Atomic Data, LLC
Type 2 SOC 3
2020
SOC 3 FOR SERVICE ORGANIZATIONS REPORT

April 16, 2019 to April 15, 2020
Table of Contents

SECTION 1  ASSERTION OF ATOMIC DATA, LLC MANAGEMENT ...........................................1
SECTION 2  INDEPENDENT SERVICE AUDITOR’S REPORT ....................................................3
SECTION 3  ATOMIC DATA, LLC’S DESCRIPTION OF ITS MANAGED SERVICES SYSTEM THROUGHOUT THE PERIOD APRIL 16, 2019 TO APRIL 15, 2020 ......................................7

OVERVIEW OF OPERATIONS .............................................................................................8
  Company Background .......................................................................................................8
  Description of Services Provided .....................................................................................8
  Principal Service Commitments and System Requirements ............................................12
  Components of the System .............................................................................................12
  Boundaries of the System ...............................................................................................19
  Changes to the System Since the Last Review ...............................................................21
  Incident Since the Last Review ........................................................................................21
  Criteria Not Applicable to the System ...........................................................................21
  Subservice Organizations ...............................................................................................21

COMPLEMENTARY USER ENTITY CONTROLS .................................................................27
SECTION 1

ASSERTION OF ATOMIC DATA, LLC MANAGEMENT
ASSERTION OF ATOMIC DATA, LLC MANAGEMENT

April 20, 2020

We are responsible for designing, implementing, operating, and maintaining effective controls within Atomic Data, LLC’s (‘Atomic Data’ or ‘the Company’) Managed Services System throughout the period April 16, 2019 to April 15, 2020, to provide reasonable assurance that Atomic Data’s service commitments and system requirements relevant to Security, Availability, and Confidentiality (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in “Atomic Data, LLC’s Description of Its Managed Services System Throughout the Period April 16, 2019 to April 15, 2020” 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 April 16, 2019 to April 15, 2020, to provide reasonable assurance that Atomic Data’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy (AICPA, Trust Services Criteria). Atomic Data’s objectives for the system in applying 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 “Atomic Data, LLC’s Description of Its Managed Services System Throughout the Period April 16, 2019 to April 15, 2020”.

Atomic Data uses DataBank Holdings, Ltd (‘DataBank’) and Cologix, Inc. (‘Cologix’) to provide data center hosting services (collectively, ‘subservice organizations'). The description indicates that complementary subservice organizations controls that are suitably designed and operating effectively are necessary, along with controls at Atomic Data, to achieve Atomic Data’s service commitments and system requirements based on the applicable trust services criteria. The description presents Atomic Data’s controls, the applicable trust services criteria, and the types of complementary subservice organizations controls assumed in the design of Atomic Data’s controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Atomic Data’s service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Atomic Data’s controls.

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 April 16, 2019 to April 15, 2020 to provide reasonable assurance that Atomic Data’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Jim Wolford
Chief Executive Officer
Atomic Data, LLC
SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT
INDEPENDENT SERVICE AUDITOR’S REPORT

To Atomic Data, LLC:

Scope

We have examined Atomic Data, LLC’s (‘Atomic Data’ or ‘the Company’) accompanying description of Managed Services System titled “Atomic Data, LLC’s Description of Its Managed Services System Throughout the Period April 16, 2019 to April 15, 2020” (description) based on the criteria for a description of a service organization’s system in DC section 200, 2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report (AICPA, Description Criteria), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 16, 2019 to April 15, 2020, to provide reasonable assurance that Atomic Data’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (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).

Atomic Data uses DataBank Holdings, Ltd (‘DataBank’) and Cologix, Inc. (‘Cologix’) to provide data center hosting services (collectively, ‘subservice organizations’). The description indicates that complementary subservice organizations controls that are suitably designed and operating effectively are necessary, along with controls at Atomic Data, to achieve Atomic Data’s service commitments and system requirements based on the applicable trust services criteria. The description presents Atomic Data’s controls, the applicable trust services criteria, and the types of complementary subservice organizations controls assumed in the design of Atomic Data’s controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organizations controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Atomic Data, to achieve Atomic Data’s service commitments and system requirements based on the applicable trust services criteria. The description presents Atomic Data’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Atomic Data’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

Atomic Data 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 Atomic Data’s service commitments and system requirements were achieved. Atomic Data has provided the accompanying assertion titled “Assertion of Atomic Data, LLC Management” (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Atomic Data is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization’s service commitments and system requirements.
Service Auditor’s Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization’s system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization’s service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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 Atomic Data’s Managed Services System were suitably designed and operating effectively throughout the period April 16, 2019 to April 15, 2020, to provide reasonable assurance that Atomic Data’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.
The SOC logo for Service Organizations on Atomic Data’s website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Atomic Data, user entities of Atomic Data’s Managed Services during some or all of the period April 16, 2019 to April 15, 2020, business partners of Atomic Data subject to risks arising from interactions with the Managed Services, and those who have sufficient knowledge and understanding of the 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.

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

Tampa, Florida
April 20, 2020
SECTION 3

ATOMIC DATA, LLC’S DESCRIPTION OF ITS MANAGED SERVICES SYSTEM THROUGHOUT THE PERIOD APRIL 16, 2019 TO APRIL 15, 2020
OVERVIEW OF OPERATIONS

Company Background

Atomic Data is a privately-owned Minnesota company with headquarters located at 250 Marquette Avenue South in Minneapolis, Minnesota. Atomic Data also has an additional office location located at 750 B Street in San Diego, California. Jim Wolford and Larry Patterson founded Atomic Data in 2001. They serve as Atomic Data’s Chief Executive Officer (CEO) and Chief Technology Officer (CTO), respectively.

Atomic Data evolved over the years to become a leading provider of a wide range of managed-infrastructure and enterprise IT services. By following its deep commitment to partnering with its clients, Atomic Data has grown to manage five data center facilities worldwide, with a core group of three data centers in the Minneapolis area.

Atomic Data connects its data centers with redundant 10-gigabit fiber links and numerous Internet connections with major international IP-transit providers. Atomic Data partners with local exchange carriers and infrastructure providers to bring last-mile connectivity back to an Atomic Data-managed national Multiprotocol Label Switching (MPLS) wide-area network. This flexibility allows Atomic Data to host high-availability web sites, applications, enterprise wide area networks (WAN), and Voice over Internet Protocol (VoIP) services for its clients.

Atomic Data monitors and manages its services from its 24x7 Network Operations Center (NOC), from which all aspects of the data center environments, network conditions, and hosting systems health are measured. The Atomic Data Service Desk and NOC combine to provide 24x7 managed help desk and other custom management services.

Atomic Data has a dedicated Security and Compliance department which sets a high standard for security controls and provides guidance for management in evaluating and remediating security risks. Oversight boards provide formal governance and approval to proposed changes, including services, policies, organizational changes, ongoing risk management, and changes to the Atomic Data Network Control Environment.

Description of Services Provided

Atomic Data offers a complete suite of managed technology services that provide clients with the building blocks for enterprise class infrastructures. These services include:

- The Atomic Cloud®
- Data Center Colocation
- Enterprise Architecture and Implementation
- Compliance as a Service
- 24x7 Network Monitoring & Management
- 24x7 Technical Support
- Orange Book - Annual IT Asset Review and Budget Planning
- Server and Workstation Management
- Remote Data Backup and Disaster Recovery
- Connectivity and ISP Services
- Hosted Solutions
- Web and Software Development
- Software and Platform Optimization Services
- Voice Solutions
The Atomic Cloud®

Atomic Data can help clients build the perfect cloud solution that leverages existing IT resources and aligns seamlessly with a client’s specific needs. Atomic Data’s virtual server environments allow companies to consolidate multiple applications and operating systems to run on a single physical server. A basic virtual server environment consists of a Storage Area Network (SAN) based virtual hard disk, a virtual server capable of running Windows or Linux operating systems, and a managed firewall. Virtual Server environments enable companies to utilize all available server capacity while providing critical applications with additional resources during peak times. Clients may purchase Atomic Data monitoring and Atomic Data patch-management services for their virtual servers. Atomic Data patches, monitors, and manages Windows and Linux virtual servers with a variety of enterprise management software suites.

Data Center Colocation

Atomic Data’s secure, global facilities are built for maximum uptime, connectivity and redundancy. Experience the benefits of enterprise-grade data center colocation combined with top-tier engineers, industry-leading partnerships, and all-encompassing service packages.

Available from one unit (1U) to multi-rack and private cage configurations, colocation allows server message blocks (SMBs) to cost-effectively house their voice, computing, and networking equipment within a highly connected, secure facility equipped with numerous layers of redundancy, monitoring, and environmental controls. Colocation is also ideal for creating a centralized computing location for companies with distributed physical locations.

Atomic Data directly controls and manages the MSP250 data center suite and all services provided at the facility. Atomic Data directly controls and manages the colocation services provided at the MSP7700 and DFW400 data centers, while utilizing DataBank Holdings, Ltd as a subservice organization for facility infrastructure and environmental protection. Atomic Data also utilizes Cologix as a network service provider and physical and environmental infrastructure provider at the MSP511 data center facility.

Enterprise Architecture and Implementation

Atomic Data’s vast, proven enterprise experience and deep bench of industry-certified engineers and architects work closely with Atomic Data’s Architecture and Implementation services. Enterprise Architecture and Professional Services departments provide network and application architecture, design, and implementation for clients. Enterprise implementations include WAN Design, Local Area Network (LAN) Design, cloud architecture and migration planning, storage evaluation and recommendations, disaster recovery playbooks, and more. Enterprise Implementation services are tailored to meet the specific client technology needs.

Security & Compliance Consulting

The safety and security of client data is Atomic Data’s highest priority. Whether it’s Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), Service Organization Control (SOC) 2 or 3, Atomic Data’s industry-certified security and compliance experts can help clients safeguard their data by assisting them in implementing managerial oversight, comprehensive policies and procedures, physical and logical access controls, computing/software/network controls, and data destruction techniques to prepare for a multitude of industry-specific security and compliance audits.
24x7 Network Monitoring & Management

Atomic Data's NOC is just a phone call, e-mail, or web portal ticket away. Using tools such as Zenoss, Nagios, Splunk, Kaseya, and Opsview, Atomic Data's highly trained and experienced NOC technicians monitor client networks 24x7 to identify and resolve network issues to prevent downtime. In addition to monitoring data centers, routers, switches, servers, applications, storage networks, and websites, Atomic Data's NOC can also manage incident response, serving as the first line of defense when network issues arise.

24x7 Technical Support

Operating from redundant Minneapolis locations, Atomic Data offers 24x7 e-mail, phone, and web portal-based support for a client's employees, executives, and even their clients. Atomic Data's Service Desk and On-Site Services are ideal for augmenting or replacing IT resources for businesses looking to eliminate the burden and cost of maintaining an internal IT staff, keeping up with growth, industry trends, or workload. From software, hardware, peripherals, to virtual private network (VPN) access, and more, the Service Desk can remotely assist with a wide array of issues and is often the primary point of contact for many of Atomic Data's clients. For more complex issues or those that cannot be resolved remotely, the Service Desk will escalate the issue to the On-Site Services department for resolution.

Operating desk-side as well as remotely, the On-Site Services department is comprised of field-based engineers who provide client support including, but not limited to, business application server support, e-mail management and support, desktop management and support, network directory services, LAN/WAN security management. In addition to regularly scheduled maintenance and support, On-Site Services also provides LAN/WAN technical support.

Orange Book - IT Asset Review and Budget Planning

The Orange Book is a comprehensive document that provides insight into all aspects of the current state of a client’s IT environment and how specific areas are performing. Atomic Data uses the Orange Book to inventory and assess switches, routers, workstations, printers, servers, backup systems, software assets, user accounts, and more. The Orange Book gives clients a useful first step in defining a custom maintenance schedule, future state upgrades, and IT-related financial planning that fits their network’s specific components and complements their business plan.

Server & Workstation Management

Atomic Data will take on the burden of patching, securing, monitoring, and auditing servers and workstations to save clients time and money, using advanced management tools like Kaseya. Clients can rest assured that once the lightweight software is installed, mission critical servers and desktops are under the competent and watchful eye of Atomic Data's 24x7 NOC and Service Desk. Server and workstation monitoring also includes patch management, endpoint antivirus, auditing, remote access, automated procedures, system imaging, and agent/system logging.

Remote Data Backup and Disaster Recovery Products

Atomic Data provides several backup products and the expertise to help ensure the safety of client’s critical data. Multi-level backup options for workstations, laptops, servers at file or block levels allow clients to configure a secure, cost-effective backup scheme tailored to their specific business needs. Atomic Data also offers disaster recovery options tailored to balance client budget and risk management requirements. From off-site data backup to a fully equipped secondary site, Atomic Data’s data security consultants help clients choose the option that best meets their needs.
Connectivity and Internet Service Provider (ISP) Services

At the foundation of Atomic Data's managed ISP services are numerous 10-gigabit border gateway protocol (BGP) peers, which provide high-capacity, redundant, multi-homed Internet availability for all clients and services within the Atomic Data network. Atomic Data's data centers are interconnected with 10-gigabit fiber links, providing redundant, transparent networking between all facilities. For Managed ISP connectivity services, Atomic Data offers a full range of bandwidth circuits, including 10 Mbps and up metro-ethernet circuits, traditional circuits such as digital signature 3 (DS3) circuits and T1 circuits, and digital subscriber line (DSL), all of which may be used to build private MPLS-based WANs.

Hosted Solutions

From Microsoft Exchange and SharePoint to domain name system (DNS) and web hosting, Atomic Data provides businesses with the enterprise-grade hosting services that include security, reliability, and support. With extensive virtualization and hosting expertise, Atomic Data offers highly available and secure hosted solutions that not only eliminate the need for large capital expenditures, but also removes the burden of server maintenance and administration.

Web and Software Development

Atomic Data's highly skilled Software Solutions department does everything from SharePoint customizations to proprietary .NET applications and SQL database clustering. By partnering with business stakeholders and IT resources, Atomic Data's Software Solutions department leverages software to enable clients to be more competitive and operate more efficiently.

Atomic Data's senior software architects and business analysts engage with clients at the front end of the software development lifecycle (SDLC) to design custom software solutions catered to an organization's business needs. Upon completion of application architecture and design, Atomic Data drives development through an iterative development process that follows the Agile software development methodology, aligning with client timeline and budget goals. Atomic Data provides flexible application development options, including complete software development services, hybrid development teams that include internal client employees, and simplified leadership and mentoring of client development teams by senior Atomic Data software architects.

In addition to development of new software applications, Atomic Data's Software Solutions department provides ongoing maintenance, support, and iterative development for existing applications, including applications written by third parties. Atomic Data's Software Solutions department will engage with a client at any point of the SDLC and custom-tailor software services for a client.

Software and Platform Optimization Services

Atomic Data provides infrastructure as a service for large software platforms and clients serving high-volume, public facing websites. Atomic Data's shared web application infrastructure supports millions of transactions per day. Atomic Data's software and platform optimization engineers assist clients in managing the deployment and ongoing monitoring and maintenance of client applications in this shared infrastructure. These services include infrastructure capacity management and performance monitoring; large volume transactional database architecture, design, and optimization; database and query optimization; application code review and optimization; high availability architecture and scaling design; managed code repositories and deployment; managed private cloud; and maintenance development services. Atomic Data's Software & Professional Services departments ensure that client applications are always running at their peak efficiency within Atomic Data's shared infrastructure.
Voice Solutions

Atomic Data's hosted VoIP offerings are built on top of a combination of Session Initiation Protocol (SIP) trunks, Public Relay Interfaces (PRI), and a Mitel VoIP system. A hosted VoIP solution combined with Atomic Data bandwidth over an MPLS network provides clients an enterprise VoIP solution without requiring an equipment investment and ongoing system management and maintenance. With SIP trunks and PRIs residing within an enterprise data center facility, a client’s voice communications become resilient to local network outages at corporate or branch locations.

Atomic Data’s hosted VoIP products are provided on a per-user basis and are easily adaptable for organizations anticipating growth or experiencing periodic fluctuations in the total number of users.

In addition to Atomic Data’s hosted VoIP products, Atomic Data also provides colocation of Mitel and other voice systems owned by clients, as well as on-premise Mitel implementations.

Principal Service Commitments and System Requirements

Atomic Data designs their processes and procedures to meet the objectives set for Managed Services. Those objectives are based on the service commitments that Atomic Data makes to user entities, the laws and regulations that govern the provision of Managed Service services, and the financial, operational, and compliance requirements that Atomic Data has established for the services.

Security commitments to clients are documented and communicated in Master Services Agreements (MSAs) and other client agreements, as well as in the description of the service offering provided to clients. Security commitments are standardized and include, but are not limited to, the following:

- Implementing the principle of least privilege for access to client systems and data
- Utilizing encryption for to protect client data
- Ensuring client data is available within stated service commitments

Atomic Data establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Atomic Data’s system policies and procedures, system design documentation, and contracts with clients. Information security policies define an organization-wide approach to how systems and data are protected, including how services are designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. 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 Managed Services.

Components of the System

The system is comprised of the following:

- Infrastructure
- Software
- People
- Policies and Procedures
- Client Data

Infrastructure

Primary infrastructure used to provide Atomic Data's Managed Services System includes confidential data. Any specific question a client or vendor may have can be answered in person during a review of this report.
Atomic Data operates within the following office and data center facilities:

- MSP250
- MSP7700
- DFW400
- MSP511

**MSP250**

MSP250 is the location of several Atomic Data's facilities, including headquarters offices, the NOC, the Service Desk, and the primary data center. These facilities occupy parts of a multi-tenant building at 250 Marquette Avenue South in Minneapolis, Minnesota. In tandem with building management, this facility provides 24x7 physical security, including security cameras, individually locking cabinets and cages, card-key access, and on-site security guards.

The MSP250 data center provides secure, highly controlled space with redundant network access for colocation equipment. Clients may choose from a wide range of space offerings including partial, full, and multiple racks; dedicated cages; and dedicated suites. Atomic Data also operates its cloud offerings from this space, providing a highly available cloud for clients to locate their services and systems.

**MSP7700**

MSP7700 is the location of one Atomic Data's colocation and cloud data centers. The facility is located at 7700 France Avenue South, in Edina, Minnesota. Atomic Data leases colocation space from Databank, who operates the facility. As a subservice organization, Databank operates the physical security controls around access to the facility, and environmental controls and monitoring of the facility. Specifics of the controls Databank operates are detailed in the "Subservice Organizations" section below. Atomic Data operates additional physical security and environmental controls within the spaces it controls.

The MSP7700 data center provides secure, highly controlled space with redundant network access for colocation equipment. Clients may choose from a wide range of space offerings including partial, full, and multiple racks. Atomic Data operates its cloud offerings from MSP7700, providing clients with another option to locate their services and systems.

**DFW400**

DFW400 is the location of one of Atomic Data's colocation and cloud data centers. The facility is located at 400 South Akard Street, in Dallas, Texas. Atomic Data leases colocation space from Databank, who operates the facility. As a subservice organization, Databank operates the physical security controls around access to the facility, and environmental controls and monitoring of the facility. Specifics of the controls Databank operates are detailed in the "Subservice Organizations" section below. Atomic Data operates additional physical security and environmental controls within the spaces it controls.

The DFW400 data center provides secure, highly controlled space with redundant network access for colocation equipment. Clients may choose from a wide range of space offerings including partial, full, and multiple racks. Atomic Data operates its cloud offerings from DFW400, providing clients with another option to locate their services and systems.

**MSP511**

MSP511 is the location of Atomic Data's network interconnection data center. The facility is located at 511 11th Avenue South, in Minneapolis, Minnesota. Atomic Data leases cabinet space from Cologix, Inc., who operates the facility. As a subservice organization, Cologix operates the physical security controls around access to the facility, and environmental controls and monitoring of the facility. Specifics of the controls Cologix operates are detailed in the "Subservice Organizations" section below.
The MSP511 data center provides Atomic Data with diverse path network interconnections between its other data centers and Internet Service Providers.

**Software**

Primary software used to provide Atomic Data’s Managed Services System includes confidential data. Atomic Data considers the specifics of the software they use to achieve their services proprietary and confidential. Any specific question a client or vendor may have can be answered in person during a review of this report.

**People**

Atomic Data is organized into functional areas supporting general business administration and technical operations under the executive leadership of CEO Jim Wolford. Business Administration includes Security & Compliance, Communications, Sales, Accounting, and Human Resources (HR). Technical operations includes Account Management, Service Desk, NOC, On-Site Services, Infrastructure Engineering, Enterprise Architecture & Professional Services, and Software Solutions.

Policies relating to appropriate business practices, knowledge, and experience of key personnel are taken into consideration when defining the organizational structure. In addition, policies are established, and communications are directed at ensuring personnel understand Atomic Data’s objectives, how individual actions interrelate and contribute to those objectives, and recognize how and for what personnel will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.

**Functional Responsibilities**

Atomic Data assigns personnel to departments organized around technical and professional responsibilities. As a human control, these departments form the basis for the role separation found in the implementation of logical and physical controls elsewhere in the environment. This clear identification of departments and their related roles promotes efficiency, limits broad exposure, and provides for a system of internal checks and balances. Primary roles and responsibilities for each of these departments are described here.

**Security & Compliance**

The Security & Compliance department operates as the information security focal point for the organization and is responsible for the operation, maintenance, and improvement of Atomic Data's internal control environment. Security & Compliance works directly with individual departments, providing clarification and guidance on policies, procedures, change management, and potential impacts to the security, availability, and confidentiality of Atomic Data computing infrastructure.

The Security & Compliance department is also responsible for ongoing management and governance of Atomic Data’s compliance initiatives, in coordination with HR and the CEO. This includes management of the SOC audit program and oversight of the supporting controls. Examples of these responsibilities include: security testing; security incident investigation and analysis; developing and conducting information security awareness training and testing; monitoring adherence to organizational controls; assessing the need for changes to controls based on organization growth and changing security landscape; serving as an authoritative body to the organization on the implementation of controls; and responding to third-party audit requests.
Communications

The Communications department is responsible for Atomic Data’s public image and message through a variety of channels including the atomicdata.com website, social media, e-mail campaigns, radio and television marketing, product and service marketing literature, video productions, events, press releases, and more. The department uses these channels to generate leads and attract new business. The department also is responsible for preparing responses to Requests for Information (RFI), Requests for Proposal (RFP), and for overseeing the usage of licensed images and assets on behalf of Atomic Data.

Sales

The Sales department is responsible for all lead generation and new business development, as well as completing all contract agreements with clients, evaluating the existing client base for additional sales opportunities, and preparing and delivering all eQuotes, proposals, and completed responses to RFIs and RFPs. In addition, the Sales department places and tracks all pending connectivity and power circuit orders, fulfills and tracks all hardware and software orders, and distributes and maintains hardware and software inventories. All new contract agreements, orders, purchases, and responses to RFIs and RFPs must be entered into the system to be fulfilled and require proper senior management authorization.

The Sales department maintains client relations and develops and maintains strategic partnerships and relationships with complementary vendors and strategic resellers to sustain the growth of Atomic Data’s market share, profitability, and success.

Accounting

The Accounting department is responsible for the financial affairs of Atomic Data and preparing financial analyses of operations, including interim and final financial statements with supporting schedules for management guidance. This department manages the day-to-day accounting operations, including payables and receivables, and oversees internal financial controls, ensuring accuracy, timely deliverables, and compliance.

HR

The HR department is responsible for the overall acquisition, development, and retention of employees and contractors. HR works with department managers to identify staff and contractor needs, outline and maintain job descriptions, and facilitate candidate searches through recruiting activities and the interview process. Benefits development, in coordination with the CEO, is another key element supporting recruiting, development, and retention activities. In addition to onboarding new resources, HR is responsible for the ongoing development and management of the employee handbook, policies, procedures, and training programs for all employees and contractors.

Additionally, annual background checks are required and maintained on file for all employees and contractors.

Software Solutions

The Software Solutions department creates custom business applications leveraging industry frameworks and platforms. These applications include, but are not limited to, online collaboration, data aggregation and rollup, cross-system integration, Web service and API development, custom business workflow automation, and more. The Software Solutions department includes senior business analysts and software architects with expertise in identifying unique and efficient solutions to complex business challenges in partnership with clients. Additionally, the Software Solutions department provides full-service development, testing, deployment, and support as part of the SDLC.
In addition to custom application development, the Software Solutions department is responsible for the ongoing development, management, maintenance, and support of cloud-based software products delivered through Atomic Data's infrastructure. Some of these products include multi-tenant hosted Microsoft SharePoint, industry specific SharePoint feature packs, and hosted source control repository via SVN.

**Account Management**

The Account Management department is responsible for ensuring that information technology projects are conducted in a disciplined, well-managed, and consistent manner that assures the delivery of quality products and services. This involves appropriate planning, scheduling, and control within Atomic Data projects and ensuring efficient use of resources and tools. This department is responsible for communicating and managing client project plans, timelines, and events and obtaining client feedback upon the implementation of products and/or services.

**Service Desk**

The Service Desk provides 24x7 troubleshooting of client technical issues received via phone, e-mail, and the online ticket portal. The Service Desk issues a ticket for each issue received. Service Desk employees use their knowledge, manuals, and troubleshooting guides to determine if the issue can be resolved at their level or if the issue needs to be escalated to a Level II or Level III Engineer for resolution.

**NOC**

The NOC is responsible for responding to any potential issues related to Atomic Data products and services. The NOC responds to information received by initiating tickets, performing initial triage, and escalating to the appropriate resource. The NOC is the first point of contact for many clients and helps management monitor company trends. The NOC is responsible for the day-to-day monitoring, maintenance, and administration of all Atomic Data and client circuits, internal networking devices, NOC management systems, and Linux-based servers.

Additionally, a core group of individuals in the NOC department are trained to identify and respond to security incidents, operating as a Security Operations Center (SOC) within the NOC. The SOC meets regularly with Security & Compliance department members and assists with optimizing processes regarding identifying and responding to security events.

**On-Site Services**

The On-Site Services department is responsible for direct support of Microsoft-based workstations, servers, and local, on-site networks. This department handles the maintenance and architecture for all client Windows domains. On-Site Services provides both remote and on-site support for client workstations, networks, and other equipment. The Service Desk provides Level I support to On-Site clients. The On-Site Services department receives escalations from the Service Desk regarding issues arising on-site.

**Infrastructure Engineering**

The Infrastructure Engineering department is comprised of Network, Systems, and Data Center engineering teams. The department manages Atomic Data's IP transit network, IP allocations, ISP services, colocation facilities, and client move-ins at the data centers. The Network Engineering team is responsible for meeting the demands of clients with enterprise LAN and WAN network architecture. The Systems Engineering team is responsible for the architecture and maintenance of Atomic Data's virtual server infrastructure, including VMware clusters, SAN storage, tape backup services, and load balancers. Systems Engineering also manages Atomic Data's Kaseya product, which provides patch management, monitoring, and anti-virus for Atomic Data and client resources, as well as Atomic Data's Black Box product, which provides for backup and disaster recovery of critical client server systems. Both teams receive escalations from the NOC and Service Desk.
Enterprise Architecture & Professional Services

The Enterprise Architecture & Professional Services department is responsible for designing and implementing data center networks that include server virtualization, LAN, WAN, intranets, extranets, network and server security, load balancing, and storage. The architects also perform system design, analysis, and planning; design network and computer security measures; and research and recommend network and data communications hardware and software. They also work with clients to design and architect solutions to meet the client’s business needs.

Data

Client data, as defined by Atomic Data, may constitute the following, depending on the services provided to the client:

- Network and system architecture diagrams
- Network device configuration files
- Application source code
- Client e-mails (e.g. if a client is using a hosted Exchange product)
- Client system images and data
- Policies and procedures
- Incident details
- Vulnerability scan data

Client data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in client contracts.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, data security, and risk management. All departments are expected to adhere to Atomic Data's policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Atomic Data team member.

Physical Security

Physical security controls aim to ensure the integrity of the physical environments involved in generating the service provided by Atomic Data. At Atomic Data offices, these protections include 24-hour video surveillance and recording, proximity-card controlled perimeter doorways, and punch-code secured interior doorways, which limit access to key storage areas to appropriate personnel. At the data centers, Atomic Data implements controls and policies that can function standalone when in sole control and as a complement to the controls of a subservice organization where Atomic Data does not control the entire facility. Some of the common expectations include 24-hour, two-factor access to the facility, cages, and racks for authorized Atomic Data personnel and clients, comprehensive monitoring of internal and external environmental conditions, and extensive video surveillance. Subservice organization physical access controls align with Atomic Data expectations and are detailed in the "Subservice Organizations" section below.

Logical Access

Logical controls provide directives for implementing policies and procedures that ensure the operating environment is properly secured from network or any other electronic access. Activities within the operating environment are properly authorized and documented. The primary framework for authenticating and authorizing administrative access is the Atomic Network Control Environment (ANCE). The ANCE relies principally on a user's Active Directory account, which is required to gain access to any privileged network within the office or in conjunction with two-factor by remote access.
All administrative interfaces are restricted to Atomic Data-controlled access, and the level of authorization is determined on a per-user basis at every administrative interface. The ANCE is monitored in multiple ways to ensure configuration integrity and detect internal and external threats.

**Computer Operations - Backups**

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions. Backup media is rotated off-site on at least a weekly basis.

**Computer Operations - Availability**

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Atomic Data monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Atomic Data evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center space, power, and cooling
- Disk storage
- Tape storage
- Network bandwidth

Atomic Data has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Atomic Data system owners review proposed operating system patches to determine whether the patches are applied. Customers and Atomic Data systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Atomic Data staff validate that all patches have been installed and, if applicable, that reboots have been completed. Subservice organization availability controls align with Atomic Data expectations and are detailed in the "Subservice Organizations" section below.

**Change Control**

Atomic Data’s Change Management Board (CMB) is responsible for ensuring that change management policies and procedures are adhered to for all changes to Atomic Data internal and client infrastructure. The CMB reviews planned changes to systems and network infrastructure to ensure that such changes meet all requirements set forth in Atomic Data’s change management policies and client change management policies, where applicable. The CMB has authority to approve operational level changes to systems and network infrastructure. The CMB reviews previously executed changes to ensure consistency with process and identify any areas for improvement or potential problems. The CMB reviews operational events and outages to determine if they were the result of unplanned changes or could be mitigated through additional planning or change management processes.

**Systems Development Lifecycle**

Atomic Data maintains documented Systems Development Lifecycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.
A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Atomic Data has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Atomic Data system owners review proposed operating system patches to determine whether the patches are applied. Customers and Atomic Data systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Atomic Data staff validate that all patches have been installed and if applicable that reboots have been completed.

**Data Communications**

Atomic Data uses various means of communication to ensure that all employees understand their individual roles and responsibilities for providing services to clients and promoting timely notification of significant events. Continuous communications and hands-on training ensure that employees are aware of important policy changes, as well as organizational changes and events. All employees are encouraged and expected to broadly communicate new, relevant information and exceptions arising from their individual job activities, observations of internal business operations, and the external environment. Managers from all departments are expected to respect the value of such communications and respond appropriately.

The Service Desk and NOC prepare reports at each shift change, which include important information about products and services, alerts, clients, and internal tasks relevant from the past 24 hours. Designated departments review these reports and are expected to communicate perceived possible risks and offer recommendations towards resolution, prevention, or mitigation. Management uses these reports as major inputs to Atomic Data’s internal quality control.

Atomic Data has developed a system that integrates numerous technical monitoring methods designed to provide early detection and immediate response to evolving risks in the operating environment. This system is monitored 24x7 by the Service Desk and NOC, which identify, communicate, ticket, triage, and escalate warnings and critical alerts as appropriate. The system provides a complete overview of performance objectives at all key levels including monitoring the physical data centers through cameras and environmental sensors; the hardware and operating system status of infrastructure servers and services through passive and active monitoring; as well as televised and automatic weather reporting for the local area and for the specific geographic locations of client points of operation throughout the country. All technical personnel contribute to the constant evolution and improvement of the overall system, and all are expected to be available 24 hours a day for escalations.

**Boundaries of the System**

The scope of this report includes the Managed Services performed in the Minneapolis, Minnesota facility.

This report does not include the Data Center Hosting Services provided by Cologix at the Minneapolis, Minnesota facility, or the Data Center Hosting Services provided by DataBank at the Edina, Minnesota and Dallas, Texas facilities.
Atomic Data Network Overview:
Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incident Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common, Availability, and Confidentiality criterion were applicable to the Atomic Data Managed Services System.

Subservice Organizations

This report does not include the Data Center Hosting Services provided by Cologix at the Minneapolis, Minnesota facility or the Data Center Hosting Services provided by DataBank at the Edina, Minnesota and Dallas, Texas facilities.

As noted above in the section on the Components of the System, Atomic Data operates within the following provider managed data center facilities:

- MSP511 - Operated by Cologix
- MSP7700 - Operated by Databank
- DFW400 - Operated by Databank

Subservice Description of Services

MSP511 Data Center Infrastructure - Cologix

Atomic Data utilizes Cologix as a network service provider at the MSP511 data center facility. Cologix is located within the 511 Building, the most highly connected telecommunications facility in Minnesota. The 511 Building is home to dozens of major network carriers, who support a common, secure perimeter for the entire facility and demand the highest reliability for all common utility services.

Cologix is a major provider within the building, providing telecommunications interconnect services for numerous ISPs and large entities. The building provides a secure entrance that is manned 24x7 and monitored by security cameras. Cologix provides security at the suite, room, and rack level, ensuring no unauthorized access is permitted. Cologix also provides infrastructure protection to their clients via environmental monitoring and failover capabilities. Cologix also provides 24-hour availability of its personnel to respond to client inquiries.

Atomic Data uses MSP511 to enhance services already available in the MSP market and add network redundancy. Multiple connections to major Internet backbone providers and regional ISPs further enhance the availability of Atomic Data’s IP transit services and reduce overall network latency. Atomic Data also uses MSP511 to provide enhanced local and long-haul point-to-point connectivity options for customers, allowing additional flexibility and more competitive pricing. Atomic Data does not store data or provide other services from this facility.
Complementary Subservice Organizations Controls

The following subservice organization controls should be implemented by Cologix to provide additional assurance that the trust services criteria described within this report are met:

<table>
<thead>
<tr>
<th>Subservice Organization Controls - Cologix</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>Common Criteria/Security</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Availability</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Category</td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
|                  | Environmental monitoring applications are utilized to monitor the environmental conditions within the data center and customer areas that include, but are not limited to, the following: | • Temperature  
• Humidity and air quality  
• Power supply and voltage |
|                  | The environmental monitoring applications are configured to alert facilities and NOC personnel via e-mail alert notifications when predefined thresholds are exceeded. |                                                                                                                                 |
|                  | Air conditioning units are inspected on an annual basis.                  |                                                                                                                                 |
|                  | The third-party monitoring vendor notifies the on-call technician of any issues related to battery health. |                                                                                                                                 |
|                  | Generators are inspected and tested at least annually for proper performance in the event of a utility failure. Generator preventative maintenance is performed annually and tested under load conditions to help ensure proper operation during extended outages. Where generators are operated by the landlord, the landlord is required to perform monthly and annual maintenance. |                                                                                                                                 |
|                  | Hand-held fire extinguishers are inspected annually.                      |                                                                                                                                 |
|                  | UPS systems and batteries are inspected, and preventative maintenance is performed on at least an annual basis. |                                                                                                                                 |
|                  | Fire detection and suppression systems are inspected on an annual basis.   |                                                                                                                                 |
|                  | A third-party fuel supplier provides emergency refueling services in the event of an extended power outage. |                                                                                                                                 |

**Subservice Description of Services**

**MSP7700 and DFW400 Data Center Infrastructure - DataBank**

DataBank is a provider of data center infrastructure, communications, and related services, whose business offerings include secure, reliable space and high-speed dedicated and Internet-based communications for primary and backup data facilities, hosting, or remote storage. DataBank operates multiple 24x7x365 commercial data centers throughout the United States. DataBank provides infrastructure protection to their clients via environmental monitoring and failover capabilities. DataBank also provides 24-hour availability of its personnel to respond to client inquiries.
DataBank offers carrier-class facilities designed to meet industry standards. Multiple high-speed fiber entrances into their facilities and redundant cooling and power systems are standard. Support services and equipment are available on an "as needed" basis allowing clients to outsource only the services they really need.

Atomic Data utilizes DataBank as a colocation and infrastructure service provider for the MSP7700 and DFW400 data center facilities. Both buildings are home to dozens of major network carriers, who support a common, secure perimeter for the entire facility and demand the highest reliability for all common utility services.

Atomic Data occupies dedicated cages at these facilities, extending its standard access control, environmental monitoring, and video surveillance infrastructures to facilitate products and services. Clients may choose from rack, multi-rack, and dedicated cage colocation solutions. Atomic Data’s network services include flexible switching, multi-homed dedicated Internet, and point-to-point access to transport facilities via high-capacity metropolitan and long-haul network facilities.

**MSP7700 Data Center**

*Network and Connectivity:*
- Secure telecom entries into a carrier-class MMR (Meet-Me-Room)

*HVAC and Environmental Design:*
- Redundant HVAC design for stable airflow, temperature and humidity
- Highly efficient perimeter cooling system
- Hot-aisle/cold-aisle configuration
- Anti-static raised flooring and overhead cable runs allow unobstructed cold air delivery

*Power:*
- 5MW of on-site power deployed via underground diverse delivery
- Dedicated parallel UPS configuration
- Dedicated diesel generators
- Dedicated on-site fuel supply for each generator
- Fully redundant PLC switching configuration
- Multiple redundant power distribution paths
- Branch circuit monitoring

*Physical Security:*
- On-site security personnel 24x7x365
- Monitored security cameras and intercom system
- Fully secured mechanical/electrical equipment
- Dual-factor authentication (key card access w/secondary biometric) on exterior entry and all data center halls
- Camera surveillance on all ingress/egress points and critical areas
- Video with access log retention for 90 days
- Custom physical security controls available for customer deployments
- Power delivery, generator and diesel fuel infrastructure maintained in secured areas
DFW400 Data Center

**Network and Connectivity:**
- Diverse and secure telecom entries into a carrier-class
- DataBank-controlled MMR (Meet-Me-Room)
- Multiple secure fiber entrances

**HVAC and Environmental Design:**
- Redundant HVAC design for stable airflow, temperature and humidity control
- Highly efficient perimeter cooling system
- On-site secured water storage tanks
- Hot-aisle/cold-aisle configuration
- Anti-static raised flooring and overhead cable runs allow unobstructed cold air delivery

**Power:**
- 28.8MW (14.4MW A + 14.4MW B) of on-site power deployed via underground diverse delivery in a 2N design
- Dedicated 2N (A/B) UPS configuration
- Dedicated 2N (A/B) configuration for diesel generators
- Dedicated on-site fuel supply for each generator
- Fully redundant (2N) Automatic Transfer Switch
- (ATS) configuration
- Multiple redundant power distribution paths
- Branch circuit monitoring

**Physical Security:**
- On-site security and support personnel 24x7x365
- Monitored security cameras and intercom system
- Full perimeter fence with secured parking
- All mechanical/electrical equipment are fully secured
- Dual-factor authentication (key card and secondary biometric) on all data center entrances
- Camera surveillance on all ingress/egress points and critical areas
- Video with access log retention for 90 days
- Custom physical security controls available for customer deployments
- Power delivery, generator and diesel fuel infrastructure maintained in secured areas

**Complementary Subservice Organizations Controls**

The following subservice organization controls should be implemented by DataBank to provide additional assurance that the trust services criteria described within this report are met:

<table>
<thead>
<tr>
<th>Subservice Organization Controls - DataBank</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Availability</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Subservice Organization Controls - DataBank

<table>
<thead>
<tr>
<th>Category</th>
<th>Criteria</th>
<th>Applicable Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>On an annual basis, management contracts third-party vendors to complete inspections on the air handling units. Inspections and maintenance of all air handling units is completed by licensed third-party vendors on a schedule equal or better to manufacturer recommendations.</td>
<td>Data center areas are equipped with water detection devices to detect and mitigate the risk of water damage in the event of a flood or water leak.</td>
</tr>
<tr>
<td></td>
<td>Data center areas are available with raised flooring and/or server racks to elevate equipment and help facilitate cooling.</td>
<td>Data center power systems are constructed with redundant UPS units.</td>
</tr>
<tr>
<td></td>
<td>Data center power systems are constructed with redundant UPS units.</td>
<td>UPS systems are equipped with maintenance bypass or &quot;wrap around&quot; breakers and can be isolated from the protected load during UPS maintenance.</td>
</tr>
<tr>
<td></td>
<td>UPS systems are equipped with maintenance bypass or &quot;wrap around&quot; breakers and can be isolated from the protected load during UPS maintenance.</td>
<td>The data centers have redundant electrical utility feeds.</td>
</tr>
<tr>
<td></td>
<td>The data centers have redundant electrical utility feeds.</td>
<td>Power infrastructure is designed and constructed redundantly to mitigate risk to customer systems and services.</td>
</tr>
<tr>
<td></td>
<td>Power infrastructure is designed and constructed redundantly to mitigate risk to customer systems and services.</td>
<td>DataBank's backup generators are started and run on a weekly basis.</td>
</tr>
<tr>
<td></td>
<td>On an annual basis, management contracts third-party vendors to complete inspections on the air handling units. Inspections and maintenance of all air handling units is completed by licensed third-party vendors on a schedule equal or better to manufacturer recommendations.</td>
<td>DataBank maintains policy and procedure manuals for backup, storage, and restoration procedures.</td>
</tr>
<tr>
<td></td>
<td>DataBank maintains policy and procedure manuals for backup, storage, and restoration procedures.</td>
<td>DataBank standard backup configuration is set to automatically perform daily backups of customer systems.</td>
</tr>
<tr>
<td></td>
<td>DataBank standard backup configuration is set to automatically perform daily backups of customer systems.</td>
<td>An incident ticketing system is utilized to document, prioritize, escalate, and help resolve problems affecting services provided.</td>
</tr>
</tbody>
</table>

Atomic Data provides additional levels of monitoring and control independent of DataBank. A separate access control system is used to restrict access to the Atomic Data controlled cages. This system requires personnel to use proximity cards and PINs to access the cages. All access attempts are electronically recorded for future auditing and review. Digital surveillance cameras are operated by Atomic Data within its cages. These cameras are monitored 24×7 by the Atomic Data NOC and camera footage is retained for a minimum of 90 days. The NOC also monitors temperature and humidity in multiple areas, and historical data is retained for 365 days.
COMPLEMENTARY USER ENTITY CONTROLS

Atomic Data’s services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. Atomic Data control procedures cannot feasibly, solely achieve all of the Trust Services Criteria related to Atomic Data’s services. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Atomic Data.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities’ locations, user entities’ auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

<table>
<thead>
<tr>
<th>User Entity Control Considerations</th>
<th>Most Relevant Criteria Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Firewall: Defining security policies and access lists appropriate for its environment.</td>
<td>CC6.1, CC6.6, CC6.7, CC6.8, CC8.1</td>
</tr>
<tr>
<td>Managed Virtual Server Guest Data Protection: Configuring its environment to effect specific backup</td>
<td>CC6.7, CC6.8, CC8.1</td>
</tr>
<tr>
<td>policies at the operating system and application levels that exceed what the product provides,</td>
<td></td>
</tr>
<tr>
<td>including requirements to meet greater granularity, frequency, or availability needs.</td>
<td></td>
</tr>
<tr>
<td>Remote Access Methods: Determining the appropriate level of network exposure and ensuring that</td>
<td>CC6.1, CC6.6, CC6.7, CC6.8</td>
</tr>
<tr>
<td>individual accounts and services in the environment are properly managed and secured.</td>
<td></td>
</tr>
<tr>
<td>Acceptable Use of Network Services: Ensuring continuing, good-faith compliance with the Atomic Data</td>
<td>CC1.4, CC2.1, CC2.3</td>
</tr>
<tr>
<td>Acceptable Use Policy.</td>
<td></td>
</tr>
<tr>
<td>Physical Colocation-Physical Access: Sending timely written notification from authorized users to</td>
<td>CC6.1, CC6.2, CC6.4</td>
</tr>
<tr>
<td>Atomic Data of all employee changes for physical access.</td>
<td></td>
</tr>
<tr>
<td>Physical Colocation-Network Security: Providing network security services for its equipment for</td>
<td>CC6.1, CC6.2, CC6.4</td>
</tr>
<tr>
<td>which Atomic Data provides network access.</td>
<td></td>
</tr>
<tr>
<td>Operating System Security: For customer servers running at Atomic Data, maintaining appropriate</td>
<td>CC8.1</td>
</tr>
<tr>
<td>operating system patches as well as determining the appropriate security standards for user</td>
<td></td>
</tr>
<tr>
<td>accounts and restrictions on external administrative access.</td>
<td></td>
</tr>
<tr>
<td>Application Security: For applications hosted on customer servers, maintaining the appropriate</td>
<td>CC6.1, CC6.2, CC6.3, CC6.7, CC6.8</td>
</tr>
<tr>
<td>security standards for user accounts and maintaining restrictions on external administrative</td>
<td></td>
</tr>
<tr>
<td>access.</td>
<td></td>
</tr>
<tr>
<td>Autotask-Logical Access Administration: Sending timely written notification from authorized users</td>
<td>CC2.2, CC6.1</td>
</tr>
<tr>
<td>to Atomic Data of all employee changes for logical access administration. The customer is</td>
<td></td>
</tr>
<tr>
<td>responsible for changing ticket and contact portal access passwords as well as administering users’</td>
<td></td>
</tr>
<tr>
<td>privileges.</td>
<td></td>
</tr>
<tr>
<td>Autotask-Administrative Security: Keeping the list of active contacts, authorization levels, and</td>
<td>CC2.2, CC6.1</td>
</tr>
<tr>
<td>contact information up to date in the Contact Portal. When necessary, the customer must send</td>
<td></td>
</tr>
<tr>
<td>timely updates of contact information and access levels.</td>
<td></td>
</tr>
<tr>
<td>User Entity Control Considerations</td>
<td>Most Relevant Criteria Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>Autotask-Notification Groups: Notifying Atomic Data in a timely manner when maintenance notification groups should be updated to reflect changed personnel information.</td>
<td>CC2.2, CC6.1</td>
</tr>
<tr>
<td>Connectivity Services-Customer Premises Equipment: Providing security, backup, and operational capacity customer for any customer-owned network devices that terminate Atomic Data Connectivity Services.</td>
<td>A1.1</td>
</tr>
<tr>
<td>Software Security Requirements: Providing Atomic Data with prescriptive lists of security requirements necessary to protect the application.</td>
<td>CC2.2, CC2.3</td>
</tr>
<tr>
<td>Software Vulnerabilities: For applications hosted at Atomic Data, customers identifying and remediating application vulnerabilities, which may include regularly patching content management frameworks to prevent misuse.</td>
<td>CC6.7, CC8.1</td>
</tr>
</tbody>
</table>