System and Organization Controls (SOC 3) Report

Independent Assurance Report on Controls at Service Organization

EasyDMARC, Inc.

Contents

Գրանթ Թորնթոն Քնսալթինգ ՓԲԸ
Երևան Պլազա բիզնես կենտրոն
ՀՀ, ք. Երևան 0015
Գրիգոր Լուսավորչի 9

Հ. + 374 10 500 964
+ 374 10 500 961

Grant Thornton Consulting CJSC
Yerevan Plaza Business Center
9 Grigor Lusavorich Street,
Yerevan 0015, Republic of Armenia

T + 374 10 500 964
+ 374 10 500 961

Independent Assurance Report on the Description of Controls, their Design and Operating Effectiveness

To the Management of EasyDMARC, Inc.

Scope

We have performed an independent reasonable assurance engagement on EasyDMARC, Inc.'s description of its system entitled "EasyDMARC, Inc.'s Services" on pages 7-9, for the period from 9 November 2021 to 1 November 2022 (the "System Description"), and on the design and operation of controls related to control objectives stated in the System Description, based on the criteria for the security, availability, and confidentiality (Control Criteria) set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

EasyDMARC, Inc. uses subservice organizations, 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 EasyDMARC, Inc., to achieve EasyDMARC, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents EasyDMARC, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of EasyDMARC, Inc.'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 EasyDMARC, Inc., to achieve EasyDMARC, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents EasyDMARC, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of EasyDMARC, Inc.'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.

Management's Responsibilities

In "EasyDMARC, Inc. Management Statement", EasyDMARC, Inc. has provided a statement about the fairness of the presentation of the System Description and the design and operating effectiveness of the controls to achieve the related control objectives. Management of EasyDMARC, Inc. is responsible for preparing the Description and the accompanying Statement on pages 5-6, including the completeness, accuracy, and method of presentation of the System Description and the Statement, providing the services covered by the System Description, specifying the control objectives and stating them in the System Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the Statement, and designing, implementing, documenting and effectively operating controls to achieve the stated System-related control objectives.

Our Independence and Quality Control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies International Standard on Quality Control 1 and accordingly maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner's Responsibilities

Our responsibility is to express an opinion on EasyDMARC, Inc.'s System Description and on the design and operating effectiveness of the controls to achieve the related control objectives stated in the System Description, based on our procedures.

We conducted our engagement in accordance with the "*International Standard on Assurance Engagements 3000 (Revised): Assurance Engagements other than Audits or Reviews of Historical Financial Information"* issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, based on the criteria stated in management's Statement, the System Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the System Description.

An assurance engagement to report on the service organization's system and the suitability of the design and operating effectiveness of controls involves performing procedures to obtain evidence about the fairness of the System Description presentation and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives, based on the criteria in management's Statement. The procedures selected depend on the practitioner's judgment, including the assessment of risks that the System Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the System Description. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the System Description were achieved. An assurance service of this type also includes evaluating the overall presentation of the System Description, suitability of the control objectives and suitability of the criteria specified by the service organization in its assertion.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations of Controls

The System Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' environments and systems and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment.

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or failures, including the possibility of human error and circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability, processing integrity, confidentiality, and privacy will be achieved.

Examples of inherent limitations in an entity's security controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer;
- Ineffective controls at a vendor or business partner;
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Also, the projection to the future of any evaluation of the fairness of the presentation of the System Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are described on pages 5-6.

In our opinion, in all material respects:

- the System Description fairly presents EasyDMARC, Inc.'s System as designed and implemented throughout the period from 9 November 2021 to 1 November 2022;
- the controls related to the control objectives stated in the System Description were suitably designed throughout the period from 9 November 2021 to 1 November 2022 if its controls operated effectively throughout the period and if the subservice organizations and user entities applied the complementary controls assumed in the design of EasyDMARC, Inc.'s controls throughout the period;
- the controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the System Description were achieved, operated effectively throughout the period from 9 November 2021 to 1 November 2022 and if the subservice organizations and user entities applied the complementary controls assumed in the design of EasyDMARC, Inc.'s controls throughout the period.

Grant Thornton Consulting CJSC

30 November 2022

EasyDMARC, Inc. Management Statement

EasyDMARC, Inc. Management's Statement Regarding the Effectiveness of its Controls, Based on the Trust Services Principles and Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy

We have prepared the accompanying description of EasyDMARC, Inc.'s System entitled "EasyDMARC Creative Platform" (including EasyDMARC Applications and "EasyDMARC for Developers" platform), throughout the period from 9 November 2021 to 1 November 2022, for user entities of the services and their auditors who audit and report on such user entities' in the areas of security, availability, confidentiality, processing integrity and privacy and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks related to internal control related to security, availability, confidentiality, processing integrity and privacy.

EasyDMARC, Inc. uses subservice organizations to provide data center facility and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at EasyDMARC, Inc., to achieve EasyDMARC, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents EasyDMARC, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of EasyDMARC, Inc.'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 EasyDMARC, Inc., to achieve EasyDMARC, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents EasyDMARC, Inc.'s controls, the applicable trust services criteria and the complementary user entity controls assumed in the design of EasyDMARC, Inc.'s controls.

The System description does not extend to the controls of the subservice organizations, or the controls of the user entities as set out in "Terms of service" at Terms of service (easydmarc.com).

We confirm, to the best of our knowledge and belief, that:

- System description fairly presents EasyDMARC, Inc.'s System during the period from 9 November 2021 to 1 November 2022 as it relates to controls of security, availability, confidentiality, processing integrity and privacy. The criteria we used in making this statement were that the System description:
  - presents how the System was designed and implemented to process relevant user entity data, including, if applicable:
    - types of services provided, including, as appropriate, the types of data processed;
    - the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities;
    - how the system captures and addresses significant events and conditions;
    - relevant control objectives and controls designed to achieve those objectives;
    - other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.
  - includes relevant details of changes to EasyDMARC, Inc.'s system during the period covered by the System Description;

  - does not omit or distort information relevant to EasyDMARC, Inc.'s system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the EasyDMARC, Inc.'s System that each individual user entity and its auditor may consider important in its own particular environment.

- controls related to the control objectives stated in the System Description were suitably designed and operating effectively throughout the period from 9 November 2021 to 1 November 2022 to achieve those control objectives, if the subservice organization and user entities applied the complementary controls assumed in the design of EasyDMARC Inc.'s controls, and those controls operated effectively throughout the period from 9 November 2021 to 1 November 2022. The criteria we used in making this assertion are the following:
  - Risks that threaten the achievement of the control objectives stated in the System Description have been identified by the management of EasyDMARC, Inc.;
  - Controls identified in the System Description would, if operated as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the System Description from being achieved;
  - Controls were consistently applied as designed, including manual controls were applied by individuals who have the appropriate competence and authority.
- System was protected against unauthorized access, use, or modification to achieve EasyDMARC, Inc.'s commitments and system requirements;
- System was available for operation and use, to achieve EasyDMARC, Inc.'s commitments and system requirements;
- System information is collected, used, disclosed, and retained to achieve EasyDMARC, Inc.'s commitments and system requirements;
- System processing is complete, valid, accurate, timely, and authorized to meet EasyDMARC, Inc.'s commitments and system requirements;
- Personal information is collected, used, retained, disclosed, and disposed to meet EasyDMARC, Inc.'s commitments and system requirements, based on the Control Criteria.

EasyDMARC, Inc. Management

3 November 2022

EasyDMARC, Inc.’s System Description

EasyDMARC, Inc. Background

EasyDMARC, Inc. (Company), founded in 2018, is building the world's largest DMARC ecosystem. They are committed to ensure businesses’ security in cyberspace. EasyDMARC solution prevents companies from data leakage, protects them from financial loss, email phishing attacks, averts customer loss, secures their email accounts and prevents the unauthorized use of domains.

Control Environment

EasyDMARC, Inc. management have identified the controls over the system throughout the period from 9 November 2021 to 1 November 2022 to achieve its commitments and system requirements related to the operation using the criteria for the security, availability, and confidentiality (Control Criteria) set forth in the AICPA’s TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this, management have selected a set of controls to provide reasonable assurance that:

- System is protected against unauthorized access, use, or modification to achieve EasyDMARC, Inc.’s commitments and system requirements;
- System is available for operation and use, to achieve EasyDMARC, Inc.’s commitments and system requirements;
- System information is collected, used, disclosed, and retained to achieve EasyDMARC, Inc.’s commitments and system requirements;
- System processing is complete, valid, accurate, timely, and authorized to meet the EasyDMARC, Inc.’s commitments and system requirements;
- Personal information is collected, used, retained, disclosed, and disposed to meet the EasyDMARC, Inc.’s commitments and system requirements, based on the Control Criteria.

Scope

The scope of the systems covered in this report includes:

The key products of the Company are:

- EasyDMARC Outgoing email security solutions
- EasyDMARC Inbound security solutions
- EasyDMARC Email deliverability.

The key organizational units (teams) of the Company are:

- Research and Development team
- Product team
- Sales team
- Marketing team
- Administrative team
- Support (Customer Service) team.

The key tools of the Company used for product development:

- AWS (AWS SES, AWS S3)
- Oracle Cloud (Oracle SQL HA server)
- Google workspace
- GitLab
- JIRA
- Slack.

Infrastructure

EasyDMARC, Inc. infrastructure includes the facilities, network, and hardware, as well as some operational software (e.g., host operating system, virtualization software, etc.) that support the provisioning and use of these resources. EasyDMARC, Inc. infrastructure is designed and managed in accordance with security compliance standards and EasyDMARC, Inc.'s security policies.

Most of EasyDMARC, Inc.'s servers are hosted at Oracle Cloud, the rest are hosted in AWS and Google Cloud. Only the network access points are located in Yerevan office.

Locations

The locations covered in this report include:

- 651 N Broad St, Suite 206, Middletown, 19709, Delaware, USA,
- Vlamingstraat 4, 2712BZ Zoetermeer, The Netherlands,
- 24/16 Azatutyan Ave, Yerevan, Armenia.

People

EasyDMARC, Inc.'s organizational structure provides a framework for planning, executing and controlling business operations. Executive and senior leadership play Important roles in establishing EasyDMARC, Inc.'s tone and core values. The organizational structure assigns roles and responsibilities to provide for adequate staffing, security, efficiency of operations, and segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel.

The Company follows a structured on-boarding process to familiarize new employees with EasyDMARC, Inc.'s tools, processes, systems, security practices, policies and procedures. Employees are provided with the set of the EasyDMARC, Inc.'s policies and pass induction training to educate them as to their responsibilities concerning information security.

Customer Data

EasyDMARC, Inc. provides solutions for protecting email domains. EasyDMARC tools help to monitor the aspects of email authentication and enforce effective protection from phishing attacks.

EasyDMARC stores the following customer data in its cloud (Oracle Cloud):

- Email registered address of the account,
- Customer name/ account (optional),
- Aggregate data for analytics.

Availability

EasyDMARC solutions are architected in a manner to maintain availability of its services through defined programs, processes, and procedures. The Business Continuity Program encompasses the processes and procedures by which EasyDMARC, Inc. identifies, responds to, and recovers from a major event or incident within the environment. This program builds upon the traditional approach of addressing contingency management, incorporating elements of business continuity and disaster recovery plans while expanding to consider critical elements of proactive risk mitigation strategies. These strategies include continuous infrastructure capacity planning.

Contingency plans and incident response playbooks are maintained to reflect emerging continuity risks and lessons learned. Plans are tested and updated through the course of business, and the EasyDMARC, Inc. Business Continuity Program is regularly reviewed and approved by senior leadership.

EasyDMARC, Inc. has identified critical system components required to maintain the availability of the system and recover services in the event of an outage. These components are replicated across multiple availability zones; authoritative backups are maintained and monitored to ensure successful replication.

EasyDMARC solutions operate on Oracle cloud. The frontend and backend are wholly hosted on Oracle Cloud. DMARC aggregate reports are received mainly from AWS, moved to Oracle Cloud and processed there.

EasyDMARC, Inc.'s backend infrastructure is entirely hosted on Oracle Cloud, it is fully automated and monitored by continuous functional tests to detect any sort of downtime, protecting infrastructure needs and supporting availability commitments and requirements. Additionally, EasyDMARC, Inc. maintains a capacity planning model to assess infrastructure usage and demands.

Security

EasyDMARC, Inc. has established information security policies and there is an executive-level commitment to implement and follow the policies throughout the organization.

Information Security program is led by the CEO of EasyDMARC, Inc.

Confidentiality

EasyDMARC, Inc. is committed to protecting the security and confidentiality of its customers' content, defined "Privacy Policy" at EasyDMARC Privacy Policy | EasyDMARC. EasyDMARC, Inc. communicates its confidentiality commitment to customers in "Terms of service" at Terms of service (easydmarc.com).

Internally, confidentiality requirements are communicated to employees through training and policies. Employees are required to attend security awareness training, which includes information, policies, and procedures related to protecting customers' content. EasyDMARC, Inc. monitors the performance of third parties through periodic reviews, which evaluate performance against contractual obligations, including confidentiality commitments.

Privacy

EasyDMARC, Inc. is committed to protecting the personal data of its customers' content, defined as "EasyDMARC – GDPR" at GDPR - General Data Protection Regulation | EasyDMARC and "Privacy Policy" at EasyDMARC Privacy Policy | EasyDMARC. EasyDMARC, Inc. communicates its privacy commitment to customers in "Terms of service" at Terms of service (easydmarc.com).

Complementary user entity controls

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

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. These controls should not be regarded as a comprehensive list of all controls that might be pertinent at the user entities' locations. User entities' management is responsible for selecting and implementing these complementary user entity controls:

1. Ensuring the compliance with EasyDMARC's Privacy Policy by their personnel and their clients;
2. Understanding and complying with their contractual obligations to EasyDMARC, Inc.;
3. Notifying EasyDMARC, Inc. of changes made to technical administrative contact information;
4. Notifying EasyDMARC, Inc. regarding new, terminated user accounts and changes necessary thereto;
5. Immediately notifying EasyDMARC, Inc. of any actual or suspected information security breaches involving the system, including compromised user accounts;
6. Grant access only to authorized and trained personnel and removing access when no longer necessary or appropriate;
7. Ensuring the supervision, management, and control of the use of the System by their personnel and their clients;
8. Developing internal policies for disaster recovery and business continuity, that address the inability to access or utilize the System;
9. Preventing the loss, malfunctioning, or damage to the System.

Complementary subservice organization controls

When controls at a vendor are necessary in combination with EasyDMARC, Inc.'s controls to provide reasonable assurance that EasyDMARC, Inc.'s service commitments and system requirements are achieved, based on the applicable trust services criteria, the vendor is considered a subservice organization. EasyDMARC, Inc.'s services are designed with the assumption that certain controls will be implemented by subservice organizations (complementary subservice organization controls). It is not feasible for all the Trust Services Criteria related to EasyDMARC, Inc.'s services to be solely achieved by EasyDMARC, Inc.'s control procedures. Accordingly, subservice organizations should establish their own internal controls or procedures to complement those of EasyDMARC, Inc.

Management has identified the following subservice organizations and has elected the carve-out method for the purpose of System Description and management assertion.

Subservice organization	Description
AWS	Cloud hosting services
Oracle	Cloud hosting services
Google	Cloud hosting services

Complementary subservice organization controls

The following are the applicable trust services criteria and controls that subservice organizations should establish to complement those of EasyDMARC, Inc., provide additional assurance that the Trust Services Criteria described within this report are met.

Criteria	Control
CC6 Series **Logical and Physical Access**	- Physical access to the datacenter facilities is restricted to authorized personnel. - Physical access to data centers is approved by an authorized individual. - Procedures are implemented to authenticate authorized users, restrict access and detect unauthorized access attempts. - Security measures are implemented to provision and de-provision user access to systems and applications based on appropriate authorization. - Encryption has been implemented, by default or as configured by the subservice organization, to secure the transmission and storage of information. - Procedures are implemented to securely decommission and physically destroy production assets.
CC7 Series **System Operations**	- Vulnerability scans and penetration testing are performed periodically to identify vulnerabilities threatening the systems. - Incident response procedures are established and implemented to identify, analyze and remediate events and/or incidents. - Environmental protections, monitoring and procedures for regular maintenance are implemented at the datacenter facilities.
CC8 Series **Change Management**	- Procedures are established and implemented to ensure changes to systems are authorized, designed, developed, configured, documented, tested, and approved prior to production deployment.
A Series **Availability**	- Monitoring tools are implemented to monitor and manage the capacity and availability of hosting infrastructure. - Environmental protections, data backup processes and recovery mechanisms have been implemented and are appropriately tested to adequately address availability requirements.

EasyDMARC, Inc.'s management, along with the subservice organizations, defines the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria trough written contracts, such as SLAs. In addition, EasyDMARC performs monitoring of the subservice organization controls, including the following:

- Holding periodic discussions with vendors and subservice organizations,
- Reviewing attestation reports over services provided by vendors and subservice organizations, if applicable.