



MAPBOX, INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE WEB SERVICES SYSTEM

FOR THE PERIOD OF MARCH 1, 2022, TO FEBRUARY 28, 2023

Attestation and Compliance Services



Proprietary & Confidential

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

INDEPENDENT SERVICE AUDITOR'S REPORT

To Mapbox, Inc.:

Scope

We have examined Mapbox, Inc.'s ("Mapbox") accompanying assertion titled "Assertion of Mapbox, Inc. Service Organization Management" ("assertion") that the controls within Mapbox's Web Services system ("system") were effective throughout the period March 1, 2022, to February 28, 2023, to provide reasonable assurance that Mapbox's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Mapbox uses a subservice organization for cloud hosting 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 Mapbox, to achieve Mapbox's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system 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.

Service Organization's Responsibilities

Mapbox 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 Mapbox's service commitments and system requirements were achieved. Mapbox has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Mapbox 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 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 systems 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 Mapbox's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Mapbox'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.

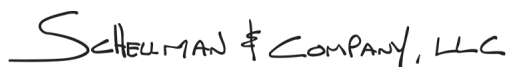
Inherent Limitations

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 Mapbox'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 Mapbox's Web Services system were effective throughout the period March 1, 2022, through February 28, 2023, to provide reasonable assurance that Mapbox's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

SCHILLMAN & COMPANY, LLC

Washington, District of Columbia
April 7, 2023

ASSERTION OF MAPBOX SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Mapbox, Inc.'s ("Mapbox") Web Services system ("system") throughout the period March 1, 2022, to February 28, 2023, to provide reasonable assurance that Mapbox's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented below 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 March 1, 2022, to February 28, 2023, to provide reasonable assurance that Mapbox's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Mapbox's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 March 1, 2022, to February 28, 2023, to provide reasonable assurance that Mapbox's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE WEB SERVICES SYSTEM

Company Background

Mapbox, Inc. was incorporated in 2013 and is based in Washington D.C. Mapbox, Inc. operates a location data platform that enables users to design and publish custom location data for mobile and web applications. Mapbox serves web and social, logistics, transportation, automotive, fitness and outdoors, natural resources, agriculture, real estate, insurance, security, finance, drones, government, health, media, and travel industries in the United States and internationally.

Description of Services Provided

Mapbox runs a location data platform for developers to bring location-based experience to life in their applications. Mapbox provides open and closed source libraries, SDKs, and APIs for maps, navigation, and geolocation search. These tools empower enterprises to analyze their data, drone companies to publish flyovers, real estate sites to visualize properties, satellite companies to process cloud-free imagery, automotive companies to create immersive navigation experiences, and insurance companies to track assets.

Mapbox APIs allow for programmatic access to Mapbox tools and services. These APIs allow consumers to retrieve information about their accounts, upload, and change resources, and use core Mapbox tools, like geolocation search and navigation. Mapbox uses telemetry from Mapbox SDKs to improve maps, directions, travel times, and search. Mapbox collects and anonymizes data about how users interact with Mapbox services to help developers build better location-based applications. Telemetry is used to discover missing roads, determine turn restrictions, build speed profiles, and otherwise improve Mapbox products and services.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principal Service Commitments and System Requirements

The principal service commitments Mapbox makes to customers related to security and availability are documented and communicated in the customer and vendor contracts provided by Mapbox. Specific commitments communicated by Mapbox for protecting customer data include, but are not limited to, the following:

- To maintain an information security program that seeks to align with generally accepted standards and is intended to minimize security and privacy risks to the service.
- To conduct annual third-party security and penetration testing.
- To make the service available according to a Service Level Agreement (SLA) of 99.9% of the time for Enterprise customers, as measured over the course of each one-calendar month excluding, without limitations, downtime due to scheduled maintenance, emergency maintenance, or other circumstances outside of Mapbox's unreasonable control.
- To provide publicly available transparency reports detailing government demands for user data on a quarterly basis.

Mapbox establishes operational and system requirements to support aspects of the information security program which include policies and procedures, access controls, training and awareness, continuity, encryption, vulnerability management, service provider security, and continuous monitoring. Such requirements enable Mapbox to deliver on security and availability service commitments in addition to complying with relevant privacy laws and regulations the service is subject to.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

Primary Infrastructure			
Production Application	Business Function Description	Operating System Platform	Physical Location
Maps, Search, Navigation	Serve map, geocoding, and traffic-enabled directions.	Amazon EC2 + Docker / AWS Elastic Container Service (ECS) / AWS Lambda	Multiple AWS regions
		AWS DynamoDB	
Telemetry	Collection of probe events which power real-time traffic for directions.	Amazon EC2 + Docker / AWS ECS / AWS Lambda / AWS Kinesis	
		AWS DynamoDB	
Firewall Systems	Protects the network perimeter and limits inbound and outbound access.	AWS Virtual Private Cloud (VPC)	

People

Personnel involved in the operation and use of the system are:

- Executive management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Human resources (HR) – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
- Legal – responsible for managing the enterprise’s legal obligations.
- Engineering Manager, Data Platform – responsible for availability of services, management of availability on-call schedule, hiring manager for the Data Platform team.
- Head of Security & Compliance – responsible for security issues and handling of security incidents, managing security on-call schedule, setting security policy across the company.
- Data Platform team – responsible for availability monitoring, holding on-call shifts, capacity planning and management, cost.
- Security & Compliance team – responsible for security monitoring and holding on-call shifts, security incident response and escalation, company-wide security training.
- IT team – responsible for managing system access and operational support to Mapbox employees.

Procedures

Access, Authentication and Authorization

Only AWS identity and access management (IAM) user accounts approved by the Mapbox Data Platform and Security & Compliance teams can access Mapbox production environments. Initial AWS IAM account setup requires a Mapbox Okta account and a two-factor authentication (2FA) device. After setup, logging in to the AWS console requires a 2FA token, which allows a user to assume an IAM role with temporary credentials. No passwords are used or transmitted. Direct access to servers on AWS requires a 2FA token, secure shell (SSH) key matching (key and secret), and certificate pinning. Firewall systems are in place to filter unauthorized inbound network traffic from the Internet. Web servers use Transport Layer Security (TLS) encryption for web communication sessions. Mapbox security policies prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted. Employee laptops and devices are encrypted, password protected, and enrolled in a central mobile device management (MDM) system by the Mapbox IT team.

Access Requests and Access Revocation

Mapbox systems use role-based access control (RBAC) and the principle of least privilege to assign employees to groups based on their teams or job responsibilities. Access changes related to an employee's team membership or job responsibilities require the approval of a manager. Requests to change a given team's resources or permissions are documented in a ticketing system and require approval of the Mapbox IT team and management. When an employee leaves the company, Mapbox HR and IT teams complete a termination checklist which includes revoking access from Mapbox systems. Quarterly, user logical access reviews are performed by management to ensure that role-based access is provisioned to Mapbox internal users based on the principle of least privilege and that terminated personnel have not retained active access to internal environments. Accounts identified as inappropriate are investigated and resolved.

Change Management

Mapbox engineering teams follow documented engineering standards for release and change management. Engineering teams hold regular scrum meetings to discuss past, ongoing, and upcoming changes that affect their systems. High-level change management meetings are held on a weekly basis inclusive of all ongoing and upcoming projects. Mapbox uses GitHub for software version control and source code. Production repositories use main ("master") branch protection. Pull requests require at least one other code reviewer, with exceptions for emergency deploys in response to incidents. Production repositories have automated tests that run on continuous integration (CI) infrastructure after every commit. Engineering teams coordinate application bug fixes, enhancements, documentation, and feature requests via centralized, shared, and persistent means. Production repositories also require a README and documentation about the project, its configuration, alarms, diagnostics, and troubleshooting. Network and systems personnel create GitHub issues for system/maintenance change requests (e.g., patches, firewall changes, etc.). The production environment is logically segmented from the development and test environments. Changes to production APIs that affect users are documented in the public API changelog in <https://www.mapbox.com/api-documentation/changelog.html>. Launches of new APIs and major changes to existing APIs undergo an availability and security launch review process.

Risks that are identified during the formal risk assessment and require application change or system/maintenance change follow the change management process. The Security & Compliance team discusses incidents, including corrective measures, during their daily scrum meetings. Incidents requiring application changes or system/maintenance changes follow engineering standards.

Data Backup and Disaster Recovery

Core Mapbox databases are automatically replicated across multiple, geographically distributed AWS regions. Backups are made on a daily basis and are stored, encrypted, on a 99.99999999% durable storage medium. Access to all backups is restricted. Restore testing is performed on a quarterly basis.

Mapbox has a disaster recovery plan that includes procedures for communications, contacting AWS support, regional failover, anti-DDoS mitigation, data recovery, and data restoration. Mapbox performs continuous disaster recovery testing that is embedded in the Mapbox platform by design.

Mapbox uses AWS CloudWatch to monitor central processing unit (CPU), memory, and disk utilization of AWS EC2 compute resources. These threshold-based alarms page members of the applicable service team via PagerDuty for review. Throughout the day Mapbox Web Services auto scale in and out of multiple AWS regions to meet global demand. Compute resources are grouped in clusters of similar families and types. Clusters are also cost optimized and resilient to regional failure. In case of disaster or an outage, AWS Route53 domain name system (DNS) records will automatically fail over web services to another AWS region.

Incident Response

The Mapbox Security & Compliance and Service Teams maintain an on-call rotation for responding to security and availability incidents. Escalation procedures are documented on the Mapbox Confluence platform, and employees are trained on how to quickly report incidents and issues. The Security & Compliance and Data Platform teams review recent security and infrastructure availability incidents as needed. The Security & Compliance team maintains an Incident Response Framework (IRF) that documents the process and expectations for parties involved in triaging a security incident. After major incidents, Service Teams publish post-mortem reflections in a central document repository. Employees can view a dashboard of active internal security and availability incidents on the Mapbox intranet. During or after a major security incident the Security & Compliance team may post an announcement on the company-wide Slack channel. Incidents from all engineering teams are presented and discussed in a weekly company-wide meeting. Mapbox publishes guidance for users, customers, and security researchers to report security incidents and vulnerabilities. Mapbox runs a public bug bounty program that rewards security researchers for responsibly reporting and disclosing security vulnerabilities in Mapbox products and infrastructure. The Security & Compliance team publishes security advisories for Mapbox products and libraries on the security bulletins page and obtains common vulnerabilities and exposures (CVEs) or Node Security Project (NSP) advisories when necessary.

System Monitoring

Mapbox uses a variety of in house and third-party intrusion detection systems (IDS) to detect, alert, and report on possible or actual network security breaches. The in-house patrol-service monitors for security violations, insecure actions, and possible breaches in AWS and GitHub. Patrol-service also integrates with AWS GuardDuty for machine learning based host intrusion and anomaly detection. The in-house SSH Police tool logs SSH activity on production servers and alarms on unauthorized logins. SumoLogic logs production systems events and monitors for and alerts on anomalous activity. Mapbox IDS systems use PagerDuty to alert on-call members of the Security & Compliance and Service Teams via e-mail, push message, phone call, and short message service (SMS) notifications. A central antivirus server is configured with antivirus software to protect registered production Windows servers and workstations with the following configurations: scan for updates to antivirus definitions and update registered clients hourly; scan registered clients on a daily basis.

Data

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
Private customer datasets	Customers fetch data via API calls.	Confidential
API server logs	Not provided to customer, but contains sensitive information, like referrers, internet protocol (IP) addresses, directions requests, geocoding requests, and area of map loaded.	

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
Telemetry data	Sent from Mapbox SDKs back to Mapbox and used to create real-time traffic profiles of road network and related products. Not provided back to customer. Some aggregated and anonymized derivatives may be used to power other products offered to customers.	Confidential
Global street map database	Customers fetch street map data via API calls.	Public
Geocoding data	Customers make geocoding requests from API calls.	
Directions data	Customers make directions requests from API calls.	

Subservice Organizations

The cloud hosting services provided by AWS were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, alone or in combination with controls at Mapbox, and the types of controls expected to be implemented at AWS to meet those criteria.

Control Activities Expected to be Implemented by AWS	Applicable Trust Services Criteria
AWS is responsible for managing the logical access to the underlying network, virtualization management, and storage devices for its Infrastructure-as-a-Service (IaaS) cloud hosting service where Mapbox systems reside.	CC6.1, CC6.2, CC6.3, CC6.5, CC6.6, CC7.1
AWS is responsible for ensuring physical access control systems are in place to restrict access to and within the data centers housing the offline storage, backup data, systems, recovery infrastructure and media (including portable media), to properly authorized individuals.	CC6.4, CC6.5
AWS is responsible for the encryption and replication of backup data to a geographically diverse site.	CC6.7
AWS is responsible for restricting physical access to backup media, identifying, and addressing environmental vulnerabilities, and changing environmental conditions through the use of environmental protections.	A1.2

Complementary Controls at User Entities

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security and availability categories are applicable to the Web Services system.