dmarcian, Inc.

Independent Service Auditor's Report on Controls at a Service Organization Relevant to Security, Availability and Privacy Trust Services Criteria on the DMARC Management Platform (SOC 3)

For the period January 1, 2021 to September 30, 2021

An Independent Service Auditor Report issued by
Dixon Hughes Goodman LLP

table of contents

section I: independent service auditor's report

To: Management of dmarcian, Inc.
Brevard, NC

Scope

We have examined the dmarcian, Inc. ("dmarcian") accompanying assertion titled "management's assertion" (assertion), that the controls within its DMARC Management Platform (system) were effective throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that dmarcian's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and privacy (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*).

dmarcian uses subservice organizations to provide data center services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at dmarcian, to achieve dmarcian's service commitments and system requirements based on the applicable trust services criteria. The description presents dmarcian's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of dmarcian's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, 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 dmarcian, to achieve dmarcian's service commitments and system requirements based on the applicably trust services criteria. The description presents dmarcian's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of dmarcian's 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

dmarcian 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 dmarcian's service commitments and system requirements were achieved. In Section II, dmarcian has also provided the accompanying assertion titled "management's assertion" (assertion) about the effectiveness of controls within the system. When preparing its assertion, dmarcian 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

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 dmarcian'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 dmarcian'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 dmarcian's DMARC Management Platform were effective throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that dmarcian's service commitments and system requirements were achieved based on the applicable trust services criteria, and is fairly stated, in all material respects.

Dixon Hughes Goodman LLP

Greenville, SC
December 3, 2021

section II: management's assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within dmarcian's DMARC Management Platform (system) throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that dmarcian's service commitments and system requirements relevant to security, availability, and privacy were achieved. Our description of the boundaries of the system is presented in Section III 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 January 1, 2021 to September 30, 2021, to provide reasonable assurance that dmarcian's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, 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*). dmarcian'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 III.

dmarcian uses subservice organizations to provide data center services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at dmarcian, to achieve dmarcian's service commitments and system requirements based on the applicable trust services criteria. The description presents dmarcian's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of dmarcian's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at dmarcian, to achieve dmarcian's service commitments and system requirements based on the applicable trust services criteria. The description presents dmarcian's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of dmarcian'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 January 1, 2021 to September 30, 2021, to provide reasonable assurance that dmarcian's service commitments and system requirements were achieved based on the applicable trust services criteria.

dmarcian, Inc.

section III: management's description of its system and controls

Background and Overview of Operations

This report only covers the services provided by dmarcian, Inc. and their DMARC Management Platform.

Founded in 2012 by one of the primary authors of the Domain-based Message Authentication, Reporting & Conformance (DMARC) specification, dmarcian is dedicated to upgrading the entire world's email by making DMARC accessible to all. dmarcian has global operations and staff in seven different countries. From small governmental organizations to Fortune 500 companies, dmarcian has an international track record for helping organizations across the globe and of all sizes successfully deploy DMARC.

dmarcian brings together thousands of senders, vendors, and operators in a common effort to build DMARC into the email ecosystem. Our customers range from banks, top internet properties, governments, marketing agencies, telecoms and commercial enterprises of all sizes. dmarcian users enjoy access to expert support, powerful tools, human friendly articles & videos, and a growing global network of DMARC deployment partners. dmarcian has offices around the world in key locations of North America, Canada, Europe and Asia Pacific. dmarcian prides itself on being a champion of DMARC and partners with organizations such as the Global Cyber Alliance (GCA), Online Trust Alliance (OTA), Certified Senders Alliance (CSA), Anti-Phishing Working Group (APWG), and the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG).

dmarcian's purpose is to spread DMARC far and wide by increasing accessibility, advocacy, and thought leadership. We achieve this by focusing on the people doing the work and helping them make the world of email and the greater world a better place for all.

DMARC Management Platform

dmarcian's DMARC Management platform receives, processes and classifies mail observed from users' domain namespace and makes sense of it for the user. The native Extensible Markup Language (XML) format in which DMARC data is transmitted is not intended for human consumption. The Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) standard are security mechanisms which prevent unauthorized individuals from sending emails on a user's behalf. Our platform visualizes the data in powerful and meaningful ways so you can quickly identify authentication gaps (SPF/DKIM) and unauthorized use of your domains.

In addition to aggregating DMARC data, our platform provides domain administration teams with the necessary features to adopt DMARC with clarity and confidence. The dmarcian reporting platform sits atop as an accurate source classification engine in the industry and affords users with assurances of the true origin of a particular mail stream. The DMARC Management platform enables users with the ability to utilize the following features:

- Free Web-based Tools that allow users to search email domains for SPF, DKIM, and DMARC records.
- Monitoring and Reporting of XML data relevant to SPF/DKIM/DMARC records. Our platform receives, processes and classifies mail observed from an organization's domain namespace.
- Deployment Services offer a project-based approach with education, training and policy enactments to ensure that companies can manage their domain catalog and email footprint upon project completion.

- Support Services offers our support team to help organizations with managing DMARC related incidents, editorializing data reviews, and embedding DMARC into their organization's daily operations.

Infrastructure

dmarcian's infrastructure is deployed entirely within the Google Cloud Platform utilizing Cloud Compute and Regional Persistent disks, Regional Snapshots, Encryption at Rest, Virtual Private Clouds isolated by application region with restricted access, minimized port exposure and network isolation only reachable via a secure gateway. The physical access to servers is managed entirely by Google's data center security procedures.

Software

The dmarcian web application is developed with the Python programming language, backed by PostgreSQL, RabbitMQ, Redis and ElasticSearch components. Our in-house Continuous Delivery development process involves automated testing, code reviews, automated security testing of the core code base and third-party libraries, vulnerability scans of the servers and combined intrusion detection systems, supplemented by an automated deployment process. Application infrastructure and code are monitored in production for performance, errors and security with alerting systems in place to notify dmarcian personnel immediately of any potential concerns. Additional supplements are in place for both abuse protection and rate limits.

Organizational Structure

dmarcian is organized to manage its services and internal operations so that client and internal needs are met, and external compliance is achieved. A sociocratic organizational structure has been developed as the governance model to maximize idea circulation. dmarcian utilizes sociocratic concepts of double-linked circles, built-in transparency, and an acknowledgement of interdependence in how the company operates. Sociocratic circles are different from traditional corporate departments in that sociocratic circles execute, measure, and control their own processes while pursuing its goals. Double linking (where two people from each circle sit at the intersection between two circles) is used to connect circles so that information can flow between and across circles and to avoid situations where a single link might lead to one-way information flow or poor decision making.

dmarcian's personnel are organized by the following business units comprising all areas of customer interaction with oversight and support by Leadership.

- Corporate Business Unit (BU)
- Europe Business Unit (BU)
- Americas Business Unit (BU)
- APAC Business Unit (BU)

All personnel provide background checks and accept the Code of Conduct upon employment. Employee onboarding consists of training sessions to review all policies and procedures and receive security training. Reviews, access assessments and training refreshers are administered on an annual basis.

Procedures

Procedures are in place to manage the security, availability and privacy of customer data.

Data

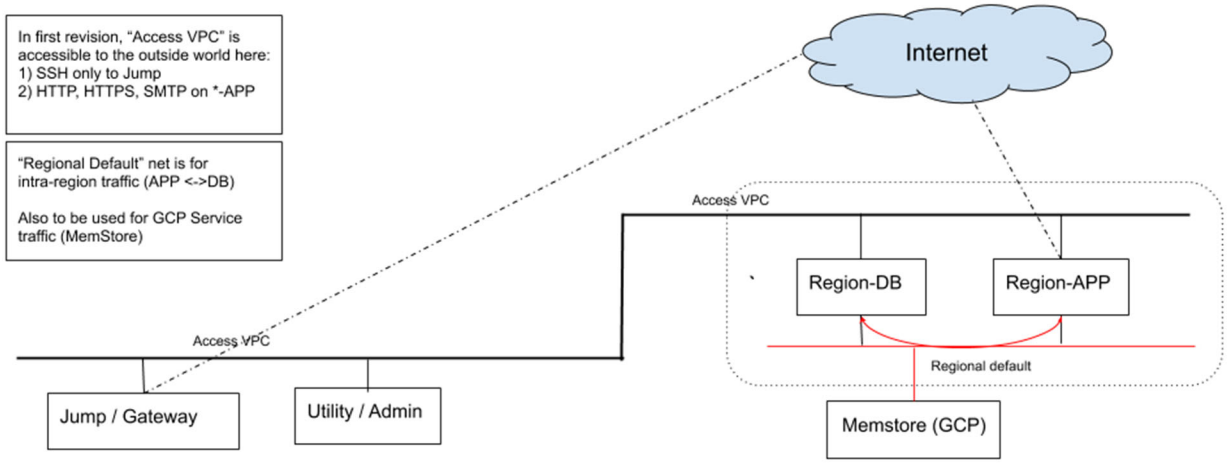
dmarcian's platform receives and processes DMARC aggregate and forensics reports delivered via email by DMARC report providers around the world, which provide insight on the authenticity of email sent on behalf of individual domains. This data is processed by our platform, and augmented with additional Domain Name System (DNS) data to provide insight, monitoring and DMARC deployment planning

A data classification scheme is defined within organizational policies and procedures to address processes for data so that it may be used and protected more efficiently. The most sensitive data classification level is confidential data which would include personally identifiable information (PII), Payment Card Industry Data Security Standard (PCI DSS), authentication verifiers, contractual documents, and other legal documents.

Boundaries of the dmarcian System

This report includes the dmarcian infrastructure and the service offerings as described above. Any other dmarcian services are not included within the scope of this report. The accompanying description references only the policies, procedures, and control activities at dmarcian and does not include the specific policies, procedures, and control activities for any subservice organizations or vendors.

The boundaries of the dmarcian system are the specific aspects of the company's infrastructure, software, people, procedures, and data that are directly necessary to provide the DMARC SaaS offerings as described above. Any infrastructure, software, people, procedures and data that indirectly support the services provided to Partners are not included within the boundaries of the system. The covered system specifically does not include the virtual or physical servers and systems within the Partner or end-customer environments that may be used to access, connect to, or utilize dmarcian's services. End-customer virtual machines within their provided virtual data center environment are the sole responsibility of the Partner and/or end-customer.



Monitoring of Subservice Organizations

dmarcian outsources data center facility management from professional data center operating companies (subservice organizations). Section IV of this report and the description of the system only cover the security, availability and privacy Trust Services Criteria relevant to dmarcian and exclude the related controls of the subservice organizations. Through the review of the subservice organizations' SOC 2 or other security policies, processes, and reports, dmarcian ensures that all subservice organizations have sufficient controls in place and monitor adherence to processes and procedures.

Data Center Facility Providers

dmarcian's data center service providers offer geographic diversity in conjunction with state-of-the-art facilities. Designed and built with reliability, security, and resiliency in mind, they provide fully redundant high-density power and cooling capacities, fully integrated UPS systems, site-wide security and fire protection systems, and access control through customer portals.

Google Cloud Platform (GCP)

Google Cloud Platform provides the physical data center facility for dmarcian Business Units. Google is responsible for physical security, environmental control, and power delivery. Multiple GCP data centers are utilized based on the region of the nearest dmarcian business unit.

Commitments and System Requirements

Commitments

Commitments are declarations made by management to customers within a combination of the Terms of Service, Privacy Policy and Data Processing Addendum. Commitments are communicated and made publicly available on the dmarcian website.

System Requirements

System requirements are specifications regarding how the infrastructure should function to meet the Company's commitments to Partners. Requirements are specified in the Company's policies and procedures, which are available to all employees. The Company's system requirements include the following:

- Change control
- Logical security
- Physical security – Managed by Google
- Availability
- Privacy

Changes to the System

The dmarcian Software Development Life Cycle (SDLC) follows the Continuous Delivery (CD) development flow and strives to best meet the Continuous Delivery Pipeline ideals.

The philosophy can be summarized as "test automatically, deploy small, deploy often." The goal is to maximize the flow of value delivery in the safest way possible, by deploying single changes in isolation often which will allow any unexpected side effects to be quickly reverted and traced back to a more easily identifiable piece of code.

This differs from more traditional change request processes, where deployments are scheduled on cadence and may involve many changes to the code base simultaneously. In the event of any issues, the ability to revert is compromised and the cause of the issue potentially attributable to any of the combined code that has shipped. These problems grow with the size of the code base and the development team.

The CD process begins with local software development on a Vagrant virtual machine, designed to mimic the production environment as much as possible using the same Ansible configuration management tooling used in Production.

Code is version controlled using Git, with the central repository managed within dmarcian's private Gitlab account. Developers will follow the Git Branching Strategy guidelines to create a branch for the related work, and regularly check in their updates.

Once code is ready to be reviewed by other members of the team, a Merge Request (MR) is created to allow other members of the team to review and approve the code changes. The Gitlab Continuous Integration system runs a growing assortment of tests to ensure the integrity of the code base, including manually written tests by the development team (such as Unit tests among others), security tests, vulnerability checks against 3rd party libraries, code structure and error checks. The Continuous Integration (CI) system will record the results of these tests within the Merge Request where the reviewers may easily access the results.

On a daily basis, developers have the opportunity to have their merge requests reviewed by the team during our daily standups. Some MRs may require a dedicated meeting for review. Merge Request reviews may continue for some time as different members of the team review, comment and make suggestions according to the team's Code Review Guidelines.

In some circumstances, long running manual test environments may be necessary to test certain features. The Lab environments may be requested by any development team and will be provisioned by the Operations team. These lab environments are full production clones (minus data) and accessible to other members of the company as needed.

When a Merge Request is approved and testing is completed, code is deployed to production using our automated deployment scripts. In the event of any issues on deployment, the changes are rolled back immediately, and the issues investigated until resolved.

Logical and Physical Security

dmarcian is headquartered in Brevard, NC and has offices around the world in key locations of North America, Canada, Europe and Asia Pacific. dmarcian is a remote-first organization with a global footprint focused on attracting the top talent without being limited by geographic borders. From an IT perspective, no critical systems

are housed on-site; all critical business functions are housed within the Google Cloud Platform (GCP), with controls over physical access being strictly monitored and controlled by Google.

Logical access to infrastructure is extensively restricted, network isolated, regionally segmented and accessible only via a secure central entry point. Access to dmarcian information systems and services is limited to those individuals who have a need-to-know. This standard is based on the principle of least privilege which states that users are only granted access necessary to complete required tasks. dmarcian employees are granted access to various systems based on current job responsibilities and no more. dmarcian employees are granted access to various systems to meet job responsibilities and no more. User access reviews are performed on a regular basis in accordance with dmarcian's Security Review Plan.

Procedures exist for provisioning access to new personnel, changing access, and revoking access to all dmarcian information systems. The access provisioning process begins with the submission of a user access request form by the requestor or the hiring Manager. Upon receipt, the IT department will confirm access approval from the appropriate department, provision the appropriate level of access by assigning a unique user ID and password. Access confirmations will then be communicated with the requestor. Access revocations are initiated by the Human Resources department. Notifications are communicated to appropriate personnel to ensure all access to dmarcian's systems are removed in a timely manner.

dmarcian utilizes Transport Layer Security (TLS) encryption to secure data in transit. Remote access to production systems is granted to authorized employees and controlled through the use of a Secure Shell (SSH) tunnel proxy over a secure gateway, which requires a unique user ID and password for authentication.

Open Source Host-Based Intrusion Detection System Security (OSSEC) and Open Vulnerability Assessment Scanner (OpenVAS) solutions are utilized to perform periodic vulnerability scans and to monitor for any potential host-based intrusion events. The dmarcian operations team manages all systems through a configuration management system to automate, centralize, version control and review that infrastructure.

Availability

The dmarcian operations team ensures availability by monitoring resource usage and processing capacity against current and future demand projections, ensuring that ample compute capacity is available to facilitate system usability as well as growth. Data centers are managed by Google Cloud Platform, providing redundancy, power backups, security and environmental protections. Business Continuity and Disaster Recovery plans are in place with annual testing to ensure that systems are capable of being restored in the event of an outage, in part or in whole via the geographically distributed incremental backups that are in place.

Privacy

dmarcian follows industry standard privacy practices. Privacy obligations are outlined in dmarcian's Privacy Policy and Terms of Service, both of which are available on the dmarcian website for all customers.

A digital snapshot is taken at the time of registration to correlate the accepted version of the policy and continued use of the platform confirms agreement. At any point the Privacy Policy is updated, current customers are notified through the email account associated with the user while a banner may be displayed within the application or under customer notifications. All policies are reviewed at least yearly.

dmarcian limits the type and amount of information collected to only what is needed to deliver service. We collect the following minimal amount of information in order to fulfill our objectives: Cookies, User-submitted content, IP Address information, email address, and email communications.

dmarcian uses this information to generate easy to consume reports, collect internal metrics and analyses, and to satisfy legal processes, regulations, and requests. The information is shared with the account holder through the display of their unique status reports.

Third party sharing is limited to only as needed to support dmarcian's services, and align with legal requirements outlined within the Electronic Communications Privacy Act (ECPA) and General Data Protection Regulation (GDPR).Any vendor that has access to information that dmarcian constitutes as "sensitive or confidential" must maintain a current and acceptable SOC 2 report and sign a Data Processing Addendum (DPA).

Under GDPR, we act as a sub-processor of data and uphold our customers' rights to access their information and its retention, including Right To Be Forgotten and the Transferability from our platform.

All privacy incidents are mitigated according to our Privacy Breach Complaint Policy and Procedures with oversight of our Privacy Officer in a timeframe consistent with GDPR standards.

Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, and Information and Communication

Control Environment

The importance of controls and ethical behavior throughout dmarcian is acknowledged by management through implementation of an established control environment that sets the tone for internal activities and processes. Key aspects of the control environment include:

- Integrity and ethical values
- Commitment to competence
- Management's philosophy and operating style
- Assignment of authority and responsibility

Integrity and Ethical Values

dmarcian has established programs and policies designed to promote and support integrity and ethical values within the organization. New employees are required to review the Employee Handbook, which covers dmarcian culture and employee responsibilities. Employees are required to sign a form acknowledging receipt and understanding of the contents of the Employee Handbook. The Employee Handbook is provided to all new employees and is accessible by all current employees via the internal document management system at all times.

Commitment to Competence

Prior to the offer of employment, all applicants within the Americas BU must undergo a full background check. Applicants will also sign a Proprietary Information and Invention Assignment (PIIA) agreement and read and sign the dmarcian employee handbook and an Employment Agreement that contains a Non-Disclosure Agreement (NDA).

The employee and supervisor will work together to create a plan that provides direction and focus for a given time period. Goals include measurable performance tracks, task completion, personal and professional development while expectations clarify the necessary competencies and behaviors to achieve those goals. One formal review will be provided yearly as well as several informal check-ins throughout the year. The company also conducts team-based 360-degree feedback and employee satisfaction surveys to encourage personal and professional growth for the entire company.

All new employees participate in onboarding training sessions to learn various aspects of dmarcian's business processes and departments, culture, and available tools. Ongoing security awareness trainings are provided for all employees and includes key IT and privacy related topics. dmarcian also encourages employees to seek out other learning opportunities.

Management's Philosophy and Operating Style

dmarcian operations proceed under direction from senior management. A Steering Committee is responsible for maintaining oversight of the organization's control environment.

Risk Assessment

dmarcian maintains a risk assessment process to identify and manage risks that could affect its ability to provide secure, reliable SaaS and Subscription based services to its users. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address and manage those risks.

Leadership's involvement in daily operations allows management to identify risks through direct personal involvement with employees, users, and vendors. Risk assessment procedures and standards are also used to provide assurance that appropriate due diligence is performed prior to the implementation of new/updated systems and services and appropriate testing is occurring in conjunction with such projects. Risks that are considered during management's risk assessment activities include consideration of the following categories:

1. Technical - Requirements, Technology, Complexity, Quality
2. Organization - Performance, Prioritization, Compliance, Resources
3. External - Suppliers, Customers, Market conditions, Regulatory

dmarcian performs a risk assessment at least annually and determines the likelihood and impact of identified risks, using qualitative and quantitative methods. The likelihood and impact associated with each risk is determined independently, considering each risk category.

Risks are mitigated to acceptable levels based on risk criteria and ongoing assessments. For each risk mitigated, it is associated with a current control. If no control is in place a new control is created and monitored until risk is

reduced or eliminated. Insurance policies covering technical errors and omissions and enterprise security and privacy are in place to protect against operational and cybersecurity related risks.

It is the policy of dmarcian to ensure the internal controls of a vendor, maintenance and upkeep of a third-party provider's systems (if applicable), and financial condition of a third-party vendor is carefully evaluated prior to the allowance of such support services to begin, and as an on-going condition of continuing support of such products or services. Competence of a vendor for outsourced work is to be carefully reviewed and considered by, at a minimum, assessing the risks to dmarcian in each of the following areas, as applicable:

1. Performance Risk
2. Strategic Risk
3. Financial Risk
4. Information Security and Regulatory Risk
5. Data Sensitivity and Business Risk
6. Access Risk
7. Contingency Risk
8. Volume Risk
9. Number of Users Risk

The Vendor Management Program details internal requirements to ensure all contracted vendors comply with dmarcian's information security and privacy standards.

Control Monitoring

Management monitors compliance with established policies, plans, procedures, laws, and regulations to which the company is subject. Management monitors the control environment to consider whether controls are operating as intended and that control activities are modified appropriately for changing conditions. Continuous monitoring activities are in place to assess the quality of internal control over time. Corrective actions are initiated through company meetings, department meetings, client conference calls, and informal notifications as needed. dmarcian contracts with an external audit firm on an annual basis to provide independent testing and third-party attestation of internal control relevance and adherence.

Information and Communication

Unique To help align dmarcian's business strategies and goals with operating performance, management is committed to maintaining effective communication with all personnel. dmarcian maintains a portal where governance documents including policies, procedures, guidelines and standards are hosted and available to all staff members. The Governance documents include policies relating to Code of Conduct, data classification and protection, information security, and physical security to help govern the protection of client and company information.

dmarcian also maintains an auxiliary storage where supplemental governance documents are available, such as but not limited to:

- Training materials
- Roles and Responsibilities
- Company Goals and Strategies
- Role-specific policies and procedures

Governance documents are considered for revision or update as well as for annual review. Employees are required to acknowledge that they will hereby agree to comply fully with all company policies and procedures, without limitation. dmarcian will utilize internal email to communicate time-sensitive changes in business processes, security and IT operations. Regular organizational communications and status updates are distributed to staff members through the Slack platform. Corporate Circle meetings are conducted on at least an annual basis to address the performance of dmarcian's service commitments.

As a result of dmarcian's sociocratic governance structure, management is involved in day-to-day operations and provides personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. Communication activities are made electronically, verbally, and through the actions of management.

Incident Response

All security incidents are retained and documented by management. Once the incident has been resolved, a Security Incident Report is created. The types of information that are logged include:

- Report Date
- Location of Incident
- Incident Start Date
- Incident Notification Date
- Identified issue
- Remediation Steps
- Recommendations
- Preventive measures
- Action Items

There were no security incidents identified throughout the reporting period.