture drives data ingestion, event processing, and user management to fulfill support needs and includes the following features:
    - Data Security & Reliability
    - Globally Distributed Cloud Infrastructure
    - Hybrid Environment Interoperability
    - Role-Based Access and Administration
    - Scalable Group Management
    - Uptime Guarantees

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of xMatters. based on Service Agreements.

xMatters establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in xMatters' system policies and procedures, system design documentation, and contracts with clients.

xMatters principal service commitments and system requirements include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• xMatters will implement appropriate technical and organizational measures to protect client data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the data (a “security incident”) • xMatters will implement measures to remedy or mitigate the effects of a security incident and to keep the client informed of all developments of such an event	• Access controls for access to all systems and data • Risk assessments • Change management controls • Encryption standards • Logging and Monitoring • Secure Development Life Cycle

Trust Services Category	Service Commitments	System Requirements
Availability	• xMatters will ensure 24/7/365 technical support availability • xMatters will ensure 99.95% or greater availability of its Production systems and services. xMatters will implement measures to remedy or mitigate the effects of an availability incident and to keep the client informed of all developments of such an event	• Business Continuity Management System • Monitoring controls • Backup and recovery standards • Disaster recovery plan
Confidentiality	• xMatters will not disclose any confidential information to any person or entity other than the representatives of xMatters who have a need to know such information in the course of the performance of their duties • Upon any termination of services, xMatters will continue to maintain the confidentiality of the customer's confidential information and, upon request and to the extent practicable, destroy all materials containing such confidential information • xMatters will notify the customer if xMatters becomes aware of a breach of confidentiality • xMatters will protect the customer's confidential information in the same manner that it protects its own confidential information, but in no event using less than reasonable care	• Data classification • Retention and destruction policy • Non-disclosure agreements (NDAs) • Employee training • Employment agreements

Components of the System

Infrastructure

xMatters utilizes Google Cloud Platform (GCP) to provide the resources to host the infrastructure. xMatters leverages the experience and resources of GCP to support the scalability, availability, and durability of the xMatters platform.

xMatters cloud-based SaaS operates within different economic regions with data centers located at:

- European Union: London (europe-west2) and Germany (europe-west3)
- Asia-Pacific: Sydney, Australia (australia-southeast1) and Singapore (asia-southeast1)
- North America: Moncks Corner, South Carolina (us-east1) and Council Bluffs, Iowa (us-central1)

Primary infrastructure used to provide xMatters Platform includes the following:

Primary Infrastructure	
Production Service	**Business Function**
Compute Engine	Virtual Machine hosting

Primary Infrastructure	
Production Service	**Business Function**
Kubernetes Engine	Kubernetes Infrastructure
Cloud Storage	Data storage
Load Balancing	Global load balancing services
Cloud Run	Container hosting
Pub/Sub	Queueing services

Software

Primary software used to provide xMatters Platform includes the following:

Primary Software	
Production Application	**Business Function**
Atlassian (Jira and Confluence)	Development Projects and service management
Mailgun Technologies	Primary provider of e-mail notifications to users of the xMatters platform
Twilio	Twilio is their primary provider of voice conferencing and SMS services to users of the xMatters platform, and secondary provider of voice notifications. Twilio's service redundancy allows it to failover to their own alternative data centers
SendGrid	Twilio (SendGrid) is their primary and secondary provider of inbound integrations via the 'E-mail Initiation' service. It is also their secondary provider of e-mail notifications. Twilio's service redundancy allows it to failover to their own alternative data centers
Zendesk	Zendesk is used to track and communicate all customer interaction with the technical support team. Publishing external knowledgebase articles for customers to view and manage content. Manage internal incident handling. Provisioning new and current customers. Manage customer access requests
Sophos	Antivirus
One Login	Single sign on service
Prometheus	Monitoring and alerting
Wazuh	Intrusion detection system (IDS), monitoring and alerting
xMatters Application	Solution for IT managers, incident notification and escalation
Splunk	Application logging
Jira	Bug and feature tracking
PostgreSQL	Data storage
GlobalProtect	Virtual Private Network (VPN)

People

xMatters is comprised and supported by the following teams responsible for the delivery and management of the xMatters SaaS:

- Engineering: Responsible for the development, testing, deployment, and maintenance of new code for xMatters
- Operations: Responsible for managing access controls, monitoring the infrastructure, and maintaining the security of the production environment
- Product Management: Responsible for overseeing the product life cycle, including adding new product functionality
- Compliance and Legal Team: Responsible for ensuring the integrity, availability, and confidentiality of customer data is protected at every stage of the product life cycle and across all Company processes
- Information Security Team: Supports xMatters platform by monitoring internal and external security threats and maintaining security systems including malware and antivirus as required
- People and Culture Department: Defines policies and procedures for recruitment and termination of employment including initiating the instruction to remove access
- Corporate IT: Responsible for implementing and maintaining internal network security and access control requirements

Data

xMatters maintains a formal documentation (e.g., Information Handling Policy and Data Processing Agreement) to guide its data collection, handling, and retention requirements, and these documents are maintained and implemented in compliance with the organization’s required regulations.

The organization’s formal Cryptographic and Key Management Policy outlines its requirements regarding its use and management of encryption keys. The organization manages its server-side encryption keys and encrypts client data at rest using Advanced Encryption Standard (AES)-256, and transport layer security (TLS) v1.2 is used to encrypt all data at rest and in transit. xMatters encrypts all its passwords at rest and in transit using an encryption solution and secure sockets layers (SSL).

xMatters maintains formal Policies and Processes that governs its use and handling of client data, and the organization securely processes, stores, and transmits client data that is used to support its services delivered. A formal data flow diagram is used to illustrate the flow of client data throughout the organization’s systems, and this diagram is reviewed, updated, and approved annually and as needed upon significant change.

Processes, Policies and Procedures

Policies and procedures are in place and include the automated and manual procedures involved in the operation and maintenance of xMatters. These include those relating to product management, engineering, technical operations, security, and IT. These procedures are drafted in alignment with the overall information security policies and include Business Continuity, Vulnerability Management, Third-party qualification, Physical Security, Operations Security, Asset Management, Cryptography, Access Control, and Acceptable Use. All policies are updated and approved as necessary for changes in the business, but no less than annually. All teams are expected to adhere to the Everbridge and xMatters policies that define how services should be delivered. These are located on xMatters’ shared drive and Everbridge’s Intranet and can be accessed by any xMatters team member.

The following table details the procedures as they relate to the operation of xMatters:

Procedure	**Description**
Access Control	How xMatters restricts logical access, provides and removes that access, and prevents unauthorized access.
Operating Procedures for Information and Communication Technology (ICT)	How xMatters manages the operation of the system and detects and mitigates processing deviations, including logical security deviations.
Change Management	How xMatters identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How xMatters identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.
Secure Development	How xMatters defines rules to ensure that information security is taken into account throughout the entire development life cycle, resulting in secure software and systems.
Cryptographic Controls	How xMatters ensures the proper and effective use of cryptographic controls in order to protect the confidentiality, authenticity, and integrity of information.
Business Continuity	How xMatters establishes the steps necessary to implement business continuity management for the xMatters product.

Physical Security

Everbridge Head Office (Burlington, MA) and xMatters Office (Victoria, BC, CA) have physical security measures that are designed to deny unauthorized access to equipment, resources ,and to protect personnel and property from damage or harm.

The organization’s sensitive areas are secured via door locks, keycard access controls, physical intrusion detection systems, visitor access control procedures, employee ID badges, and video surveillance systems. xMatters uses keycard access control systems and badge readers to restrict access to its facilities, and these employee badges and key cards are assigned to personnel using the principle of least privilege.

The company manages its surveillance systems, access controls systems, and alarms. The organization’s facilities are monitored by security surveillance camera systems, with cameras monitoring all ingress and egress points and sensitive areas.

Visitors to the facilities are required to complete an entry in its visitor logs, which document all relevant details regarding the visitor.

Logical Access

Access Control

The onboarding process is initiated by the People and Culture team after the employee completes a successful background check. User accounts are provisioned by Everbridge Corporate IT team according to the Access Control Policy.

Each user has a unique identifiable user account. Access to all systems, networks, services, and information is forbidden unless expressly permitted to individual users or business roles. Password complexity is managed in accordance with Everbridge Access Control Procedure as part of the Information Security Management System (ISMS) and multi-factor authentication (MFA) is required for all users.

Privileged user access

A privileged user has access to make changes to the production environment. Privileged access rights are restricted and controlled. Privileged rights are allocated to users for ongoing access (on a need-to-use basis) or for temporary access (on an event-by-event basis).

Privileged access is granted upon revision and approval:

- To the infrastructure management role that requires it
- Temporarily, during an event which requires the delegation of access (e.g., a security incident which needs prompt investigation)

Requests for new privileged access must be made to the asset owner in writing so that a record is kept. All privileged logins into the production environment are logged.

Requests for new privileged access must be made to the asset owner in writing so that a record is kept.

The asset owner approves access based on the above guidelines and, if in doubt, consults the Information Security Manager (ISM). All privileged access to assets, other than by the asset owner, must be recorded by the asset owner or ISM, including any changes to privileged access (addition or removal).

User Account Revocation

Upon termination of employment or an external party contract, the People and Culture Department immediately initiates the removal of all access rights granted to the party in question to avoid unauthorized access by ex-employees or ex-contractors. The following is performed when revoking user access:

- Collecting physical assets allocated to the user (e.g., laptop, office key)
- Removing access to the password management system
- Removing application user accounts by their asset owners
- Removing or suspending the user's user ID (e.g., e-mail address)
- Updating access right records to reflect the changes

User Access Review

xMatters reviews user access on a quarterly basis. When these events are triggered, the employee account is checked for any irregularities in access rights, and access rights are amended or removed, as necessary.

When reviewing the access rights of an asset, the asset owner should consider:

- Whether the current users' access rights match their current role and access profile
- If redundant user access is removed
- Whether privileged access that is no longer needed is removed

Network Access

When considering logical access to xMatters systems, xMatters differentiates between the corporate office network and the hosted (cloud) infrastructure. There is no permanent connection between the office and the cloud infrastructure, and logical access to these networks is managed independently.

Cloud Infrastructure Access

The cloud infrastructure has been divided into development, testing, and production instances. The instances serve as permission boundaries and resources from one instance cannot access resources in another instance. Permission is assigned as described in the Access Control section above. Logical connectivity is controlled by a combination of internal protocol (IP) address filtering and authentication.

Computer Operations - Backups

The organization maintains a formal backup and testing process to ensure that its regularly scheduled system backups enable the full recovery of systems in the event of a disaster. xMatters performs full-system backups daily, and backups are retained for seven days to allow review and recovery. The performance of these backups is tracked and logged to ensure completion. The organization's system backups are encrypted to ensure security and appropriate access.

Computer Operations - Availability

The availability category refers to the accessibility of the system or services as committed by xMatters' Master Service Agreement (MSA). xMatters is dependent on many aspects of xMatters' operations. The risks that would prevent xMatters from meeting its availability commitments and requirements are diverse. Availability includes consideration of risks during normal business operations, during routine failure of elements of the system, as well as risks related to the continuity of business operations during a natural or man-made disaster.

xMatters has designed its controls to address the following availability risks:

- Insufficient processing capacity
- Loss of processing capability due to a power outage
- Loss of communication with user entities due to a break in telecommunication services
- Loss of key processing equipment, facilities, or personnel due to a natural disaster
- Primary datacenter outage
- Cyberattack
- Among others

In order to mitigate any identified availability risks, xMatters uses GCP services to ensure that every component of xMatters infrastructure is fault tolerant through use of both redundancy and resiliency.

GCP and other external tools continually monitor the system and send alerts to the technology teams when configured thresholds are exceeded. This can assist in ensuring that capacity is sufficient for the number of customers.

Change Control

xMatters formal Change Management Policy and Process are used to approved, document, and implement all changes to the organization's standards, systems, and assets. This documents are reviewed, updated, and approved annually. The organization tracks and documents all necessary changes within its internal ticketing system and change request tickets are used to propose new changes. Each change request ticket documents the following information and attributes regarding the proposed change:

- Clearly identified roles and responsibilities
- Impact or risk analysis of the change request
- Testing prior to the implementation of the change
- Evaluation of the change for potential costs
- Authorization and approval of the change

Data Communications

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. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the GCP data center 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.

In-scope workstations are protected by virus protection software. The software is configured to perform updates to the list of known threats and to protect data from infection by malicious code or viruses in real time.

Penetration testing is conducted annually to identify vulnerabilities in the environment.

Vulnerability scanning is performed by Veracode on a quarterly basis at a minimum.

Boundaries of the System

The scope of this report includes xMatters Platform performed in the Victoria, British Columbia and Burlington, Massachusetts facilities.

The scope of this report does not include the cloud hosting services provided by GCP at multiple facilities.

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 review 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 review period.

Criteria Not Applicable to the System

All Common/ Security, Availability, and Confidentiality criterion was applicable to xMatters Platform.

Subservice Organizations

This report does not include the cloud hosting services provided by GCP at multiple facilities.

Subservice Description of Services

xMatters uses GCP as a subservice organization for SaaS provider. Complementary Subservice Organization Controls are expected to be in place at GCP related to physical security and environmental protection.

Complementary Subservice Organization Controls

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

The following subservice organization controls have been implemented by GCP to provide additional assurance that the trust services criteria are met:

Subservice Organization - GCP		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.1	Audit logs are continuously monitored for events related to security, availability, processing integrity, and confidentiality threats. Alerts are generated for further investigation.
		Security event logs are protected and access is restricted to authorized personnel.
		The organization has established formal guidelines for passwords to govern the management and use of authentication mechanisms.
		The organization has an established policy specifying that access to information resources, including data and the systems which store or process data, is authorized based on the principle of least privilege.
		External system users are identified and authenticated via the Google Accounts authentication system before access is granted.
	CC6.4; CC7.2	Physical protection and guidelines are described in the Physical Security Policy, Data Security Policy, Google Photography Policy, and the Data Center Access policy.
		Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge readers, secondary identification mechanisms, and/or physical locks.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of their visit.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.

Subservice Organization - GCP		
Category	**Criteria**	**Control**
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.
		Visitors to corporate offices must be authenticated upon arrival and remain with an escort for the duration of their visit.
	CC7.2	Audit logs are continuously monitored for events related to security, availability, processing integrity, and confidentiality threats. Alerts are generated for further investigation.
		Security event logs are protected and access is restricted to authorized personnel.
		The organization has a security guideline that requires users to lock their workstations and mobile devices when unattended. Access to unattended workstations is prevented by a password protected screen-saver after 15 minutes of inactivity.
Availability	A1.2	Critical power and telecommunications equipment in data centers is physically protected from disruption and damage.
		Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).
		Data centers are equipped with fire detection alarms and protection equipment.
		The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.

xMatters management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, xMatters performs monitoring of the subservice organization controls, including the following procedures:

- Communicating with vendors and subservice organization(s) to monitor compliance with the service agreement and stay informed of changes planned at the hosting facility and relay any issues or concerns to GCP management
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring the services performed by vendors and subservice organization(s) to determine whether operations and controls expected to be implemented are functioning effectively

COMPLEMENTARY USER ENTITY CONTROLS

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

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services 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 having policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by xMatters according to contractually specified time frames.
2. User entities are responsible for controls to provide reasonable assurance that xMatters is notified of changes in user entity vendor security requirements and the authorized users list.
3. User entities are responsible for having policies and procedures to inform their employees and users that their information or data is being used and stored by xMatters.
4. User entities are responsible for having policies and procedures to determine how to file inquiries, complaints, and disputes to be passed on to xMatters.
5. User entities are responsible for granting access to xMatters' system to authorized and trained personnel.
6. User entities are responsible for controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by xMatters.
7. User entities are responsible for deploying physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.