A-LIGN

Atomic Data, LLC

Type 2 SOC 3

2025

ATOMIC data™

A-LIGN.COM

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

April 16, 2024 to April 15, 2025

Table of Contents

SECTION 1

ASSERTION OF ATOMIC DATA, LLC MANAGEMENT

ASSERTION OF ATOMIC DATA, LLC MANAGEMENT

April 22, 2025

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, 2024 to April 15, 2025, 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* in AICPA, *Trust Services Criteria*. 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, 2024 to April 15, 2025" 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, 2024 to April 15, 2025, to provide reasonable assurance that Atomic Data's service commitments and system requirements were achieved based on the trust services criteria. Atomic Data's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Atomic Data, LLC's Description of Its Managed Services System throughout the period April 16, 2024 to April 15, 2025".

Atomic Data uses Cologix to provide telecommunications services and Databank Holding, Ltd. ('Databank') to provide colocation, environmental infrastructure, and preventative maintenance services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization 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 organization 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, 2024 to April 15, 2025 to provide reasonable assurance that Atomic Data's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Atomic Data's controls operated effectively throughout that period.

Christopher E Heim

Chris Heim
CEO
Atomic Data, LLC

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

A-LIGN

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Atomic Data, LLC

Scope

We have examined Atomic Data's accompanying assertion titled "Assertion of Atomic Data, LLC Management" (assertion) that the controls within Atomic Data's Managed Services System were effective throughout the period April 16, 2024 to April 15, 2025, 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* in AICPA *Trust Services Criteria*.

Atomic Data uses Cologix to provide telecommunications services and Databank to provide colocation, environmental infrastructure, and preventative maintenance services. The description indicates that complementary subservice organization 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 organization 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 organization 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 also provided the accompanying assertion (Atomic Data assertion) about the effectiveness of controls within the system. When preparing its assertion, Atomic Data is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that 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 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

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

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements 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, 2024 to April 15, 2025, 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, if complementary subservice organization controls and complementary user entity controls assumed in the design of Atomic Data's controls operated effectively throughout that period.

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 System during some or all of the period April 16, 2024 to April 15, 2025, business partners of Atomic Data subject to risks arising from interactions with the Managed Services System, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity 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.

A-LIGN ASSURANCE

Tampa, Florida
April 22, 2025

SECTION 3

ATOMIC DATA, LLC'S DESCRIPTION OF ITS MANAGED SERVICES SYSTEM THROUGHOUT THE PERIOD APRIL 16, 2024 TO APRIL 15, 2025

OVERVIEW OF OPERATIONS

Company Background

Atomic Data is a privately-owned company with headquarters located at 250 Marquette Avenue South in Minneapolis, Minnesota. Initially founded in 2001 as a data center services provider, Atomic Data now provides a broad range of managed Information Technology (IT) solutions to hundreds of businesses across the United States.

Atomic Data manages three data center facilities, each connected via redundant 10-gigabit fiber links and numerous Internet connections with major international Internet Protocol (IP)-transit providers. Atomic Data partners with local exchange carriers and infrastructure providers to bring last-mile connectivity back to Atomic Data's core and managed national multi-protocol label switching (MPLS) wide-area network (WAN). This flexibility allows Atomic Data to host high-availability platforms, applications, and enterprise networks.

Atomic Data monitors and manages its infrastructure and services from its 24x7 Network Operations Center (NOC), from which aspects of the data center environments, network conditions, and hosting systems health are measured. The Atomic Data Client Support and NOC teams combine to provide 24x7 managed end-user support and other custom management services.

Atomic Data has a dedicated security and compliance team which sets a high standard for internal and client 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 enterprise IT solutions in four primary practice areas. These include:

1. Security and Compliance
2. Infrastructure and Cloud, including data center colocation
3. Data Intelligence and Automation
4. Microsoft Solutions

Security and Compliance

Atomic Data helps organizations strengthen security, reduce risk, and achieve or maintain compliance. Atomic Data assesses vulnerabilities, develops security programs, and enhances resilience through proactive threat detection, risk management, and incident response. Atomic Data's phased and managed approach to defense in depth is standardized around CIS controls and includes everything from security awareness training to data loss prevention, incident response, SOC as a Service, and more.

Infrastructure And Cloud, Including Data Center Colocation

Atomic Data is built on decades of expertise in data center, private cloud, and network design. On the frontlines, 24x7 NOC monitors, detects, and responds to every alert to keep your business running. Ten floors below, deep within a former Federal Reserve vault, the data center delivers cloud and connectivity solutions that meet your customers at the edge-while helping clients reclaim control from the hyperscalers. Network architecture services empower clients to develop their own advanced networks and data centers.

Atomic Data's facilities are built for maximum uptime, connectivity, and redundancy. Atomic Data offers data center colocation combined with engineers, partnerships, and all-encompassing service packages.

Available from 1U to multi-rack and private cage configurations, colocation allows small and midsize businesses to cost-effectively house their physical infrastructure and servers 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 services provided at the facility. Atomic Data directly controls and manages the colocation services provided at the DFW400 data center, while utilizing Databank as a subservice organization for facility infrastructure.

Data Intelligence and Automation

Accelerate your decision making and be more scientific with Atomic Data's artificial intelligence, machine learning, and automation platforms. Integrated with your applications and workflows, Atomic Intelligence and Automation will help you automate high-effort/low-value tasks, cut reliance on siloed data sources, and fine-tune the levers of success within clients' business.

Microsoft Solutions

With 20 years of Microsoft partnership, Atomic Data designs, implements, right-sizes, and manages Microsoft products across three key areas: identity, modern work, and infrastructure. From securing user access with Entra ID to optimizing Microsoft 365 for collaboration and managing Azure cloud environments, Atomic Data ensures clients' Microsoft ecosystem is secure, efficient, cost-effective, and scalable.

Principal Service Commitments and System Requirements

Atomic Data designs their processes and procedures to meet the objectives set for Managed Services products and services. Those objectives are based on the service commitments that Atomic Data makes to user entities, the laws and regulations that govern the provisioning of Managed 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 offerings 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 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 products and services.

Components of the System

The system is comprised of the following:

- Infrastructure
- Software
- People

- Policies and Procedures
- Client Data

Infrastructure

Atomic Data operates within the following office and data center facilities:

- MSP250
- DFW400
- MSP511

MSP250

MSP250 is the location of several of Atomic Data's facilities, including headquarter offices, the Network and Security Operations Center, Client Support, 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, multi-factor card-key access, and on-site security guards.

The MSP250 data center provides secure, 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.

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 operations are detailed in the "Subservice Organizations" section below. Atomic Data operates additional physical security and environmental controls within the leased space.

The DFW400 data center provides secure, 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, who operates the facility. As a subservice organization, Cologix operates physical security controls around access to the facility, and environmental controls and monitoring of the facility. Specifics of the controls Cologix operations 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

Atomic Data considers the specifics of the software they use to offer their services to be proprietary and confidential. Any specific questions can be answered during an in-person 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, Chris Heim. Business administration teams include People and Culture, Client Engagement, Revenue Operations and Sales, Legal, and Accounting. Technical operations teams include Security and Compliance, Network Engineering, Platform Engineering, Network and Security Operations Center, Professional Services and Engineering, Product Operations, Onsite Services, Client Support, and Service Offerings.

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.

People and Culture

The People and Culture department includes the Human Resources (HR) and Learning and Organizational Development teams. HR 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, and personnel-specific policies and procedures for employees and contractors. Additionally, annual background checks are required and maintained on file for employees and contractors.

The Learning and Organizational Development team is responsible for fostering a culture of continuous learning and leadership growth. This includes designing and implementing training programs, leadership development initiatives, and change management strategies to support employee and organizational effectiveness. The team ensures that employees have access to the resources, skills, and knowledge needed to drive business success while aligning development efforts with the company's core values and strategic goals.

Client Engagement

The Client Engagement department is responsible for ensuring that IT projects are conducted in a disciplined, well-managed, and consistent manner that ensures 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.

Revenue Operations and Sales

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

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

The marketing team is responsible for Atomic Data's internal and external brand and messaging. The team communicates the Atomic Data story 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 team uses these channels to build awareness, generate leads, attract new business, and aid in recruitment. The team is also responsible for overseeing the usage of licensed images and assets on behalf of Atomic Data.

Legal

The Legal department is responsible for ensuring the company's compliance with applicable laws and regulations while mitigating legal risks. This includes drafting, reviewing, and managing contracts, advising on corporate governance, overseeing regulatory compliance, and supporting risk management initiatives. The department works closely with leadership and key stakeholders to provide legal guidance that aligns with business objectives and protects the organization's interests.

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 day-to-day accounting operations, including payables and receivables, and oversees internal financial controls, ensuring accuracy, timely deliverables, and compliance.

Security and Compliance

The Security and 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 and 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 and Compliance department is also responsible for ongoing management and governance of Atomic Data's compliance initiatives, in coordination with HR and the VP of Technology Operations. This includes management of the Service Organization Control (SOC) 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.

The Security and Compliance department is also responsible for improving client security posture and strengthening their overall IT hygiene. This involves offering comprehensive policy and procedure development, security awareness training and phishing simulations, and vulnerability scanning and management.

Network Engineering

The Network Engineering department is comprised of Network and Data Center engineers. The department manages Atomic Data's IP transit network, IP address allocations, ISP services, colocation facilities, and client move-ins at the data centers. The Network Engineering department receives escalations from the NSOC and Client Support teams.

Platform Engineering

The Platform Engineering department builds and maintains scalable platform solutions that power Atomic Data and clients while managing critical business definitions and data flow across the ecosystem. The department creates reliable and efficient software systems through automation and streamlined IT processes to reduce cognitive load on engineers, ensure consistent data access for internal teams and clients, and embed vital policies into systems. The department focuses on delivering platform reliability, compliance with security frameworks, and technical innovation with goals of high platform availability, comprehensive automation, and maintaining high satisfaction scores for both developers and clients, ensuring Atomic Data can consistently scale and deliver high-quality solutions.

Network and Security Operations Center (NSOC)

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

Additionally, a core group of individuals on the NSOC team are trained to identify and respond to security incidents, operating as a Security Operations Center team within the NSOC. This team meets regularly with the Security and Compliance department members and assists with optimizing processes regarding identifying and responding to security events.

Professional Services and Engineering

The Professional Services and Engineering department is responsible for direct support of client workstations, servers, and local, on-site networks. This team manages the maintenance and architecture for client Windows domains. The Professional Services and Engineering department receives escalations from the Client Support and NSOC teams.

Product Operations

Product Operations engineers are responsible for the architecture and maintenance of Atomic Data's virtual server infrastructure, including VMware clusters, SAN storage, and load balancers. Product Operations engineers also manage Atomic Data’s platform for agent-based remote administration, which provides patch management, and monitoring for Atomic Data and client resources, as well as Atomic Data’s backup services. The Product Operations department receives escalations from the NSOC and Client Support teams.

Onsite Services

The Onsite Services department is responsible for direct support of Microsoft-based workstations, servers, and local, onsite networks. This team manages the maintenance of all client Windows domains. Onsite Services provides both remote and onsite support for client workstations, networks, and other equipment. The Client Support department provides Level I support to Onsite clients. The Onsite Services team receives escalations from Client Support regarding issues arising at client sites.

Client Support

The Client Support department provides 24x7 troubleshooting of client technical issues received via phone, e-mail, and the Service Desk mobile app. The Client Support department creates a ticket for each issue received. Client Support specialists use their knowledge, manuals, and troubleshooting guides to resolve the issue or determine if the issue needs to be escalated to a Level II or Level III engineer for resolution.

Service Offerings

The Service Offerings department shapes and identifies what products Atomic Data sells to clients and works with Engineering teams to ensure Atomic Data can deliver consistently to meet client expectations and needs. The Service Offerings department provides technical sales experience and is charged with moving Atomic Data's services/solutions to methods that are more consistent for customers. The Service Offerings department also engages with Engineering teams to ensure Atomic Data builds services that can scale, avoid being overly complex, and allow for high levels of automation for consistent work output.

Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, data security, and risk management. Personnel are expected to adhere to Atomic Data's policies and procedures that define how services should be delivered. These 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, multi-factor key card access to the facility and cages for authorized Atomic Data personnel and clients, comprehensive monitoring of internal and external environmental conditions, and extensive video surveillance.

Atomic Data also operates in facilities owned by Cologix and Databank. As such, some physical and environmental equipment protections are the responsibility of Cologix and Databank. For a listing of controls implemented by Cologix and Databank, refer to the 'Subservice Organizations' section below.

Logical Access

Logical access 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 (AD) account, which is required to gain access to any privileged network within the office or in conjunction with Multi-factor Authentication (MFA) for remote access. 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 - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to IT 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 patches. Clients and Atomic Data system owners review proposed patches to determine whether the patches are already applied. Clients 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 patches have been installed and, if applicable, that reboots have been completed.

Part of the infrastructure supporting the Managed Services is hosted within Databank and Cologix facilities. As such, some of the environmental equipment protections are the responsibility of Databank and Cologix. For a listing of controls implemented by Databank and Cologix, refer to 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 changes to Atomic Data internal and client infrastructure. The CMB reviews planned changes to Atomic Data's systems and network infrastructure to ensure that such changes meet 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.

Software Development Life Cycle (SDLC)

Atomic Data maintains documented SDLC policies and procedures to guide personnel in documenting and implementing application changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance (QA) 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. QA 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.

Data Communications

Atomic Data uses various means of communication to ensure that 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. Employees are encouraged and expected to communicate new, relevant information and exceptions arising from their individual job activities, observations of internal business operations, and the external environment. Managers from departments are expected to respect the value of such communication and respond appropriately.

The Client Support and NSOC teams 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 Client Support and NSOC teams, which identify, communicate, ticket, triage, and escalate warnings and critical alerts as appropriate. The system provides a complete overview of performance objectives at 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. Technical personnel contribute to the constant evolution and improvement of the overall system and are expected to be available 24 hours a day for escalations.

Client 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

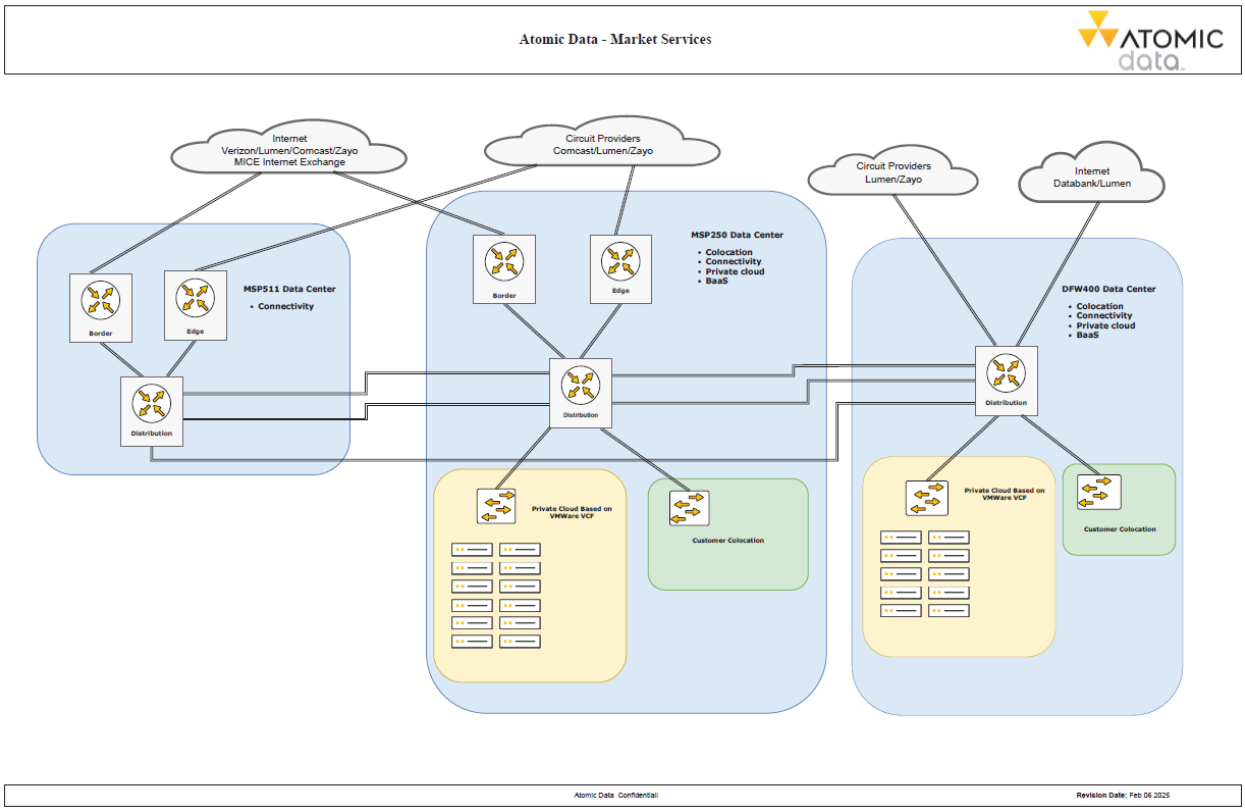
Client data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in client contracts.

Boundaries of the System

The scope of this report includes the Managed Services System products and services provided by Atomic Data in the Minneapolis, Minnesota facility.

This report does not include the telecommunications services provided by Cologix at the Minneapolis, Minnesota facility or the colocation, environmental infrastructure, and preventative maintenance services provided by Databank at the Dallas, Texas facility.

Atomic Data Network Overview



Changes to the System Since the Last Review

The MSP7700 data center location is no longer utilized for colocation. The decommissioning of the MSP7700 data center location was completed prior to the review period of this report.

Incidents 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/Security, Availability, and Confidentiality criteria were applicable to the Atomic Data Managed Services System products and services.

Subservice Organizations

This report does not include the telecommunications services provided by Cologix at the Minneapolis, Minnesota facility or the colocation, environmental infrastructure, and preventative maintenance services provided by Databank at the Dallas, Texas facility.

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
- DFW400 - Operated by Databank

Subservice Description of Services

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 DFW400 data center facility. The facility is home to dozens of major network carriers, who support a common, secure perimeter for the entire facility and demand the highest reliability for 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.

DFW400 Data Center

Network and Connectivity

- Diverse and secure telecom entries
- Diverse and secure fiber entries
- Multiple Databank-controlled MMRs (Meet-Me-Room)

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
- Mechanical/electrical equipment are fully secured
- Dual-factor authentication (key card and secondary biometric) on data center entrances
- Camera surveillance on 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

This report does not include the colocation, environmental infrastructure, and preventative maintenance services provided by Databank at the Edina, Minnesota and Dallas, Texas facilities.

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 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 staffed 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 is also available 24x7 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 Organization 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:

Subservice Organization Controls - Cologix		
Category	**Criteria**	**Applicable Controls**
Common Criteria/Security	CC6.4, CC7.2	Visitors are required to register in a visitor log prior to accessing the data center facilities. Logs are reviewed monthly to ensure that the logs were filled out completely, and logs are retained at least 90 days.
		Employee/contractor access to the data center requires approval by the employee/contractor's immediate entity supervisor.
		A badge access system is utilized to secure exterior and interior access to the office facility.
		The badge access system logs access attempts traceable to specific badge access cards. Security personnel review the access log on an ad hoc basis.
		Digital surveillance cameras are in place to monitor and record activity throughout the data center.
		Data centers are equipped with video surveillance cameras located throughout the premises and footage is retained for a minimum of 90 days.
		Badge access lists are reviewed monthly to help ensure data center access remains limited to authorized employee and customer personnel.
Availability	A1.2	A disaster recovery plan is maintained, updated, audited, and designed to respond to a range of facilities and/or operational incidents on a 24/7 basis that are a result of noncompliance with security policies.
		Management performs an assessment to identify potential threats of disruption to systems including an assessment of the physical and environmental risks to the facilities.
		Uninterruptible Power Supply (UPS) systems are in place to provide backup power in the event of a power outage.
		Generators are located on the premises to provide backup power in under a minute in the event of power failure.
		Data centers are equipped with pre-action sprinkler fire suppression systems.
		Hand-held fire extinguishers are inspected annually.

Subservice Organization Controls - Cologix		
Category	**Criteria**	**Applicable Controls**
		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 a quarterly basis.
		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.
		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.

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:

Subservice Organization Controls - Databank		
Category	**Criteria**	**Applicable Controls**
Common Criteria/Security	CC6.4	Visitors are required to register in a visitor log prior to accessing the data center facilities. Logs are reviewed monthly to ensure that the logs were filled out completely, and logs are retained at least 90 days.
		Employee/contractor access to the data center requires approval by the employee/contractor's immediate entity supervisor.
		A badge access system is utilized to secure exterior and interior access to the office facility.
		Badge access lists are reviewed monthly to help ensure data center access remains limited to authorized employee and customer personnel.
		Data centers are equipped with video surveillance cameras located throughout the premises and footage is retained for a minimum of 90 days.

Subservice Organization Controls - Databank		
Category	**Criteria**	**Applicable Controls**
	CC6.4, CC7.2	The badge access system logs access attempts traceable to specific badge access cards. Security personnel review the access log on an ad hoc basis.
		Digital surveillance cameras are in place to monitor and record activity throughout the data center.
Availability	A1.2	Data center areas are equipped with fire detection and suppression systems including: • Smoke detectors • Audible and visual fire alarms • Automated extinguisher system • Hand-held fire extinguishers
		Data center areas are equipped with multiple dedicated air handling units.
		On an annual basis, management contracts third-party vendors to complete inspections on the air handling units. Inspections and maintenance of air handling units are completed by licensed third-party vendors on a schedule equal or better to manufacturer recommendations.
		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.
		Data center areas are available with raised flooring and/or server racks to elevate equipment and help facilitate cooling.
		Data center power systems are constructed with redundant UPS units.
		UPS systems are equipped with maintenance bypass or "wrap around" breakers and can be isolated from the protected load during UPS maintenance.
		The data centers have redundant electrical utility feeds.
		Power infrastructure is designed and constructed redundantly to mitigate risk to customer systems and services.
		Databank maintains policy and procedure manuals for backup, storage, and restoration procedures.
		Databank standard backup configuration is set to automatically perform daily backups of customer systems.
		An incident ticketing system is utilized to document, prioritize, escalate, and help resolve problems affecting services provided.

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. 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 24x7 by the Atomic Data NSOC and camera footage is retained for a minimum of 90 days. The NSOC 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 solely achieve all 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.

Most Relevant Criteria Description	User Entity Control Considerations
CC6.1 CC6.6 CC6.7 CC6.8 CC8.1	Managed Firewall: User entities are responsible for defining security policies and access lists appropriate for its environment.
CC6.7 CC6.8 CC8.1	Managed Virtual Server Guest Data Protection: User entities are responsible for configuring its environment to effect specific backup policies at the operating system and application levels that exceed what the product provides, including requirements to meet greater granularity, frequency, or availability needs.
CC6.1 CC6.6 CC6.7 CC6.8	Remote Access Methods: User entities are responsible for determining the appropriate level of network exposure and ensuring that individual accounts and services in the environment are properly managed and secured.
CC1.4 CC2.1 CC2.3	Acceptable Use of Network Services: User entities are responsible for ensuring continuing, good-faith compliance with the Atomic Data Acceptable Use Policy.
CC6.1 CC6.2 CC6.4	Physical Colocation-Physical Access: User entities are responsible for sending timely written notification from authorized users to Atomic Data of employee changes for physical access.
CC6.1 CC6.2 CC6.4	Physical Colocation-Network Security: User entities are responsible for providing network security services for its equipment for which Atomic Data provides network access.

Most Relevant Criteria Description	User Entity Control Considerations
CC8.1	Operating System Security: User entities are responsible for maintaining appropriate operating system patches, as well as determining the appropriate security standards for user accounts and restrictions on external administrative access, for customer servers running at Atomic Data.
CC6.1 CC6.2 CC6.3 CC6.7 CC6.8	Application Security: User entities are responsible for maintaining the appropriate security standards for user accounts and maintaining restrictions on external administrative access for customer servers running at Atomic Data.
CC2.2 CC6.1	Autotask-Logical Access Administration: User entities are responsible for sending timely written notification from authorized users to Atomic Data of employee changes for logical access administration. The customer is responsible for changing ticket and contact portal access passwords as well as administering users' privileges.
	Autotask-Administrative Security: User entities are responsible for keeping the list of active contacts, authorization levels, and contact information up to date in the Contact Portal. When necessary, the customer send timely updates of contact information and access levels.
	Autotask-Notification Groups: User entities are responsible for notifying Atomic Data in a timely manner when maintenance notification groups should be updated to reflect changed personnel information.
A1.1	Connectivity Services-Customer Premises Equipment: User entities are responsible for providing security, backup, and operational capacity customer for any customer-owned network devices that terminate Atomic Data Connectivity Services.
CC2.2 CC2.3	Software Security Requirements: User entities are responsible for providing Atomic Data with prescriptive lists of security requirements necessary to protect the application.
CC6.7 CC8.1	Software Vulnerabilities: User entities are responsible for identifying and remediating vulnerabilities within applications hosted at Atomic Data, which may include regularly patching content management frameworks to prevent misuse.