Report on Eventbrite, Inc.’s Software-as-a-Service (SaaS) Solution Relevant to Security, Availability, and Confidentiality Throughout the Period February 1, 2022 to January 31, 2023

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Eventbrite, Inc. ("Eventbrite")

Scope

We have examined Eventbrite's accompanying assertion titled "Assertion of Eventbrite, Inc. Management" (assertion) that the controls within Eventbrite's Software-as-a-Service (SaaS) Solution (system) were effective throughout the period February 1, 2022 to January 31, 2023, to provide reasonable assurance that Eventbrite's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (2017 TSC).

Eventbrite uses a subservice organization to provide cloud-hosting Infrastructure-as-a-Service (IaaS) services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Eventbrite, to achieve Eventbrite's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Eventbrite's controls. 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.

Service Organization's Responsibilities

Eventbrite 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 Eventbrite's service commitments and system requirements were achieved. Eventbrite has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Eventbrite is responsible for selecting, and identifying in its assertion, the applicable trust service 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the 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 Eventbrite'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 Eventbrite'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 Eventbrite's SaaS Solution were effective throughout the period February 1, 2022 to January 31, 2023, to provide reasonable assurance that Eventbrite's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Eventbrite's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Westminster, Colorado
March 29, 2023

Section 2

Assertion of Eventbrite, Inc. Management

Assertion of Eventbrite, Inc. (“Eventbrite”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within Eventbrite’s Software-as-a-Service (SaaS) Solution (system) throughout the period February 1, 2022 to January 31, 2023, to provide reasonable assurance that Eventbrite’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (2017 TSC). Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

Eventbrite uses a subservice organization for cloud-hosting Infrastructure-as-a-Service (IaaS) services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Eventbrite, to achieve Eventbrite’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Eventbrite’s controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organization.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period February 1, 2022 to January 31, 2023, to provide reasonable assurance that Eventbrite’s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Eventbrite’s controls operated effectively throughout that period. Eventbrite’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, 2022 to January 31, 2023, to provide reasonable assurance that Eventbrite’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Eventbrite, Inc.

Attachment A

Eventbrite, Inc.’s Description of the Boundaries of Its Software-as-a-Service (SaaS) Solution

Type of Services Provided

Eventbrite, Inc. (“Eventbrite” or “the Company”) is a United States-based event management and ticketing website. Eventbrite was founded in 2006 to allow users to browse, create, and promote local events. Eventbrite’s platform allows event organizers to plan, promote, and sell tickets to events and publish these events through various marketing channels, including Eventbrite Search/Directory, organizer websites, search indexes, and social media outlets.

The boundaries of the system in this section of the report details the Eventbrite Software-as-a-Service (SaaS) Solution. Any other Eventbrite services are not within the scope of this report.

The Boundaries of the System Used to Provide the Services

The boundaries of the Eventbrite SaaS Solution are the specific aspects of the Company’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Eventbrite SaaS Solution.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

The Company utilizes Amazon Web Services (AWS) to provide the resources to host the Eventbrite SaaS Solution. The Company leverages the experience and resources of AWS to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the Eventbrite SaaS Solution architecture within AWS to ensure the availability, security, and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools, which include the following:

- Public cloud-hosted virtual private clouds (VPCs) via an isolated production account in AWS
- Virtualized network equipment
- Windows and Unix server operating systems (OSs)
- MySQL databases hosted by Amazon Aurora
- AWS native storage solutions
- Multi-availability zone design

Software

Software consists of the programs and software that support the Eventbrite SaaS Solution (OSs, middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor the Eventbrite SaaS Solution include the following applications:

- Eventbrite SaaS application
- Data Foundry SaaS application
- Application monitoring tools: Datadog, PagerDuty, VictorOps, Sentry
- Web application firewall: Signal Sciences (February-October 2022) AWS WAF (October 2022-forward)
- Intrusion detection system (IDS): Threat Stack
- Multi-factor authentication: Duo Security
- Backup and replication software: Aurora and tooling for backup and replication
- Security information and event manager (SIEM) and logging system: rsyslog, Splunk, AWS
- Infrastructure monitoring: Datadog
- Single sign-on and federation services: Okta
- Patch management: InsightVM, Nexpose
- File integrity monitoring: Threat Stack
- Server anti-virus: ClamAV, Rkhunter, Chkrootkit
- Workstation anti-virus: Carbon Black

People

The Company develops, manages, and secures the Eventbrite SaaS Solution via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Information Security Team	Responsible for all aspects of information security across the enterprise, including web and mobile application security, security awareness training, policies and procedures, and some components of compliance such as the Payment Card Industry Data Security Standard (PCI-DSS) program and the SOC (both SOC 2 and 3) programs.
Product and Engineering	Responsible for all aspects of the system development life cycle (SDLC), including product specifications, requirements, design, implementation, testing, release engineering, and on-going maintenance.
Information Technology (IT) Team	Responsible for all technology for internal users, user access to those technologies, and the overall corporate IT environment.

People	
Group/Role Name	**Function**
Human Resources (HR)	Responsible for hiring, training, change of role, and termination practices.
Legal	Responsible for reviewing contracts that customers submit and preparing any custom drafting required for sales contracts, including new and later drafts of contracts or cases where an organizer requests specific legal documentation. Assists if an organizer is in breach of contract and can help answer product-related and privacy-related questions.
Site Reliability Engineering (SRE) Team	Responsible for designing and maintaining the infrastructure that runs Eventbrite, making sure new features and products can work at scale, and keeping the site running in the face of hardware or software issues.

Procedures

Procedures include the automated and manual procedures involved in the operation of the Eventbrite SaaS Solution. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, IT, and HR. These procedures are crafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of the Eventbrite SaaS Solution:

Procedures	
Procedure	**Description**
Policy Management and Communication	How the Company designs and maintains policies and ensures that they are made available to all employees.
Operations Security	How the Company ensures proper management of customer production environments, including change management, capacity management, malware detection and prevention, data backup, logging, security monitoring, vulnerability management, and system patching.
Network Operations	How the Company governs communications security and defines controls related to network security, segregation, network services, transfer of information, and messaging.
Change Management	How the Company manages changes to the architecture and configuration of servers.
Incident Response	How the Company utilizes incident management procedures, including reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence.

Procedures	
Procedure	**Description**
Data Backup and Replication	How the Company carries out regular backups and replication to ensure that the Company can recover from unforeseen events, system failure, and accidental or deliberate loss of information or facilities.
System Development	How the Company develops, maintains, replaces, and enhances software for software products and how it defines a methodology for improving the quality of software and the overall development process.

Data

Encrypted connections are made to the Eventbrite SaaS Solution using a client's virtual private network (VPN) connection, and servers operate following transport layer security (TLS) standards and protocols.

Data collected by the Eventbrite SaaS Solution includes the personal data of users, organizers, and consumers. When a user registers for the services or otherwise submits personal data to the Eventbrite SaaS Solution, it may be associated with other non-personal data (including non-personal data collected from third parties). Data is segmented on multi-tenant MySQL databases hosted by Aurora and secured datastores.

User Entity Responsibilities

Management of user entities is responsible for the following, which should not be regarded as a comprehensive list of all controls that should be employed by user entities.

- User entities should have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames.
- Controls to provide reasonable assurance that the Company is notified of changes in:
  - User entity vendor security requirements
  - The authorized users list
- It is the responsibility of the user entity to have policies and procedures to:
  - Inform their employees and users that their information or data is being used and stored by the Company.
  - Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
- User entities should only grant access to the Company's system to authorized and trained personnel.
- Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.
- User entities should deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.

Subservice Organization and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS as a subservice organization for cloud-hosting Infrastructure-as-a-Service (IaaS) services. Eventbrite's controls related to the Eventbrite SaaS Solution cover only a portion of the overall internal control for each user entity of the Eventbrite SaaS Solution.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. CSOCs are expected to be in place at AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the AWS SOC 2 report annually. In addition, through its operational activities, Eventbrite management monitors the services performed by AWS to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with AWS to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the Eventbrite SaaS Solution to be achieved solely by Eventbrite. The CSOCs that are expected to be implemented at AWS are described below.

Criteria	Complementary Subservice Organization Controls
CC6.4	• AWS restricts data center access to authorized personnel. • AWS monitors data centers 24/7 by closed circuit cameras and security personnel.
CC6.5 CC6.7	• AWS securely decommissions and physically destroys production assets in its control.
CC7.2 A1.2	• AWS installs fire suppression, fire detection, and environmental monitoring systems at data centers. • AWS protects data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS oversees the regular maintenance of environmental protections at data centers.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the Eventbrite SaaS Solution. Commitments are communicated in the Terms of Service, Privacy Policy, and Data Processing Addendum (DPA). The Company's principal service commitments related to the Eventbrite SaaS Solution include the following:

Trust Services Category	Service Commitments
Security	• Eventbrite will implement technical and organizational security measures that are designed to protect customer data against unauthorized or unlawful processing, accidental loss, destruction, damage, alteration, or disclosure. • In the event of a data security breach, Eventbrite will notify the event organizer without undue delay and will provide reasonable assistance where applicable.
Availability	• Eventbrite will maintain the availability of the system.
Confidentiality	• Upon the organizer's written request, Eventbrite will return, delete, or destroy the confidential customer data processed on the organizer's behalf and copies thereof.

System requirements are specifications regarding how the Eventbrite SaaS Solution should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures, which are available to all employees. The Company's system requirements related to the Eventbrite SaaS Solution include the following:

- Employee provisioning and deprovisioning standards
- Logical access controls, such as the use of user IDs and passwords to access systems
- Protection of data in transit
- Protection of data at rest
- Risk assessment and risk mitigation standards
- System monitoring
- Change management procedures
- Incident response plans and tests
- Confidentiality agreements
- Background checks