Frazier & Deeter
CPAs & ADVISORS

Independent Service Auditor's System and Organizational Controls SOC3® Report

On Zapier Inc.'s Assertion of the Effectiveness of Its Controls Relevant to Security, Availability, Confidentiality, and Privacy

For the Period February 1, 2021 to April 30, 2021

zapier

Zapier, Inc.
548 Market Street, #62411
San Francisco, California 94104

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations™

Assertion of Zapier, Inc.'s Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Zapier Inc.'s ("Zapier" or "the Company") software as a service ("SaaS") system ("the System") throughout the period February 1, 2021 to April 30, 2021, to provide reasonable assurance that Zapier's service commitments and system requirements relevant to security, availability, confidentiality and privacy were achieved. Our description of the boundaries of the System is presented in Attachment 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 February 1, 2021 to April 30, 2021, to provide reasonable assurance that Zapier's service commitments and system requirements were achieved based on the Trust Services Criteria relevant to security, availability, confidentiality 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*).

Zapier'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 Attachment 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 February 1, 2021 to April 30, 2021, to provide reasonable assurance that Zapier's service commitments and system requirements were achieved based on the applicable Trust Services Criteria.

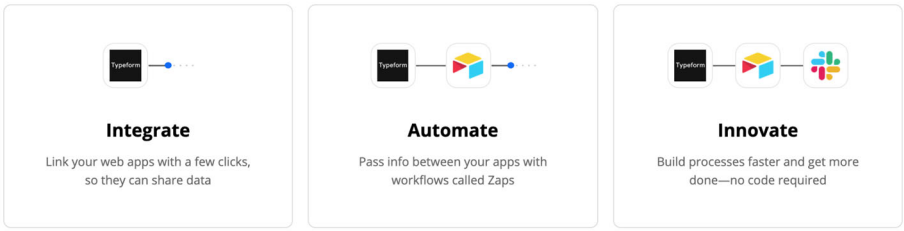
Attachment A

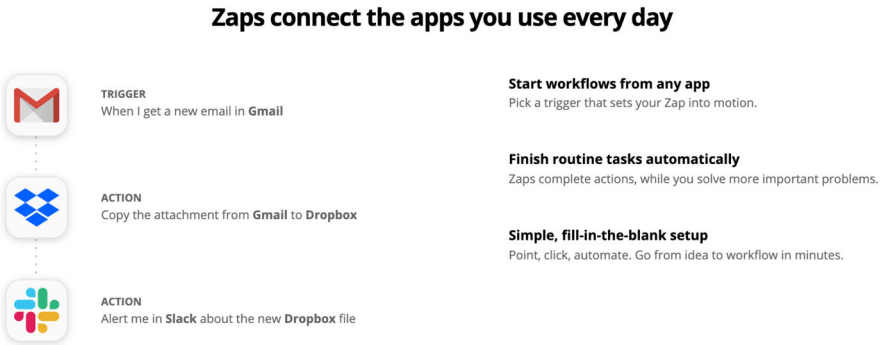
Zapier, Inc.'s Description of the Boundaries of Its Software as a System

Company Overview and Services Provided

Zapier is an online automation tool that integrates various web applications and services. Users can connect two or more applications via their application programming interfaces (APIs) and automate repetitive tasks without needing the ability to code or rely on developers to build out the integration. Zapier is a cloud-based platform offering its product features through various plans and pricing models.

Zapier is a global organization that is remotely operated and maintains a customer base of over 8 million users. Zapier is headquartered in San Francisco, California and was founded in 2011.





Components of the System Used to Provide the Services

Infrastructure and Software

Infrastructure supporting the Zapier application is hosted, owned, and managed by Amazon Web Services (AWS). The software associated with the Zapier application are the AWS cloud-native services associated with microservices, continuous integration and continuous deployment (CI/CD) tools, containers, and version control. AWS is also utilized for configuring firewall rules to allow or deny traffic to and from the virtual machines.

Attachment A

Zapier, Inc.'s Description of the Boundaries of Its Software as a System

Network

Unauthorized use of the network in whole or in part is strictly prohibited. To ensure users are responsible, productive network users, guidelines regarding use of the network are in place and regularly communicated. Violations of any guidelines governing the use of the network may result in disciplinary action, up to and including immediate termination of employment. If necessary, Zapier will advise appropriate regulatory bodies of any violations.

Zapier maintains information security policies with the purpose of establishing technical guidelines for network design and security, and to communicate controls to secure the corporate network. The scope of these policies as they relate to network security, apply to IT systems, devices, rules, and configurations that are designed to protect the integrity, confidentiality, and accessibility of Zapier networks.

Zapier maintains an Acceptable Use Policy and Access Control Policy which details the requirements expected of users that are connecting to the corporate network and authenticating within compliance of least privilege access. The scope of these policies includes all users who have access to company-provided or company-approved laptops and to those who require access to the corporate network and/or systems.

Anti-Virus/Malware Protection

Zapier's Security team has implemented an end-point protection solution as part of its network security protection program. All personnel with access to Zapier's network are required to have this solution installed on their workstation laptops in order to lessen security threats to organizational assets. This requirement is defined in Zapier's Acceptable Use Security Policy and acknowledged by personnel annually.

Organizational Structure

Zapier maintains clear and concise communication channels to disseminate information regarding control requirements to appropriate levels within the organization. Zapier is managed by and under the direction of the Executive Leadership Team, responsible for various operational areas of the Company, including general management and administration. A Board of Managers is established, and includes individuals independent from the Company, and possess relevant skills and expertise to provide oversight responsibilities for Zapier.

Formal organizational charts have been developed representing Zapier functions and reporting lines. The organization is hierarchical, which is conducive to control through segregation of responsibilities. Written job expectations have been developed and describe the duties and responsibilities for key positions. When assigning authority and responsibilities, Management considers the nature of the employee positions as well as ensuring suitable segregation of duties is maintained.

Attachment A

Zapier, Inc.'s Description of the Boundaries of Its Software as a System

Management meets regularly to discuss a wide range of topics relative to the system and is also responsible for establishing corporate policies and procedures addressing the operational, financial, cultural, and social aspects of Zapier.

Data

Zapier maintains a Data Classification & Handling Policy that applies to all data processed within Zapier systems and defines how the organization categorizes the data it stores. This policy also addresses the identification and handling of confidential data.

Policies and procedures are formally documented to provide guidance for the following data governance processes:

Data Classification

Classification of data provides guidance to Zapier personnel for how to handle and protect information appropriately. Data classification types allow for information to be grouped by similar security and privacy protection needs and have relevant information security procedures. Per Zapier's Terms of Service, users are prohibited from using any sensitive personal data within the Service. All customer data received is classified as "Confidential" and securely protected.

Data Storage

Zapier stores data within encrypted AWS S3 buckets and maintains regular data back-ups. Data at rest is encrypted using AES-256.

Data Use and Disclosure

Zapier's use of data is disclosed through the company's external Privacy Policy. Zapier also maintains a Data Processing Addendum (DPA) for the contractual commitments made to paid subscribed users.

Data Transmission

Zapier ensures proper encryption strength is implemented and when transmissions occur as part of the web application, ensures that HTTPS and digital certificates are in place. In addition, Zapier data in transit is encrypted using TLS 1.2.

Attachment A

Zapier, Inc.'s Description of the Boundaries of Its Software as a System

Data Destruction

Zapier maintains data retention schedules according to data classification type. All customer data is retained and destroyed in accordance with Zapier's Privacy Policy, Data Classification and Handling Policy, and Data Processing Addendum (DPA). Further details are also documented within Data Privacy at Zapier.

Processes and Procedures

Zapier has developed and documented formal information security policies and procedures for any processes that could impact the security, availability, confidentiality, or privacy of its services. These policies and procedures are designed to segregate duties and enforce responsibilities for Zapier's internal controls. Policies are communicated to employees and are made readily available via Zapier's intranet. Policies and procedures are reviewed and approved by the Head of Security on an annual cadence, at minimum. Zapier maintains the following list of information security policies:

- *Acceptable Use Security Policy*
- *Access Control Policy*
- *Business Continuity Policy*
- *Change Management Policy*
- *Data Classification & Handling Policy*
- *Encryption Management Policy*
- *Information Security Policy*
- *Logging and Monitoring Policy*
- *Risk Management Policy*
- *Security Incident Response Policy*
- *Software Development Lifecycle (SDLC) Policy*
- *Vendor Management Policy*
- *Vulnerability Management Policy*

Attachment B

Zapier, Inc.'s Principal Service Commitments and System Requirements

Principal Service Commitments

Zapier designs processes and procedures to meet the objectives of its Software as a Service ("SaaS") platform. Those objectives are based on the service commitments that Zapier makes to its users, any relevant laws and regulations that govern the provision of Zapier services, and the operational and compliance requirements that Zapier has established for its services.

Security and service commitments to users/customers/partners are documented and communicated in Zapier's Terms of Service, Privacy Policy, Data Processing Addendum, Non-Disclosure Agreements (NDAs) and other customer and/or partner agreements. Security commitments are also presented within the Security webpage of the Zapier's website/description of service offerings provided online. Zapier has implemented administrative and technical safeguards to prevent the loss, unauthorized use, access, or disclosure of Zapier and customer proprietary data.

Zapier grants its subscribers a limited, worldwide, non-exclusive, non-sublicensable, non-transferable right during a contracted term to (a) use the hosted software and (b) reproduce, without modification, and internally utilize Zapier's online user documentation.

Global customer support is offered 24/7 to active and authorized users. Zapier maintains a Help & Support webpage that provides users resources for service use and account management. All other user inquiries are handled via email by Zapier's Customer Champions on the Support team. The Support team works closely with all team divisions at Zapier, including the Engineering team to resolve any issues related to code base or custom functionality.

Zapier communicates contractual commitments as a service provider and user responsibilities through its Terms of Service and Terms of Use. Zapier reports on the health status of its Service through the Zapier Status webpage. Zapier is committed to providing uninterrupted services to customers, except for an unforeseeable event. Zapier hosts its IT infrastructure and service offerings through Amazon Web Services, Inc. (AWS). Therefore, Zapier relies on AWS, as its cloud service provider, to service any Zapier commitments related to file backups, retention, business continuity and disaster recovery planning, and availability of the service. As a critical vendor to Zapier's business operations, a vendor risk assessment of AWS is conducted on an annual basis.

Scheduled maintenance is performed during pre-determined times during which access to Zapier's service may be disrupted for scheduled standard maintenance. Maintenance windows are communicated through subscription to the Zapier Status - Incident History webpage and email distribution list.

Unplanned or emergency maintenance periods are those where system access is not available to address a critical or emergency issue. When possible, subscribers are notified prior to unplanned or emergency maintenance that falls outside scheduled maintenance windows. Notifications are also delivered through the Zapier Status - Incident History webpage.

Attachment B

Zapier, Inc.'s Principal Service Commitments and System Requirements

Zapier performs daily and monthly backups of customer content that is uploaded and stored. Data back-up files are stored securely using AWS as a cloud service provider.

System Requirements

Zapier establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Requirements are communicated in the organization's information security policies and procedures, system design documentation, and any contracts with users/customers/partners. Information security policies define an organization-wide approach to system security and data protection. These policies address how services are designed and developed, system operations, management of internal business systems and networks and the process for hiring and training employees. In addition to these policies, operating procedures have been documented addressing manual and automated processes required in the operation and development of Zapier's system.

Subservice Organizations

Zapier utilizes Amazon Web Services (AWS) to perform certain key operating functions, specifically related to cloud environment hosting. The accompanying assertion includes only those policies, procedures, and controls at Zapier, and does not include policies, procedures, and controls at the third party subservice organization described below. The examination by the independent auditors did not extend to policies, procedures, and controls at the subservice organization.

The types of controls at AWS that are expected to be in place, assumed in the design of Zapier's controls, and significant to Zapier's systems, in combination with controls at Zapier, are as follows:

Subservice Organizations	Services Provided	Applicable Trust Criteria
Amazon Web Services (AWS)	Cloud data center hosting services	CC.6 - Logical & Physical Access CC.7 - System Operations A.1 - Additional Criteria for Availability C.1 - Additional Criteria for Confidentiality P.4 - Additional Criteria for Privacy

Attachment B

Zapier, Inc.'s Principal Service Commitments and System Requirements

Complementary User Entity Controls

Zapier's services were designed with the assumption that certain controls would be implemented by user entities. These controls should be in operation at user entities to complement Zapier's controls. The user entity controls subsequently presented should not be regarded as a comprehensive list of all controls that should be employed by user entities.

User auditors should consider whether the following controls have been placed in operation at user organizations:

- User entities are responsible for notifying Zapier of any issues on a timely basis. User entities are responsible for validating the accuracy of their data as presented / reported by Zapier.
- User entities are responsible for communicating accurate contact information to Zapier.
- User entities are responsible for ensuring that their passwords to the Zapier application accounts are kept confidential.
- User entities are responsible for notifying Zapier of any unauthorized use of any password or account, or any other known or suspected breach of security related to the use to the application.
- User organizations are responsible for using secure methods to facilitate data transfers outside of the established system.
- Controls should be maintained to provide reasonable assurance that user entities adhere to the Terms of Service, Terms of Use and Zapier's Acceptable Use Policy.

Independent Service Auditor's SOC 3® Report

Independent Service Auditor's Report

To the Management of Zapier, Inc.:

- We have examined Zapier, Inc.'s ("Zapier" or "the Company") accompanying assertion entitled "Assertion of Zapier, Inc. Management" (assertion) that the controls within Zapier Inc.'s Software as a System (System) were effective throughout the period February 1, 2021 to April 30, 2021, to provide reasonable assurance that Zapier's service commitments and system requirements were achieved based on the Trust Services Criteria relevant to security, availability, confidentiality 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).
- Zapier 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 Zapier's service commitments and system requirements were achieved. Zapier has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Zapier 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.
- 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 Zapier's service commitments and system requirements based on the applicable Trust Services Criteria.

Independent Service Auditor's Report

- Performing procedures to obtain evidence about whether controls within the System were effective to achieve Zapier'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.

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 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 policies or procedures may deteriorate.

- In our opinion, Management's assertion that the controls within Zapier's Software as a Service System were effective throughout the period February 1, 2021 to April 30, 2021, to provide reasonable assurance that Zapier's service commitments and system requirements were achieved based on the applicable Trust Services Criteria is fairly stated, in all material respects.

Frazier & Deeter, LLC

July 2, 2021
Atlanta, Georgia