BITSIGHT

BitSight Technologies, Inc.

Independent Service Auditor's SOC 3 Report

For the

Security Ratings Platform

For the Period of September 1, 2022, to August 31, 2023

Attestation and Compliance Services

schellman
Quality, above all.

INDEPENDENT SERVICE AUDITOR'S REPORT

To BitSight Technologies, Inc.:

Scope

We have examined BitSight Technologies, Inc.'s ("Bitsight") accompanying assertion titled "Assertion of BitSight Technologies, Inc. Service Organization Management" ("assertion") that the controls within Bitsight's Security Ratings Platform and VisibleRisk ("systems") were effective throughout the period September 1, 2022, to August 31, 2023, to provide reasonable assurance that Bitsight's service commitments and system requirements were achieved based on the trust services criteria relevant to security (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)*.

Bitsight 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 Bitsight, to achieve Bitsight'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

Bitsight 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 Bitsight's service commitments and system requirements were achieved. Bitsight has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Bitsight 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 Bitsight'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 Bitsight'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 Bitsight'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 Bitsight's Security Ratings Platform and VisibleRisk systems were effective throughout the period September 1, 2022, through August 31, 2023, to provide reasonable assurance that Bitsight's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Washington, District of Columbia
September 19, 2023

Assertion of Bitsight Service Organization Management

We are responsible for designing, implementing, operating, and maintaining effective controls within BitSight Technologies, Inc.'s ("Bitsight") Security Ratings Platform and VisibleRisk ("systems") throughout the period September 1, 2022, to August 31, 2023, to provide reasonable assurance that Bitsight's service commitments and system requirements relevant to security 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 September 1, 2022, to August 31, 2023, to provide reasonable assurance that Bitsight's service commitments and system requirements were achieved based on the trust services criteria relevant to security (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)*. Bitsight's objectives for the system in applying the 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 September 1, 2022, to August 31, 2023, to provide reasonable assurance that Bitsight's service commitments and systems requirements were achieved based on the applicable trust services criteria.

Description of the Boundaries of the Security Ratings Platform System

Company Background

Bitsight is a cybersecurity risk management company based out of Boston, Massachusetts dedicated to helping customers identify, quantify, and mitigate security risks. Bitsight Security Ratings Platform and VisibleRisk systems are used by leaders in the financial services, healthcare, retail, technology, and defense sectors to address a number of security risk management issues. Bitsight is used by organizations around the world for vendor risk management, mergers and acquisitions, benchmarking security performance, and cyber insurance underwriting. Bitsight users include Chief Information Security Officers, Chief Risk Officers, Risk Managers, Security Directors, and Cyber Insurance Underwriters from organizations. Founded in 2011, Bitsight is backed by Comcast Ventures, GGV Capital, Liberty Global, Menlo Ventures, Globespan Capital Partners, Flybridge Capital Partners, Commonwealth Capital Ventures, SingTel Innov8, the National Science Foundation, Warburg Pincus, and Moody’s.

Description of Services Provided

The Bitsight Security Ratings Platform system is a Software as a Service (SaaS) offering that gives customers insights into the information security posture of companies using an outside-in approach. Ratings are generated from data that includes evidence of system compromises, such as botnets and other malware, security diligence practices, such as SSL configurations and open ports, and evidence of file-sharing activities on a company's network. Users can log in to the platform using a browser, either with credentials provided by Bitsight or using the Single Sign-On (SSO) capabilities of their organizations. Ratings and associated data are updated every day, and customers can choose to receive alerts about changes in their Bitsight portfolio. Customers have the ability to export data in a comma-separated value (CSV) format as well as via an application program interface (API). A Bitsight security rating is a number from 250 to 900 that describes a company's internet security posture and serves as a measure of its risk. Each organization's rating falls into one of three categories: Basic, Intermediate, or Advanced. Organizations with high ratings historically have strong security postures and provide the lowest risk.

The Bitsight VisibleRisk Platform system is a SaaS offering that gives customers insights into the information security posture of companies using an outside-in approach. VisibleRisk is a cybersecurity-focused company creation platform, that is focused on creating a standard benchmark for communicating cyber risk to Boards of Directors and senior business executives in order to improve the global dialog about this important issue. The risk rating incorporates the requisite external and internal factors that impact an organization’s cyber risk.

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

Bitsight designs its processes and procedures to meet the security criteria for its Security Rating Platform and VisibleRisk systems. Those objectives are based on the service commitments that Bitsight makes to user entities, the laws and regulations that govern the Security Ratings Platform and VisibleRisk systems, and the financial, operational, and compliance requirements that Bitsight has established for the services.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

The principal security commitments are standardized and include, but are not limited to, the following:

- Maintain an information security program designed to take reasonable steps to protect the personal information provided via the Sites and Services from loss, misuse, and unauthorized access, disclosure, alteration, or destruction.
- Maintain administrative and logical safeguards to protect the security and integrity of the Security Rating Platform and VisibleRisk systems and customer data in accordance with Security Rating and VisibleRisk's security requirements.
- Use formal access management processes for the request, review, approval, and provisioning of Bitsight personnel with access to production systems.
- Use commercial industry-standard secure encryption methods to protect customer data at rest and in transit.

Bitsight establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Bitsight's system policies and procedures, system design documentation, and contracts with customers.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the customer data platform.

In accordance with Bitsight's 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 and Software

Bitsight's Security Ratings Platform and VisibleRisk systems are hosted in AWS. Bitsight's Security Ratings Platform and VisibleRisk systems are hosted in a Virtual Private Cloud (VPC) located in the Amazon East Coast service location.

Bitsight relies on a layered approach to access security, requiring customers and employees to pass through different authentication points before connecting to the appropriate systems and data. These authentication layers may include:

- Network Infrastructure Authentication
- Operating System Authentication
- Application Authentication (i.e., web-based)
- Database Authentication (dependent on the application)

Access to each layer is controlled and monitored by Bitsight operations personnel through formal defined authorization, approval, and monitoring processes. Authentication at the network, operating system, and database layers (network and infrastructure layers) incorporates a number of additional security measures, including firewalls, routers, unique user ID accounts, multi-factor authentication, and the use of Secure Socket Shell (SSH) keys.

People

The IT Services' organizational structure provides the overall framework for planning, directing, controlling, and monitoring business operations. Employees and business functions are separated into departments according to operational responsibilities. The Bitsight organization structure has been formally defined and documented. The structure also provides defined job titles and lines of authority for reporting and communication. The following are the functional areas of operation within Bitsight:

- Executive Management - This area oversees operations. The executive team includes the:
  - Chief Executive Officer (CEO), Chief Financial Officer (CFO), Chief Customer Officer (CCO).
  - Chief Technology Officer (CTO), Chief Marketing Officer (CMO), Chief People Officer (CPO).
  - Chief Strategy Officer (CSO), General Counsel, Chief Risk Officer (CRO), Chief Product Officer (CPO).
- Customer Success - This area supports Bitsight customers.
- Data Science - This area curates data sources for the Security Ratings Platform system.
- Engineering - This area develops and manages the core software platform.
- Finance - This area performs financial management and accounting functions.
- Information Technology (IT) + Internal Security + Governance, Risk, and Compliance (GRC) - This area oversees and manages the Bitsight information security program and leads security and compliance activities for the organization, as well as the product.
- Marketing - This area performs marketing operations.
- Operations - This area is the custodian of AWS-managed infrastructure and deployments.
- Product Management - This area manages product features.
- Sales - This area performs sales operations and business development functions.
- Sales Engineering - This area provides pre-sales support.
- Human Resources and Recruiting - This area supports all employees throughout their life cycle, including hiring, onboarding, training and development, compensation and benefits management, performance management, and offboarding.

Procedures

Access, Authentication, and Authorization

Access to the system information is protected by authentication and authorization mechanisms. Administrative access to production systems is restricted to authorized personnel.

Access Requests and Access Revocation

A formal process has been established to manage user access requests, modifications, and deletions. Onboarding Employee access to protected resources is created or modified by the IT department based on the role initiated via an appropriate request from the HR department. Access requests are approved by the group manager or asset owner. Bitsight IT uses the principle of least privilege to help ensure access is appropriate. Additionally, employees can request additional tools/services needed to perform their job functions. These requests are subject to approval by management.

The IT department disables user accounts for terminated employees based on management and HR requests through the use of employee termination request forms. Access to Bitsight resources is revoked when notification is received by IT from the HR team, VP of Finance, or the employee's Director. Additionally, user access rights on the Security Ratings Platform and VisibleRisk systems are reviewed on at least a quarterly basis.

Network Security

External points of connectivity are protected by an industry-standard firewall. Access to make changes to the firewall configurations is restricted to appropriate personnel, and firewall configurations, and security group appropriateness are reviewed on an annual basis by the security engineering team to assess the suitability of rulesets and confirm business justifications exist. Workstations and servers are protected from malware and viruses via an antivirus tool configured to download real-time updates and run periodic scans. Logging is enabled on the network to capture and analyze anomalies to identify security events. These activity logs are retained for subsequent review in case further evaluation is required.

Endpoint Security

An enterprise Mobile Device Management (MDM) as well as an enterprise Endpoint Detection and Response (EDR) is deployed to all company-issued laptops. A mobile MDM is required on employee personal mobile devices who wish to access their company e-mail account.

Change Management

Application development includes the development of new features and changes based on business requirements and application bug fixes. Bitsight follows agile software principles for software development and applies a systematic approach to managing change so that changes to customer-impacting services are reviewed, tested, approved, and well-communicated. A documented change management policy exists and describes the development, acquisition, implementation, and maintenance processes for in-scope system changes.

Incident Response

A defined incident response program for reporting and how to report operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so) is published to enable personnel to understand, contain, remediate, and communicate security incidents as appropriate. The information security incident response plan is triggered when an information security incident is determined to have occurred. Bitsight employees, customers, and third parties may report suspected incidents to IT via multiple paths for follow-up and resolution.

System Monitoring

Bitsight utilizes monitoring software to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. Upon detection of an unusual system activity, the software creates a ticket automatically, which is routed to the appropriate personnel. This includes the use of a vulnerability scanning tool that is configured to perform various scans of the application continuously to identify vulnerabilities that could be exploited. Critical findings and evidence of resolution are followed up to resolution.

Data

The primary types of data handled by Bitsight are publicly observable security metrics and events. When malicious activity occurs on a network, evidence of that activity is often observable from outside the organization. Bitsight focuses on gathering as much of this externally available evidence as possible. Bitsight does not conduct intrusive penetration testing on the organization being rated, nor does it ask them questions about their network policies or procedures. Each day, Bitsight automated systems collect billions of security measurements about organizations and across industries, using sensors (sinkholes) deployed across the globe. Some of these sensors are owned and operated by our partners, while others are owned by Bitsight. Bitsight manages one of the world's largest sinkhole networks. Policies for data classification and protection are documented and are accessible to staff in the Information Security Policy via the Company's intranet.

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 Bitsight, and the types of controls expected to be implemented at AWS to achieve Bitsight service commitments and system requirements based on the applicable trust services criteria.

Control Activities Expected to be Implemented by AWS	Applicable Trust Services Criteria
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Bitsight applications reside.	CC6.1 - CC6.3, CC6.6 - CC6.7
AWS is responsible for restricting and monitoring physical access to data center facilities, backup media, and other system components for its cloud hosting services where the production systems reside.	CC6.4, CC6.5, CC7.2

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 categories are applicable to the Security Ratings Platform and VisibleRisk systems.