BitSight Technologies, Inc.

System and Organization Controls (SOC) 3

Report on BitSight Technologies, Inc.'s Security Ratings Platform System Relevant to Security

Throughout the Period
September 1, 2019 to August 31, 2020

BITSIGHT

Contents

I. Independent Service Auditor's Report

Tel: 617-422-0700
Fax: 617-422-0909
www.bdo.com

One International Place
Boston, MA 02110

Independent Service Auditor's Report

To the Management of
BitSight Technologies, Inc.
Boston, Massachusetts

Scope

We have examined BitSight Technologies, Inc.'s (BitSight or service organization) accompanying assertion titled *Assertion of BitSight Technologies, Inc. Management* (assertion) that the controls within BitSight's Security Ratings Platform System were effective throughout the period September 1, 2019 to August 31, 2020, 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, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

BitSight uses Amazon Web Services (AWS), a subservice organization, to provide data center services. 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. Section III presents the types of complementary subservice organization controls assumed in the design of BitSight'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.

Complementary user entity 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. Section III presents the complementary user entity controls assumed in the design of BitSight's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

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 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 service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of 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 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.

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 the service organization'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 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.

Emphasis of Matter

The World Health Organization classified the COVID-19 outbreak as a pandemic in March 2020. Based on the rapid increase in exposure globally, the gravity or length of the impact of the COVID-19 outbreak cannot be estimated at this time.

Opinion

In our opinion, management's assertion that the controls within BitSight's Security Ratings Platform System were effective throughout the period September 1, 2019 to August 31, 2020, 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.

Restricted Use

This report is intended solely for the information and use of BitSight, user entities of BitSight's Security Ratings Platform System during some or all of the period September 1, 2019 to August 31, 2020, business partners of BitSight subject to risks arising from interactions with the Security Ratings Platform System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

BDO USA, LLP

January 15, 2021

II. Assertion of BitSight Technologies, Inc. Management

111 Huntington Ave
Suite 2010
Boston, MA 02199

Assertion of BitSight Technologies, Inc. Management

We are responsible for designing, implementing, operating and maintaining effective controls within BitSight Technologies, Inc.'s (BitSight or service organization) Security Ratings Platform System throughout the period September 1, 2019 to August 31, 2020, 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 in Section III and identifies the aspects of the system covered by our assertion.

BitSight uses Amazon Web Services, a subservice organization to provide data center services. 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. Section III presents the types of complementary subservice organization controls assumed in the design of BitSight's controls.

Complementary user entity 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. Section III presents the complementary user entity controls assumed in the design of BitSight's controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period September 1, 2019 to August 31, 2020, 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, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA, Trust Services Criteria). BitSight'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 Section III.

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, 2019 to August 31, 2020, to provide reasonable assurance that BitSight's service commitments and system requirements were achieved based on the applicable trust services criteria.

BitSight Technologies, Inc.

January 15, 2021

III. BitSight Technologies, Inc.'s Description of Its Security Ratings Platform System

BitSight Technologies, Inc.'s Description of Its Security Ratings Platform System

Scope and Boundaries of the System

This is a System and Organization Controls (SOC) 3 report regarding BitSight Technologies, Inc.'s (BitSight, service organization or Company) Security Ratings Platform System, and the controls in place 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, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria), throughout the period September 1, 2019 to August 31, 2020, which may be relevant to users of the Security Ratings Platform System. It does not encompass all aspects of the services provided or procedures followed for other activities performed by BitSight.

Company Background

BitSight is a cybersecurity risk management company based out of Boston, MA 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, GGC Capital, Liberty Global, Menlo Ventures, Globespan Capital Partners, Flybridge Capital Partners, Commonwealth Capital Ventures, SingTel Innov8, the National Science Foundation and Warburg Pincus.

Services Provided

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 CSV format, as well as via an application program interface (API).

A BitSight Security Rating is a number from 250 to 900 which 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.

Principal Service Commitments and System Requirements

BitSight designs its processes and procedures to achieve its service commitments and system requirements based on the criteria relevant to security for its Security Ratings Platform System and

the service commitments that BitSight makes to user entities, the laws and regulations that govern the Security Ratings Platform System, and the financial, operational, and compliance requirements that BitSight has established for the services.

System Incidents

System incidents for BitSight may include, but are not limited to, the following:

- Unauthorized disclosure of sensitive information
- Theft or loss of equipment that contains potentially sensitive information
- Extensive virus or malware outbreak or traffic
- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Compromised user accounts
- Extensive disruption of the system services

BitSight did not identify any system incidents during the period based on these criteria.

Components of the System Used to Provide the Services

Infrastructure

BitSight's platform is hosted in AWS. BitSight's Security Ratings Platform is hosted in a Virtual Private Cloud (VPC) located in the Amazon East Coast service location. The different Amazon infrastructure services that BitSight uses include the following:

- Amazon Elastic Compute Cloud to host all virtual instances
- Amazon Relational Database Service and Elastic MapReduce
- Amazon Elastic Block Store + S3 for storage
- Amazon Elastic Beanstalk to launch containers and scale apps
- Amazon Elastic Load Balancing for high availability
- Amazon VPCs to logically isolate sections of AWS

Software

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)

Except for the application authentication layer, which is a shared responsibility of the customer and not included in the scope of this report, 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) incorporate 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

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 responsibilities 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 Product Officer (CPO), Chief Technology Officer (CTO), Chief Marketing Officer (CMO), General Counsel, Senior Vice President (SVP) of Partnerships, Vice President (VP) of Strategic Partnerships, VP of Finance, VP of Marketing, and the Chief Architect.
- *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.
- *IT + Security* - 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.

The responsibility for provisioning employee access is shared across Human Resources (HR), IT, and the Hiring Manager. Roles and responsibilities are defined in written job descriptions and are reviewed and updated as necessary prior to posting of the job opening. Job requirements are documented in the job descriptions and candidate's abilities to meet these requirements are evaluated as part of the hiring evaluation process. The employee's information, including name, department, start date, personal email, manager, position, background check status and signed employee (Code of Conduct), agreement is added to the HR New Hires file. The hiring manager works with HR to fully execute new employee requirements. Upon the onboarding training, new employees read and accept the Code of Conduct. In addition, management provides mandatory training for employees. Several days prior to the user's start date, an invitation will be sent to the employee's personal email address inviting them to the BitSight SSO service. To access BitSight

resources via the SSO service, employees create a complex password and configure multi-factor authentication. Prior to hiring, a candidate goes through a background check and within the first week of hire, the employee participates in an onboarding training where the newly hired employee gains sufficient training before they assume the responsibilities of their new position. Upon the hiring of a new employee, HR updates BitSight's Organizational Chart.

New-hire access to product related infrastructure resources and tools, including but not limited to, Network Configurations, Storage, and EC2 Instances, are assigned based on Identity and Access Management (IAM) roles developed by IT based on the new hire's job description. Additionally, employees can request additional tools/services needed to perform their job functions. These requests are subject to approval by management.

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.

Processes and Procedures

BitSight has documented policies and procedures that support the management, operations, monitoring, and controls over in scope systems. Specific examples of relevant policies and procedures include, but are not limited to, the following:

- Acceptable Use Policy
- Incident Management Policy
- Information Security Policy
- Change Management Policy
- Access Control Policy
- Software Security Policy
- Vulnerability Management Policy

Management has implemented various methods of internal communication through informal meetings and email communication to help ensure employees are aware of significant events and initiatives and, in addition, understand their individual roles and responsibilities within the organization. These methods include frequent updates from the management team, which discuss

significant projects and initiatives and the overall strategic direction, and changes to published policies and procedures. In addition, relevant security and operational policies, and procedures that include responsibility for reporting operational failures and incidents, are available on BitSight's intranet.

COVID 19 Disclosure

The World Health Organization (WHO) announced the coronavirus (COVID-19) as a global health emergency on January 30, 2020, which prompted national governments to begin putting actions in place to slow the spread of COVID-19. On March 11, 2020, the WHO declared COVID-19 a global pandemic and recommended containment and mitigation measures worldwide.

Complementary Subservice Organization Controls (CSOCs)

BitSight's controls related to the Security Ratings Platform System cover only a portion of the overall control environment required to provide reasonable assurance that the service commitments and system requirements were achieved. It is not feasible that the service commitments and system requirements can be achieved solely by BitSight's controls. The CSOCs in the table below are expected to be implemented and operating effectively:

Number	CSOCs	Applicable Criteria
Applicable to AWS		
1.	Physical access to the data centers, backup media storage and sensitive system components is restricted to authorized personnel.	CC6.4
2.	Intrusion detection systems monitor the network for potential threats and vulnerabilities, and unauthorized access.	CC6.6
3.	Defined protocols followed by operations and security personnel when resolving and escalating reported events.	CC7.2
4.	The registration and authorization of new users is controlled.	CC6.1, CC6.2, CC6.3
5.	Access of users that no longer require access to the systems is revoked.	CC6.1, CC6.2, CC6.3
6.	A formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances is performed.	CC3.1, CC7.4, CC9.1
7.	Logical access security measures protect against security and availability threats.	CC6.6
8.	Procedures are followed to identify (define), report and respond to security and availability breaches.	CC7.2
9.	Security breaches are identified, reported to appropriate personnel and acted on in accordance with established incident response procedures.	CC7.2

Number	CSOCs	Applicable Criteria
10.	System changes that affect internal and external system user responsibilities or the entity's commitments and requirements relevant to security and availability are communicated to those users in a timely manner.	CC8.1
11.	Changes are tested, reviewed and approved prior to implementation.	CC8.1

Complementary User Entity Controls (CUECs)

BitSight's controls related to the Security Ratings Platform System cover only a portion of the overall control environment required to provide reasonable assurance that the service commitments and system requirements were achieved. It is not feasible that the service commitments and system requirements can be achieved solely by BitSight's controls. The CUECs in the table below are expected to be implemented and operating effectively:

Number	CUECs	Applicable Criteria
1.	Customers are responsible for providing BitSight with the initial list of administrator users, as well as notify BitSight with modifications resulting from employee movement and turnover.	CC6.1, CC6.2, CC6.3
2.	Customers are responsible for granting customer personnel appropriate user-level access within the Security Ratings Platform System based on direct job responsibilities.	CC6.1, CC6.2, CC6.3
3.	Customers are responsible for ensuring that access for their personnel is appropriate based upon job responsibilities, and for periodically reviewing user access rights within their Security Ratings Platform System application-level accounts.	CC6.1
4.	Customers are responsible for immediately notifying BitSight of any actual or suspected information security breaches, including compromised user accounts.	CC7.2
5.	Customers are responsible for promptly communicating identified bugs or system functionality issues to BitSight.	CC7.2