BITSIGHT

BitSight Technologies, Inc.

Independent Service Auditor's SOC 3 Report

For the Security Rating Platform System

For the Period of September 1, 2021, to August 31, 2022

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 Rating Platform system ("system") were effective throughout the period September 1, 2021, to August 31, 2022, 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; and
- 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.

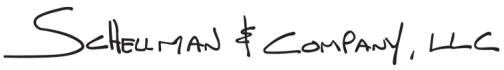
Inherent limitations

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 Rating Platform system were effective throughout the period September 1, 2021, through August 31, 2022, 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
October 20, 2022

ASSERTION OF BITSIGHT SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within BitSight Technologies, Inc.'s ("BitSight") Security Rating Platform system ("system") throughout the period September 1, 2021, to August 31, 2022, 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, 2021, to August 31, 2022, 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, 2021, to August 31, 2022, 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 RATING 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 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 their 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.

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 system. Those objectives are based on the service commitments that BitSight makes to user entities, the laws and regulations that govern the Security Rating Platform system, and he 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 system and customer data in accordance with Security Rating'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

The BitSight Security Rating Platform system is hosted within Amazon Web Services (AWS) in a Virtual Private Cloud (VPC) located in Amazon's East Coast service location. The infrastructure is summarized as follows:

- Amazon Relational Database Service (RDS)
- Amazon Elastic Block Store+ Simple Storage Services (S3) for storage.
- Amazon Elastic Load Balancers and Application Load Balancers for high availability.
- Amazon Elastic Kubernetes Service (EKS) to manage BitSight's Kubernetes clusters and Secrets Manager for credentials/ API tokens for services.
- Amazon VPCs to logically isolate sections of AWS.

BitSight's Security Rating Platform relies on a layered approach to access security, requiring employees to pass through different authentication points before connecting to the appropriate systems and data.
These authentication layers may include:

- Network Infrastructure 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.

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

Primary Infrastructure			
Production System	**Business Function Description**	**Operating System Platform**	**Physical Location**
Okta	Authenticates and authorizes BitSight personnel accessing the production network.	Okta	AWS US-East
Security Rating Application	The BitSight product provides security ratings to customers of their third parties and own entities	Linux	
Virtual Server Management Consoles / Firewall System	AWS administrative console used for managing virtual machines, security groups, and route tables.	AWS hosted web servers	
Virtual Private Network (VPN)	SSL VPN client utilized for secure remote access to the production environment. .	Pritunl	
Production Server Operating Systems	Application and database servers supporting the BitSight SaaS Platform.	AWS EKS	
RDS	Allows a user to set up, operate, and scale a relational database in the cloud while managing database administration tasks.	MySQL	
AWS S3	Database storage for customer data.	AWS	

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.
- 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

Documented logical access policies and standard build procedures are in place to guide BitSight personnel in information security practices that include, but are not limited to, password requirements, access provisioning, access termination, and the installation and maintenance of production servers. Access to system information by BitSight personnel is protected by multiple authentication and authorization mechanisms. VPN software is used to restrict remote access to only authorized users. BitSight requires multifactor authentication (MFA) over an approved VPN service for access to internal AWS resources. Users who wish to gain access to the Security Ratings Platform system are required to authenticate with a valid SSH key only (passwords are disabled). SSH authentication. The Security Ratings Platform system has defined roles and application privileges to restrict access to information within the systems to authorized users. Information system access is limited to authorized users, processes acting on behalf of authorized users or devices (including other information systems), and the types of transactions and functions that authorized users are permitted to exercise. Administrator access to in-scope systems is restricted to user accounts accessible by authorized personnel The concepts of least privilege and separation duties are enforced. Each user is assigned a unique user ID to access the system once they have been approved. Sharing of user accounts is not permitted. Privileged internal BitSight access to sensitive resources is restricted to defined user roles, and access to these roles is approved by IT management. Privileged customer accounts are created based on a written authorization request from the designated customer point of contact. These accounts are used by customers to create customer user accounts. A master list of the organization's system components is maintained, accounting for additions and removals, for management's use.

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. The BitSight IT department has implemented standard access, which is granted to users based on their job titles and responsibilities. The addition or modification of user accounts is performed by the IT Group based on authorized requests from management and HR for new hires and contractors. New-hire access to product-related infrastructure resources and tools, including, but not limited to, network configurations, storage, and elastic compute cloud (EC2) instances, are assigned based on Identity and Access Management (IAM) roles developed by IT, based on the new hire's job description. 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, or the employee's Director. Access to BitSight services is revoked by disabling the user's SSO account and any additional BitSight-related accounts not supported by the SSO service. Access to infrastructure is revoked by removing the AWS IAM account permissions and disabling VPN access. Additionally, user access rights on the security ratings platform 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. All company-issued laptops are FileVault2 encrypted via the MDM. Lastly, 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. A change proposal is sent by the change initiator to the change management team to request a change through the change management ticketing system utilized to track change requests and approvals. The change management team reviews the change request and performs a risk and impact assessment, as necessary. After their review, the change management team approves the proposal, if appropriate; otherwise, the proposal is rejected. The change proposal is communicated to any parties that will be affected by the proposed change. Once approved by the change management team, development of the change begins. Once development is completed, changes are tested and approved prior to migration to production within a repository system that is configured to send a notification to IT personnel after application changes are implemented into production. The change management team helps ensure that issues noted during testing are resolved. Once testing is complete, management reviews the change and provides approval to move the change to production. Post-implementation procedures are designed to verify the operation of system changes are performed. Separate environments exist to segregate development, test, and migration activities. The repository system is utilized to restrict access to application source code and provide rollback capabilities if required. The ability to migrate changes to production and build within the development environment is segregated and restricted to appropriate personnel.

Additionally, a file integrity monitoring system is in place and configured to alert the IT security personnel when updates are made to the production libraries. Administrative access to the file integrity monitoring system is restricted to user accounts accessible by authorized personnel.

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. An information security incident is defined as any event that comprises or is likely to result in compromise of the confidentiality, integrity, or availability of an information asset- which may include one or more of the following:

- Unauthorized access to or acquisition of Sensitive Information
- Corruption of information
- Theft of IT resources
- Any evidence of unauthorized activity, including the detection of unauthorized wireless access points, critical intrusion detection alerts, and reports of unauthorized critical system or content file changes.

The Incident Manager will be the primary point of contact for receiving reports of incidents and will enter these reports into the appropriate internal software tool/storage solution. The Incident Manager will make an initial assessment and rate the potential severity level of the incident in accordance with the incident response plan. Following the assessment, an incident response team is formed, and activities are implemented to contain the incident and isolate the damage. The cause of the incident is determined, and the information security team implements activities to eradicate the incident and restore the affected systems to the unaffected state. Affected parties are notified of the incident as appropriate based on the risk impact level. Once an incident has been

remediated, the affected systems and/or data repaired and recovered, and the affected parties notified, a post-mortem analysis of the compromised system is performed to review the information gathered and to gain an understanding of the weaknesses that resulted in the incident as well as to identify other potentially vulnerable areas. For high-severity incidents, a root-cause analysis is prepared and reviewed by operations management. Based on the root-cause analysis, change requests are prepared, and the entity's risk management process and relevant risk management data is updated to reflect the planned 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.

A system security policy is in place to guide personnel on minimum technical requirements and configurations for in-scope systems. BitSight monitors backup activities through AWS's console. Daily full backups are configured for critical production data. The operations team will verify that successful backups are completed, and restorations of production programs and data can be performed when necessary. If errors or failures occur during the backup process, the operations team documents the steps necessary to remediate the backup failure within a support ticket. Access to modify the backup schedules is restricted to authorized operations personnel only.

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 meet those 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 implementing controls to restrict physical access to the production systems.	CC6.4
AWS is responsible for restricting logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the BitSight applications reside.	CC6.5

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 category are applicable to the Security Rating Platform system.