xMatters, Inc.

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security and Availability categories for the period of April 1, 2020 through September 30, 2020.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

ASSERTION OF XMATTERS, INC. MANAGEMENT

ASSERTION OF XMATTERS, INC. MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within xMatters, Inc.'s Incident Management Software as a Service (SaaS) system (system) throughout the period April 1, 2020, to September 30, 2020, to provide reasonable assurance that xMatters, Inc.'s service commitments and system requirements relevant to Security and Availability were achieved. Our description of the boundaries of the system is presented in section 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 system throughout the period April 1, 2020, to September 30, 2020, to provide reasonable assurance that xMatters, Inc.'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*). xMatters, Inc.'s 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 section 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 system were effective throughout the period April 1, 2020, to September 30, 2020, to provide reasonable assurance that xMatters, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR'S REPORT

Karen Meohas
Information Assurance Manager
xMatters, Inc.
12647 Alcosta Boulevard, Suite 425
San Ramon, CA 94583

Scope

We have examined xMatters, Inc.'s accompanying assertion titled "Assertion of xMatters, Inc. Management" (assertion) that the controls within xMatters, Inc.'s incident management software as a service system (system) were effective throughout the period April 1, 2020, to September 30, 2020, to provide reasonable assurance that xMatters, Inc.'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*).

Service Organization's Responsibilities

xMatters, Inc. is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that xMatters, Inc.'s service commitments and system requirements were achieved. xMatters, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, xMatters, Inc. 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 whether 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 American Institute of Certified Public Accountants. 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 controls were not effective to achieve xMatters, Inc.'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 xMatters, Inc.'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 xMatters, Inc.'s incident management software as a service system were effective throughout the period April 1, 2020, to September 30, 2020, to provide reasonable assurance that xMatters, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

October 28, 2020

XMATTERS, INC.'S DESCRIPTION OF ITS INCIDENT MANAGEMENT SOFTWARE AS A SERVICE SYSTEM

SECTION A:
XMATTERS, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS INCIDENT MANAGEMENT SOFTWARE AS A SERVICE SYSTEM

Services Provided

xMatters, Inc. (xMatters) offers a 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. The organization 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 & 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

Infrastructure

xMatters maintains an accurate inventory of its systems and assets, and it reviews and compares its inventory using centrally managed systems. This inventory includes virtual systems, and items in this inventory are categorized as critical or non-critical.

xMatters also maintains formal network diagrams and a Separation in Operation document that illustrates its networks, systems, and the separation of its environments. These diagrams are reviewed, updated, and approved annually and as needed, and the Information Assurance Team and Cloud Architect are responsible for these documents.

xMatters' system is hosted within Google Cloud Platform (GCP), which ensures secure access to infrastructure. Multiple economic regions within the GCP data center are used to house and process client data. Client instances are secure, and xMatters ensures 24/7 technical support is in place.

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. Two annual, comprehensive risk assessments are performed based on ISMS methodology and Data Processing Impact Analysis (DPIA) methodology. All identified risks are logged in a centralized Governance, Risk and Compliance (GRC) system and assigned a rating that is updated following the performance of risk mitigation activities. Annual third-party audits of xMatters' internal infrastructure are conducted.

Software

xMatters utilizes various tools for Inventory Management; Log Monitoring; GRC Management Solution; Antivirus; Endpoint Protection; Vulnerability Scanning; and Project Management. Additionally, xMatters maintains a complete software inventory that is reviewed, updated, and approved annually, or as needed. The inventory is managed using a GRC Management Solution. Many of the software applications used by the organization are SaaS platforms and xMatters' critical software in use include the following:

- Aspect
- Bitbucket
- Clickatell
- Confluence
- Google Cloud Platform (GCP)
- Jira
- Mailgun
- Microsoft Office
- Open Market
- SendGrid
- Twilio
- Veracode
- Zendesk

People

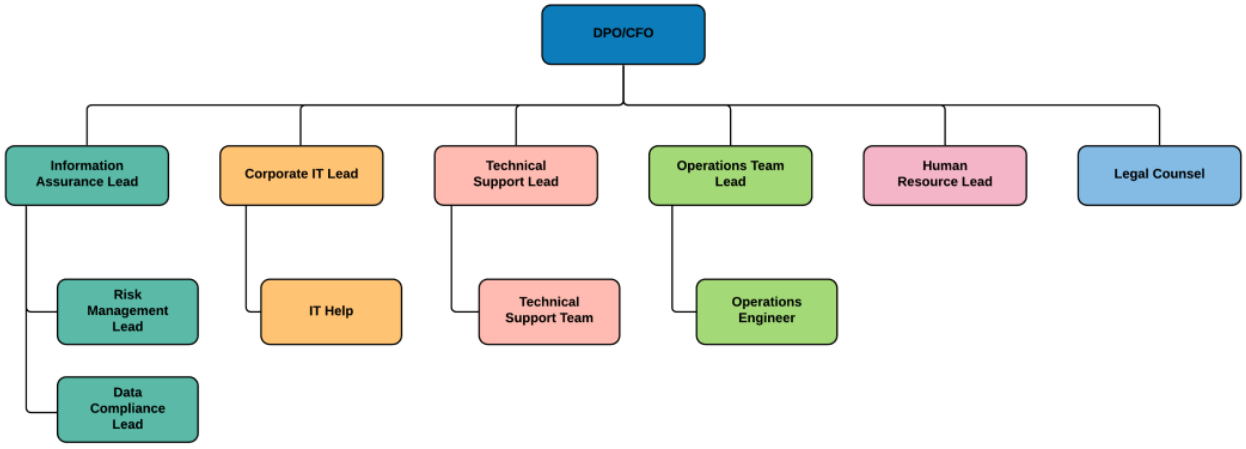
The organization has established a board of directors that is responsible for the oversight and stewardship of xMatters, represents the interests of its shareholders, is responsible for the strategy, direction, and financial health of xMatters, and retains responsibility for all corporate governance. The board of directors is comprised of two sub-committees, the independent Audit Committee and the Compensation Committee, and these committees maintain separate roles and responsibilities used to govern different facets of xMatters.

The organization has also established an Information Security Management System (ISMS) Steering Committee that is responsible for maintaining independence from executive management and ensuring that best practices and necessary compliance controls are implemented. The ISMS Steering Committee is comprised of multiple roles with respective responsibilities, including the following:

- Data Protection Officer (DPO) – supports and enables xMatters Privacy, Risk Management, and Security programs
- Operations Team Lead/Cloud Architect – leads the creation of a technology framework and providing technical leadership in support of xMatters initiatives in cloud computing and automation
- Human Resources – maintains all administrative policies and procedures for xMatters employees, including background checks, onboarding, and employment termination
- Director of Technical Support – provides customer-focused support for SaaS availability
- Legal Counsel – administers relevant documentation pertaining to privacy and security, including Confidentiality and Non-Disclosure Contracts, Master Service Agreements (MSAs), Data Processing Agreements (DPAs), etc.

- Director of Corporate IT – ensures the definition of appropriate technical architecture and ensures appropriate compliance monitoring
- Information Assistance Team
    - Information Assurance Manager – owns the Security Program, reports to the DPO, and serves as management's representative for ensuring the success and sustainability of information security deployment
    - Risk Management Analyst – reviews internal items related to risks and vulnerabilities
    - Data Compliance Analyst – reviews activity related to data compliance and associated best practices

A formal organizational chart (below) is maintained that illustrates xMatters' functional structure and represents its ISMS. This chart illustrates the hierarchy and clear reporting lines of the organization.



Data

xMatters maintains a formal privacy notice to guide its data collection, handling, and retention requirements, and this policy is 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 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 govern the use (handling) of client data for secure processing, storing, and disclosure of data for service purposes. A formal data flow diagram is used to illustrate the flow of client data throughout the organization's systems. The diagram is reviewed, updated, and approved annually and as needed upon significant change.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Acceptable Use Policy
- Access Control Policy
- Business Continuity Plan
- Business Impact Analysis
- Cloud Security Hardening Standards
- Competence and Training Process
- Corporate IT Hardening Standards
- Cryptographic and Key Management
- Data Classification and Configuration
- Data Deletion Process
- Data Incident Response Plan
- Data Loss Prevention
- Data Retention Policy
- Disaster Recovery Plan
- Human Resources/Employment Processes
- Incident Response
- Installation of Software
- Logging and Monitoring
- Patch Management
- Risk Management Process
- Security Log Reviews
- Supplier Assessment and Monitoring
- Vulnerability Management

SECTION B:
PRINCIPLE SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Regulatory Commitments

xMatters has formally acknowledged its compliance with the General Data Protection Regulation (GDPR), Australian Privacy Act, California Consumer Privacy Act (CCPA) and Personal Information Protection and Electronic Documents Act (PIPEDA). Privacy law compliance is audited annually by an independent third party. Personnel are required to review and acknowledge consent to the organization's applicable regulations and requirements. Annual privacy training is required to be completed by personnel.

Contractual Commitments

xMatters executes contracts with its clients outlining organizational and client responsibilities, including security breach reporting requirements. Contractual commitments also detail security and confidentiality of data, data retention and deletion, controlling access to data, transparency, and limiting the use of sub-processors to approved third parties. The organization employs service-level agreements (SLAs) with all clients and third parties, and xMatters uses publicly available status pages to externally communicate its uptime performance and services provided.

System Design

xMatters designs its Incident management SaaS system to meet its regulatory and contractual commitments. These commitments are based on the services that xMatters provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that xMatters has established for its services. 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, contracts with clients, and its xMatters Trust Portal (website) and Support Portal.