Frazier & Deeter
CPAs & ADVISORS

SOC 3® Report

On Zapier, Inc.'s Assertion for the Software-As-A-Service System Relevant to Security, Availability, Confidentiality, and Privacy

For the Period May 1, 2023 to May 31, 2024

zapier

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

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

Frazier & Deeter
CPAs & ADVISORS

Table of Contents

Section One

Independent Service Auditor's Report

Section One

Independent Service Auditor's Report

To the Management of Zapier, Inc.:

Scope

We have examined Zapier, Inc.'s ("Zapier" or "the Company") accompanying assertion titled "Management of Zapier, Inc.'s Assertion" (the Assertion) that the controls within Zapier's Software-As-A-Service system (the System) were effective throughout the period May 1, 2023 to May 31, 2024, 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*, in AICPA Trust Services Criteria.

Zapier uses the subservice organization identified in Attachment A to perform some of the services provided to the user entities. Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Zapier, to achieve Zapier's service commitments and system requirements based on the applicable trust services criteria. Attachment A does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Attachment A indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Zapier, to achieve Zapier's service commitments and system requirements based on the applicable trust services criteria. Attachment A presents the complementary user entity controls assumed in the design of Zapier'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

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.

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 (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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.
- 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.

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 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.

Frazier & Deeter
CPAs & ADVISORS

Section One

Independent Service Auditor's Report

Opinion

In our opinion, management's Assertion that the controls within Zapier's Software-As-A-Service System were effective throughout the period to May 1, 2023 to May 31, 2024, 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.

July 31, 2024
Atlanta, Georgia

Section Two

Management of Zapier, Inc.'s Assertion

Section Two

Management of Zapier, Inc.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Zapier, Inc.'s ("Zapier" or "the Company") Software-As-A-Service system (the System) throughout the period May 1, 2023 to May 31, 2024, to provide reasonable assurance that Zapier's service commitments and system requirements relevant to security, availability, confidentiality, and privacy 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*, in AICPA *Trust Services Criteria*. 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 May 1, 2023 to May 31, 2024, to provide reasonable assurance that Zapier's service commitments and system requirements were achieved based on the applicable 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 A.

Zapier uses a subservice organization identified in Attachment A to perform some of the services provided to the user entities. Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Zapier, to achieve Zapier's service commitments and system requirements based on the applicable trust services criteria. Attachment A does not disclose the actual controls implemented at the complementary subservice organization.

Attachment A indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Zapier, to achieve Zapier's service commitments and system requirements based on the applicable trust services criteria. Attachment A presents the complementary user entity controls assumed in the design of Zapier'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 May 1, 2023 to May 31, 2024, 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 Principal Service Commitments and System Requirements and Description of the Boundaries of Its Software-As-A-Service System

Principal Service Commitments and System Requirements

Service Commitments

Zapier designs processes and procedures to meet the objectives of its 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.

Service commitments are declarations made by Zapier management to its clients regarding the performance of the Zapier platform.

- Zapier has implemented and maintains technical, and administrative security measures designed to protect the Zapier platform from unauthorized access, destruction, use, modification, or disclosure.
- Zapier's availability is programmatically supported by its implementation of Business Continuity, Disaster Recovery and Redundancy, which is designed to maintain both its infrastructure and product updates with limited downtime.
- Pursuant to its user agreements and acceptable use of the product, Zapier takes applicable measures to protect confidential and private data from loss, misuse, alteration, and unauthorized access.
- Zapier manages data in its capacity as a processor through its implementation of user agreements, a privacy notice, and privacy related commitments that are applicable to its offered products and services.

System Requirements

System requirements are specifications regarding how the Zapier SaaS system should function to meet the Company's commitments and relevant laws and regulations. Zapier's system requirements include the following:

- Zapier manages its technical security measures through enforcing its Information Security Policy, access controls, monitoring and logging, vulnerability and breach detection, incident response, and encryption.
- Zapier has designed availability components within its environmental architecture to prevent the operation of services and user data from being impacted by a single point of failure.

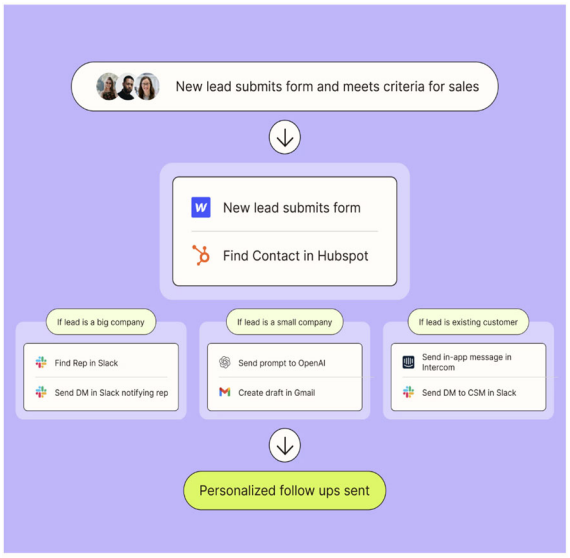
- Zapier maintains the confidentiality of data through access controls, third party contracts, and employment agreements.
- Zapier implements and maintains data classification and handling practices, retention schedules, access limitations and data subject requests.

Zapier, Inc.'s Description of the Boundaries of Its Software-As-A-Service System

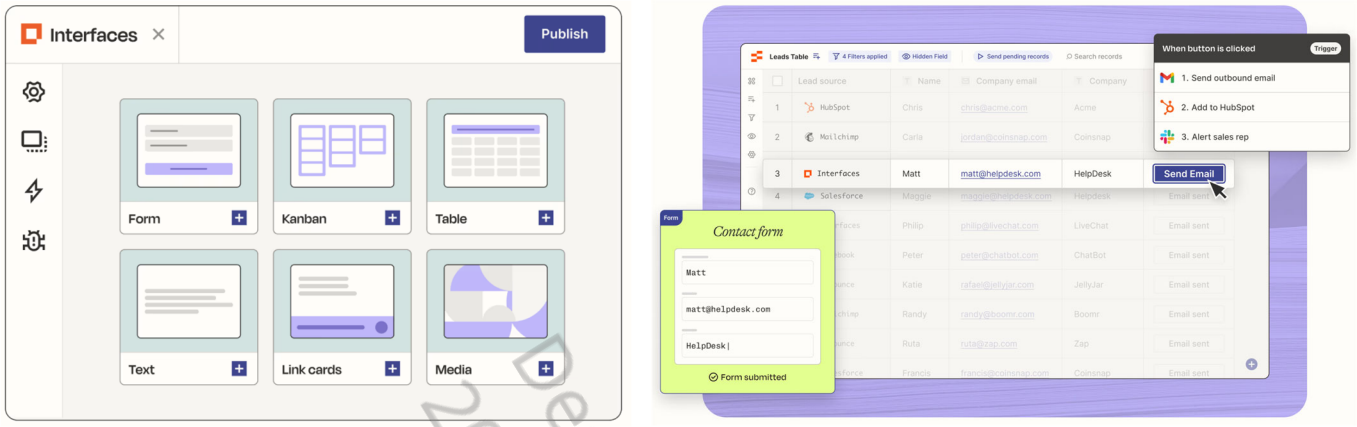
Company Overview and Services Provided

Zapier, Inc. is a cloud-based platform and online automation tool that integrates various web applications and services. Founded in 2012, Zapier is a global organization that is remotely operated and is headquartered in San Francisco, California. Users can create Zaps, which are automated workflows consisting of a trigger and action, that connect two or more applications via their application programming interfaces (APIs). These Zaps automate repetitive tasks without needing the ability to code or rely on developers to build out the integration. Zapier Interfaces and Tables enable users to extend automation workflows by triggering Zaps from user designed no-code web pages and data tables respectively.

In providing these services to users, Zapier serves as the data processor of user personal information, responsible for safeguarding customer content that is transferred in and out of Zaps as data flows through the system, while the users are considered the data controllers.



An example Zap



An example of Interfaces (left) and Tables (right)

Scope of the Description

While Zapier offers multiple services, this description addresses only Zapier's Software-As-A-Service (SaaS) platform provided to user entities and excludes other services provided by Zapier. The description is intended to provide information for user entities of the Zapier SaaS System to obtain an understanding of the SaaS System and the controls over that System relevant to security, availability, confidentiality, and privacy.

Zapier uses Amazon Web Services, Inc. (AWS), a subservice organization, to provide certain off-site data center hosting services. The description includes only the controls of Zapier and excludes the controls of the subservice organization.

Infrastructure

Infrastructure supporting the Zapier application is hosted and managed by AWS. The infrastructure in-scope consists of multiple applications, operating system platforms, and databases, as shown in the table below:

SERVICE CATEGORY	AWS SERVICE TYPE	PURPOSE
Compute	AWS Lambda	Serverless compute machines
	Elastic Compute Services (EC2)	Virtual machines running application

SERVICE CATEGORY	AWS SERVICE TYPE	PURPOSE
	Elastic Kubernetes Service (EKS)	Hosted container orchestration
Data Storage	Simple Storage (S3)	Data Storage
	Relational Database Service (RDS)	Relational database service
	DynamoDB	Database / auto-scaling
	Redshift	Data warehouse
Network	Virtual Private Cloud	Logical network
	Route 53 / Certificate Manager	Domain Name Service (DNS)
	Elastic Load Balancer (ELB)	Load balancer
	AWS WAF / Shield	Firewall
	CloudFront	Content Delivery Network (CDN)
Other	Key Management Services (KMS)	Cryptographic key management
	Guard Duty	Threat Detection

Software and Tools

Zapier's SaaS application is used to provide the services to user entities. 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. Changes to software are made according to the Change Management Policy and Software Development Lifecycle Policy which define baseline hardening standards. Zapier utilizes various tools and software in the daily operation of services provided to user entities as summarized in the table below:

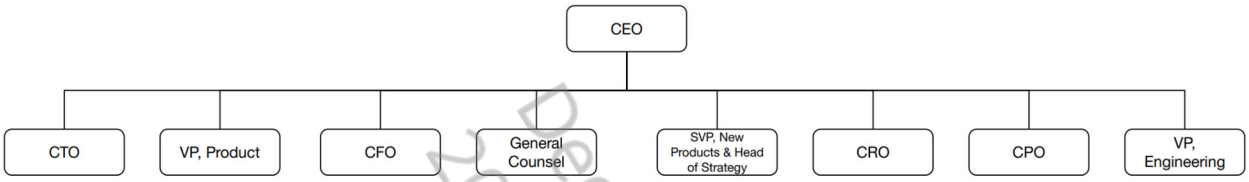
Software	
TOOL	**PURPOSE**
Google Workspace, Slack	Collaboration and Productivity
Okta	Identity and Access Management (IAM)
PagerDuty	Incident Management and Alerting
Datadog, Graylog	Monitoring and Logging
Looker	Analytics
Jira	Project Management and Issue Tracking
Guard Duty, Wiz	Security, Vulnerability, and Threat Detection
Panther	Security Information & Event Management
GitLab	Version Control and Software Development
Zendesk	Customer Support Ticketing
Jamf Pro	Workstation Mobile Device Management (MDM)
Jamf Protect	Workstation Endpoint Detection & Response (EDR)
Redis	Caching Services

Attachment A

Zapier, Inc.'s Principal Service Commitments and System Requirements and Description of the Boundaries of Its Software-As-A-Service System

People

Zapier maintains communication channels to disseminate information regarding control requirements to various 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.

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 aspects of Zapier.

Zapier's Risk Advisory Group is composed of select leadership figures, Security Team members, and the Head of Security, tasked as escalation points for risk management. Members of this group provide guidance on individual risk tolerance relating to their domain within Zapier.

The Security Team is made up of Application Security, Infrastructure Security, Governance, Risk & Compliance, IT Systems Engineering and Security Incident Response. On at least a weekly basis, the Head of Security holds Security Meetings with reporting members to discuss the security review of systems, the status of ongoing projects and production events, including security and incident logs (when applicable). As a contributing function to enterprise-wide risk management, the Security Team is responsible for conducting ongoing assessments to evaluate Zapier's internal compliance with its Information Security Policies.

Data

Zapier maintains a Data Classification & Handling Policy that applies to 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.

Public – Information that can or must be available to the general public.

Internal – Information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized user access, and as such is limited to appropriate users.

Confidential – Information that Zapier considers sensitive to the security of the system. Customer data received, including personally identifiable information, is classified as "confidential" and securely protected.

Personally Identifiable Information (PII) – A sub-classification within Confidential Data. Information that can be used to identify an individual directly, or indirectly when used in combination with another element of data.

Data Storage

Zapier stores data within encrypted AWS S3 and AWS RD. Both are monitored regular data back-ups that are performed by AWS. 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. The Privacy Policy is available on the public website and user entities are responsible for reading the policy and subsequent updates to the policy. Zapier also maintains a Data Processing Addendum (DPA) for the contractual commitments made to paid subscribed users.

Data Transmission

Zapier implements encryption and when transmissions occur as part of the web application, HTTPS and digital certificates are in place. In addition, Zapier data in transit is encrypted using TLS 1.2 or greater.

Data Destruction

Zapier maintains data retention schedules according to data classification type. Customer data is retained and destroyed in accordance with Zapier's Privacy Policy, Data Classification & Handling Policy, and DPA.

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 delineate 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*

Vendor Management

Zapier's Vendor Management Policy details the due diligence and management processes of vendors, their access to customer data, and their impact to security, availability, confidentiality, and privacy of Zapier. This process includes an annual review of attestation report and/or performance of a vendor risk assessment for vendors classified as critical.

Subservice Organizations and Complementary Subservice Organization Controls

Zapier's Software-As-A-Service system uses the subservice organization identified below to perform some of the services provided to user entities. Although the subservice organization has been carved out for the purposes of this report, Zapier management has assumed, in the design of the system, that certain complementary subservice organization controls (CSOCs) would be implemented by the subservice organization. CSOCs that are suitably designed and operating effectively are necessary, along with controls at Zapier, to achieve Zapier's service commitments and system requirements based on the applicable trust services criteria. The CSOCs presented below should not be regarded as a comprehensive list of all controls that should be designed, implemented, or operated by carved out subservice organizations.

The carved out subservice organization and CSOCs relevant to Zapier's Software-As-A-Service system are described in the following table:

Subservice Organizations	Complementary Subservice Organization Controls
Amazon Web Services (AWS)	IT access privileges are reviewed on a periodic basis by appropriate personnel. Two-factor authentication is required over an approved cryptographic channel for authentication to the internal AWS network from remote locations. Physical access to facilities such as data centers, office spaces, and work areas, is added or modified based on authorization from the system's asset owner. Physical access to locations containing sensitive or confidential data is secured via access control mechanisms including locked doors and electronic badging. Monitor systems for availability and uptime 24/7. S3 buckets backups are performed and monitored for successful replication. Customers are notified of breaches and incidents as legally required in accordance with team processes. Data security and privacy commitments are communicated within the Customer Agreement prior to activating an account and available to customers to review at any time on the AWS website.

Complementary User Entity Controls

Zapier management has assumed, in the design of the system, that certain complementary user entity controls (CUECs) would be implemented by user entities. CUECs that are suitably designed and operating effectively are necessary, along with controls at Zapier, to achieve Zapier's service commitments and system requirements based on the applicable trust services criteria. The CUECs presented below should not be regarded as a comprehensive list of all controls that should be designed, implemented, or operated by user entities.

The CUECs relevant to Zapier's Software-As-A-Service system are described in the following table:

	Complementary User Entity Controls
1	User entities should have controls in place for notifying Zapier of suspected breach of security related to the use of the application.