Dun & Bradstreet Inc.

System and Organization Controls (SOC) 3 Report

Report on the Data Cloud Products and Solutions System Relevant to Security, Availability, and Confidentiality

For the period August 1, 2020 to July 31, 2021

Ernst & Young LLP
One Commerce Square
Suite 700
2005 Market Street
Philadelphia, PA 19103

Tel: +1 215 448 5000
Fax: +1 215 448 5500
ey.com

Report of Independent Accountants

To the Management of Dun & Bradstreet Inc.

Scope
We have examined management's assertion, contained within the accompanying Management's Report of its Assertions on the Effectiveness of Its Controls over the Data Cloud Products and Solutions System based on the Trust Services Criteria for Security, Availability, and Confidentiality (Assertion), that Dun & Bradstreet Inc.'s (D&B) controls over the Data Cloud Products and Solutions System (System) were effective throughout the period August 1, 2020 to July 31, 2021, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Dun & Bradstreet Inc. (D&B) uses Ensono, and INAP (subservice organizations) to provide data center hosting, environmental safeguards, and physical access to hosted systems and resources. D&B uses Amazon Web Services ("AWS") to provide data center hosting, environmental safeguards, physical access to hosted systems and resources, system monitoring and system availability. The Description of the boundaries of the System (Attachment A) indicates that D&B's controls can provide reasonable assurance that certain service commitments and system requirements, based on the applicable trust services criteria, can be achieved only if AWS, Ensono and INAP's controls, assumed in the design of D&B's controls, are suitably designed and operating effectively along with related controls at the service organization. The Description presents D&B's system and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS, Ensono and INAP. Our examination did not extend to the services provided by AWS, Ensono and INAP and we have not evaluated whether the controls management assumes have been implemented at AWS, Ensono and INAP have been implemented or whether such controls were suitably designed and operating effectively throughout the period August 1, 2020 to July 31, 2021.

Management's Responsibilities
D&B's management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Data Cloud Products and Solutions System (System) and describing the boundaries of the System

- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of the system

- identifying, designing, implementing, operating, and monitoring effective controls over the Data Cloud Products and Solutions System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement

Our Responsibilities
Our responsibility is to express an opinion on the Assertion, based on our examination. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of D&B's relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating D&B's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations
Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve D&B's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion
In our opinion, D&B's controls over the system were effective throughout the period August 1, 2020 to July 31, 2021, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria, if the subservice organization applied the controls assumed in the design of D&B's controls throughout the period August 1, 2020 to July 31, 2021.

Restricted use
This report is intended solely for the information and use of D&B and user entities of D&B's Cloud Data Products and Solutions system during some or all of the period August 1, 2020 to July 31, 2021 and prospective user entities, independent auditors and practitioners providing services to such user entities 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, subservice organizations, or other parties, including complementary user entity controls and subservice organization controls assumed in the design of the service organization's controls

- Internal control and its limitations

- User entity responsibilities and how they interact with related controls at the service organization

- 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.

Ernst & Young LLP

November 12, 2021

**Management's Assertion Regarding the Effectiveness of Its Controls
Over the Data Cloud Products and Solutions System
Based on the Trust Services Principles and Criteria for Security, Availability, and Confidentiality**

November 12, 2021

We, as management of, Dun & Bradstreet Inc. (D&B) are responsible for:

- Identifying the Data Cloud Products and Solutions System (System) and describing the boundaries of the System, which are presented in Attachment A

- Identifying our principal service commitments and system requirements

- Identifying the risks that would threaten the achievement of our principal service commitments and service requirements that are the objectives of our system, which are presented in Attachment B

- Identifying, designing, implementing, operating, and monitoring effective controls over the Data Cloud Products and Solutions System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement

- Selecting the trust services categories that are the basis of our assertion

Dun & Bradstreet Inc. (D&B) uses Ensono and INAP to provide data center hosting, environmental safeguards, and physical access to hosted systems and resources. D&B uses Amazon Web Services ("AWS") to provide data center hosting, environmental safeguards, physical access to hosted systems and resources, system monitoring and system availability. The Description includes only the controls of D&B and excludes controls of AWS, Ensono and INAP, however it does present the types of controls D&B assumes have been implemented, suitably designed, and operating effectively at AWS, Ensono and INAP. The Description also indicates that certain trust services criteria specified therein can be met only if AWS, Ensono and INAP's controls assumed in the design of D&B's controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of AWS, Ensono and INAP.

However, we perform annual due diligence procedures for third-party sub-service providers and based on the procedures performed, nothing has been identified that prevents D&B from achieving its specified service commitments.

We assert that the controls over the system were effective throughout the period August 1, 2020 to July 31, 2021, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability and confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Very truly yours,

Dun & Bradstreet Inc.

Description of Dun & Bradstreet's Data Cloud Products and Solutions relevant to Security, Availability, and Confidentiality

Overview of D&B's Data Cloud Products and Solutions

Corporate Overview

D&B transforms commercial data into valuable insight which is the foundation of our global solutions that customers rely on to make critical business decisions.

D&B provides solution sets that meet a diverse set of customers' needs globally. Customers use Risk Management Solutions™ to mitigate credit, compliance and supplier risk, increase cash flow and drive increased profitability. Our Sales & Marketing Solutions™ help customers better use data to grow sales, digitally engage with customers and prospects, improve marketing effectiveness and allow for data management capabilities that provide effective and cost-efficient marketing solutions to increase revenue from new and existing customers.

D&B's Data Cloud Products and Solutions Information

D&B's Data Cloud Products and Solutions	Data Centers	Environment	Data Center Provider	Infrastructure Components
D&B Hoovers D&B DataVision	Somerville, Massachusetts	Production	INAP	MS SQL, Oracle, Sybase, Mainframe, DB2 Linux, Windows, MongoDB, DynamoDB
	Conway, Arkansas	Staging and Disaster Recovery	Ensono	
Data Integration Batch D&B Match Customer File Processing Safe Transport D&B Finance Analytics (formerly DNBi) Market Insight Small Business Risk Insight	Conway, Arkansas	Production	Ensono	
	Little Rock, Arkansas	Disaster Recovery	Ensono	
D&B Compliance Check	Leeds, United Kingdom	Production	Ensono	
	Conway, Arkansas	Disaster Recovery	Ensono	
D&B Credit D&B Direct+ Registration Portal D&B Connect D&B Analytics Studio	Amazon Web Services (AWS) Cloud Platforms located: US West (Oregon) US East (Virginia) EU West (Dublin)		AWS	Supported by subservice provider

D&B Data Products Descriptions

D&B's Data Cloud Products and Solutions	Product Description
D&B Hoovers	D&B Hoovers delivers a sales acceleration platform packed with insight, so customers can target more strategically, have better informed conversations, and enhance the productivity of their sales and marketing teams. The product helps accelerate sales with more leads, improved win-rates, and shortened sales cycles.
D&B DataVision	D&B DataVision leverages business records from several sources across various geographies to help marketer's profile, visualize, and segment data to identify the right targets for growth.
Data Integration Batch	Data Integration Batch consists of cleanse/match/append processing for customers and delivery of prospect universe files. Customers need DUNS Numbers on their records to take advantage of D&B risk, marketing, or supply data, all enabled through batch flat-file processing, matching, and data append.
D&B Finance Analytics (formerly DNBi)	D&B Finance Analytics is a Software as a Service (SaaS) risk management product suite serving commercial customers. It provides real-time access to D&B data and predictive analysis on global commercial entities to help evaluate financial risk on new customers, and to identify and manage risk and opportunity across a customer's entire portfolio. D&B Finance Analytics has multiple editions based on geography (US, Canada, EU, Australia) and customer segments (Premium, Enterprise), with varying access to modules (Account Manager, Portfolio Risk Manager, etc.) that serve advanced use cases.
Market Insight	Market Insight is a hosted application that helps enable marketing professionals to apply advanced analytical tools to customer, D&B, and third-party industry data to identify attractive markets, prospects, and up-sell/cross-sell opportunities.
Small Business Risk Insight	Small Business Risk Insight (SBRI) originated at the request of financial services customers (banks, credit card issuers, etc.) who needed better insight to inform their small business lending decision processes. SBRI is a data repository of commercial credit card, line, loan, and lease financial payment information that enables the creation and delivery of highly predictive scores and attributes. Today, SBRI scores and attributes are delivered through our online and batch platforms to participating customers, enabling better small business risk decisions.
D&B Compliance Check	D&B Compliance Check is a powerful compliance "Know Your Vendor" solution which provides advanced screening, monitoring of third parties and facilitates compliance with global anti-bribery and corruption regulations. It allows global organizations to identify banned, suspect or higher-risk entities, strengthen fraud protection, help ensure regulatory compliance, manage supply and distribution risk, and protect brand equity. It is supplemented by adverse media information from Regulatory Data Corporation's database of global watch lists, regulatory authority actions, law enforcement sources, global news sources and proprietary research, recognized as one of the most robust sources of data available.

D&B's Data Cloud Products and Solutions	Product Description
Registration Portal	D&B's Registration Portal capability provides our clients with the ability to automate the third-party data collection process as part of their Third-Party Due Diligence program. Registration Portal is an add-on product within D&B Compliance Check.
D&B Credit	D&B Credit is a cloud-based risk solution that is globally deployable and meets customer trade-credit requirements through modern interfaces and user experience. Search & find capability includes more intelligence to quickly deliver the right business. The credit reports tell a risk story that enable better credit decisions. Enhanced alert capabilities inform users of any recent risks or opportunities with intuitive navigation and additional supporting data.
D&B Direct+	D&B Direct+ is a cloud-based API designed to help customers solve various use cases, including Master Data-as-a-Service, Fast Type-Ahead for Custom Lead Forms, Custom Marketing Automation, High Volume Advanced Monitoring, Fast Match & Append, and Custom CRM Integration, among others.
Lattice	D&B Lattice is a B2B customer data platform providing AI-enabled ABM solutions at scale. It is built to drive 1-to-1 experiences across the entire buyer's journey and, can help customers personalize digital experiences to increase the efficiency of their sales and marketing teams by prioritizing contacts for lead and account-based (ABM) programs, identifying net new contacts and implementing cohesive omni-channel campaign. .
D&B Connect	D&B Connect is a self-service data management platform. It connects, manages and visualizes data across an organization. This means a portal to help organizations manage sales and marketing data and achieve a complete view of a customer.
D&B Analytics Studio	D&B Analytics Studio is a cloud-based analytics platform that provides clients with a single, integrated solution to seamlessly explore, synthesize and operationalize data and analytics in order to remain competitive in the era of digital transformation.

D&B Data Services Descriptions

D&B's Data Cloud Products and Solutions	Product Description
D&B Match	D&B Match provides services for enriching client's database with D&B data. Matching is the D&B proprietary process (DUNSRIGHT™) by which an input record (from the customer) is compared to D&B's company database. D&B will collect, aggregate, edit, and verify data from thousands of sources daily so that customers can use the information to make profitable decisions for their businesses.
Customer File Processing	Customer File Processing (CFP) is the batch processing system that receives files directly from customers to fulfil records related to the business (i.e., company name, full address, phone number, website domain, c-level/owner contact). The fulfillment process includes cleanse, match, and append process. CFP application also supports appending of data elements for DUNS numbered files. CFP utilizes the SAS data warehouse to append elements for the DUNS provided. CFP applications support appends from mainframe source files through the customized plug and play jobs written specific to each customer requirements.
Safe Transport	Safe Transport (STP) is used for all internal and external file transfers within D&B.

D&B Architecture Overview

Amazon Web Services (AWS)

AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. AWS provides hosting and resizable computing capacity in the cloud for:

- D&B Credit
- D&B Direct+
- Registration Portal
- Lattice
- D&B Connect
- D&B Analytics Studio

In turn, D&B assumes responsibility for management of the following:

- Patching and updating Operating systems (Linux, Windows, MySQL)
- Configuration of the AWS-provided security group firewall
- Maintenance and implementation of Information Security policies within the organization and supporting IT environment
- Administering and controlling access to accounts and credentials
- Enabling applicable encryption connections for interactions with AWS

- Responsible for VPC specific network security requirements and managing rules and access controls lists to secure our S3 buckets

- Ensuring our AWS resources have the appropriate levels of redundancy and isolation

The control process areas applicable to D&B's customers that are not covered in the scope of this report and are the responsibility of AWS include:

- Data center hosting and cloud services

- Environmental safeguards

- Physical access to hosted systems and resources

- Monitoring system availability

Ensono Data Center Hosting Services

Ensono provides co-location physical hosting services for the following D&B Data Cloud Products and Solutions:

- Data Integration Batch

- D&B Match

- Customer File Processing

- Safe Transport

- DNBi Risk Management (Formerly DNB Interactive – DNB Premium)

- Market Insight

- Small Business Risk Insight

- D&B Compliance Check

D&B relies on Ensono to perform data center hosting, environmental safeguards, and physical access to hosted systems and resources. Data center processes and controls are managed and delivered to D&B by Ensono and are not included in the scope of this report.

In turn, D&B assumes responsibility for management of the following:

- Specifying users' access rights into their applications and databases, including the mainframe; client/server applications; and Oracle, SQL, and similar databases.

- Communicate to Ensono a current list of user entity employees who have security administrative and/or security approval authority. Changes are also communicated to Ensono as needed.

- Communicating to Ensono the security access levels that should be assigned to Ensono support personnel who help resolve security or operational issues

- Ensure controls are in place for managing a current list of users who are allowed access to a user entity emergency or 'Firecall' IDs if any exist.

- Patching and updating Operating systems (Linux, Windows, MySQL)

- Configuration and implementation of firewalls and rules

- Maintenance and implementation of Information Security policies within the organization and supporting IT environment

- Enabling applicable encryption connections

- Responsible for network security requirements and managing rules and access controls lists

- Ensuring our resources have the appropriate levels of redundancy and isolation

The control process areas applicable to D&B's customers that are not covered in the scope of this report and are the responsibility of Ensono include:

- Data center hosting

- Environmental safeguards

- Physical access to hosted systems and resources

- Monitoring system availability

INAP Data Center Hosting Services

Dun & Bradstreet utilizes INAP in Somerville, MA for co-location physical hosting services for the following:

- D&B Hoovers

- D&B Datavision

D&B relies on INAP to perform data center hosting, environmental safeguards, and physical access to hosted systems and resources. Data center processes and controls are managed and delivered to D&B by INAP and are not included in the scope of this report.

In turn, D&B assumes responsibility for management of the following:

- Applying logical access security controls, including user authentication, password complexity requirements, password history requirements, password change procedures, account lockout procedures, and related procedures

- Protecting and maintaining the network security of system resources (for example, secure VPN, configuration and use of firewalls and intrusion detection, and disabling of unneeded network services

- Maintaining system components and configurations, including the application of change controls and procedures as necessary

- Data encryption controls and the secure transfer of data through networks, including public, semi-private, and virtual private networks

- Performing data backup procedures and data classification procedures as necessary

- Protecting systems against infection by computer viruses, malicious codes, and unauthorized software

The control process areas applicable to D&B's customers that are not covered in the scope of this report and are the responsibility of INAP include:

- Data center hosting

- Environmental safeguards

- Physical access to hosted systems and resources

- Monitoring system availability

Service Provided and Expected Controls

D&B uses Amazon Web Services ("AWS"), Ensono, and INAP to provide data center hosting, environmental safeguards, and physical access to hosted systems and resources.

The list below identifies the specific controls that D&B expects subservice organizations to have implemented, suitably designed, and effectively operating. Implementation, suitable design, and effective operation of relevant controls at the subservice organizations is necessary for D&B to meet applicable Trust Services Criteria, either alone, or in combination with the controls at the service organization.

- Ensuring appropriate safeguards for data at rest, including defined encryption standards, methods and/or policies.

- Identifying sensitive data and licensed software on assets and information system media and ensuring appropriate removal or data is overwritten securely when assets are decommissioned.

- Monitoring current usage against predefined thresholds, including appropriate monitoring and resolution of alerts or issues when thresholds are exceeded. Corrective actions, including but not limited to new asset deployment are implemented as necessary.

- Monitoring of environmental threats or physical security threats and notification if threats are identified. Identified threats are investigated until resolution.

- Developing, implementing, and maintaining policies and procedures to promote adequate safeguarding and access to backup and recovery systems, storage media, and data records.

- Ensuring appropriate environmental safeguards and adequate physical security, including appropriate removal of internal users from secure locations to protect backup and recovery systems, storage media, and data records.

- Restricting access to backup and recovery systems, storage media, and data records to authorized personnel.

- Upon notification from authorized D&B contact, granting and revoking of D&B access is performed to validate access is appropriately restricted to backup and recovery systems, storage media, and data records.

Details regarding management's monitoring control over the sub-service providers

As an additional layer of defense, D&B employs an Internal Audit function with due professional care to periodically evaluate risks and assess conformance to D&B security, availability and confidentiality processes. Further, assurance is provided by the D&B Global Security and Risk team (such as the Incident Management, Vulnerability Assessments, Penetration Testing, and Governance Risk and Compliance teams) or by independent third-party assessors. These assessors provide an independent assessment of risk management content/processes by performing periodic security, availability, and confidentiality assessments and compliance audits or examinations (e.g. GDPR, DFARs, ISO, PCI audits) to evaluate the security, integrity, availability and confidentiality of information and resources.

D&B Management leverages the Internal Audit, Global Security and Risk and third-party assessments to determine the health of the D&B control environment including third parties such as subservice organizations.

Principal Service Commitments and System Requirements

D&B designs its processes and procedures to meet its objectives for the Data Cloud Products and Solutions System. Those objects are based on the service commitments that D&B makes to user entities, the laws and regulations that govern the provision of the Data Cloud Products and Solutions System and compliance requirements that D&B has established for the services.

The following processes and system requirements function to meet D&B's commitments to customers with respect to the terms governing the usage of the Data Cloud Products and Solutions System:

- Access Management – The Access Management Policy provides global information security requirements to protect against unauthorized access to data owned by or in the custody of D&B, protect against unauthorized access to computer systems, applications, or operating systems; allow only authorized users the appropriate level of access to the information or portion of the system, application, or operating system necessary to accomplish designated responsibilities, i.e., business need to know; and to help ensure users are accountable for safeguarding their authentication information.

- Change Management – Changes to Information assets and systems undergo formal change management review and approval process prior to any implementation in the production environment. The following are considered as part of change management process:
  - Risk impact;
  - Change approval by authorized personnel;
  - Functionality and security testing;
  - Implementation, Testing and Backout plans;
  - Updates to the configuration management repository

- Data Management & Confidentiality – D&B has placed in operation procedures to achieve objectives in accordance with defined policies including data handling, cryptographic standards, data encryption and key management in alignment with commitments and requirements.

- Risk Management – D&B has established standards and measurements to identify risks, conduct risk assessments, management exposure, monitor effectiveness and complete risk reporting in alignment with commitments and requirements.

- Business Continuity & Availability – D&B uses Disaster Recovery Institute International (DRII), Business Continuity Institute (BCI) guidelines based on the ISO Standard 22301 and industry best practices as the guiding principles and structure for its BCM program. Each business unit has an assigned Business Continuity Coordinator (BCC) who liaise between the business unit and the BCM Team to complete Business Impact Analysis (BIA's), Business Continuity Plans (BCP's) and coordinate testing. Business Continuity plans are tested annually via tabletop exercises. After action reports are completed upon the completion of the testing and results are shared with the BCC team. Additionally, emergency notification testing is performed, and results communicated.