



**Atomic Data, LLC  
Minneapolis, Minnesota**

**SOC 3® Report for Atomic Data, LLC**

April 16, 2016 to April 15, 2017



**WIPFLI**<sub>LLP</sub>  
CPAs and Consultants

SOC 3® is a registered service mark of the American Institute of Certified Public Accountants

*This report is not to be copied or reproduced in any manner without the express written approval of Atomic Data, LLC and Wipfli LLP. The report, including the title page, table of contents, and exhibits constitutes the entire report and should be referred to only in its entirety and not by its component parts. The report contains proprietary information and is considered confidential.*

# Table of Contents

---

Section 1: Atomic Data, LLC’s Assertion on Controls .....	2
Section 2: Independent Service Auditor’s Report .....	4
Section 3: Description of the Managed-infrastructure and Enterprise IT Services Provided by Atomic Data, LLC.....	6
Overview .....	7
Description of Services.....	8
Organization, Management, and Functional Responsibilities.....	12
Relevant Aspects of the Control Environment .....	19
Roles and Responsibilities .....	20
Subservice Organizations and Facilities .....	22
Atomic Data Network Overview .....	24
Atomic Data Security Controls.....	25

# **Section 1**

## **Atomic Data, LLC's Assertion on Controls**

---

## **Management of Atomic Data, LLC's Assertion Regarding the Effectiveness of Its Controls Over the Managed-infrastructure and Enterprise IT Services Based on the Trust Services Principles of Security, Availability, and Confidentiality**

Atomic Data, LLC (Atomic Data) maintained effective controls over the security, availability, and confidentiality of Atomic Data's Managed-infrastructure and Enterprise IT Services ("the system") to provide reasonable assurance, during the period April 16, 2016 through April 15, 2017, based on the American Institute of Certified Public Accountant's (AICPA) Trust Services Criteria for Security, Availability, and Confidentiality, which are available at [www.aicpa.org](http://www.aicpa.org), that:

1. The system was protected from unauthorized access, use, or modification.
2. The system was available for operation and use, as committed or agreed.
3. Information designated as confidential was protected by the system, as committed or agreed.

The attached system description in Section of Atomic Data's Managed-infrastructure and Enterprise IT Services summarizes the aspects of this system covered by our assertion.

# **Section 2**

# **Independent Service Auditor's Report**

## Independent Service Auditor's Trust Services Report

### *Scope*

We have examined management's assertion that during the period April 16, 2016 through April 15, 2017, Atomic Data, LLC ("Atomic Data") maintained effective controls over the Managed-infrastructure and Enterprise IT Services (the "System") to provide reasonable assurance that:

- The system was protected from unauthorized access, use, or modification;
- The system was available for operation and use, as committed or agreed; and
- Information designated as confidential was protected by the system, as committed or agreed;

based on the AICPA and CPA Canada trust services security, availability, and confidentiality criteria.

Atomic Data's management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the managed services system covered by its assertion is attached. We did not examine this description, and accordingly we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Atomic Data's relevant controls over the security, availability, and confidentiality of the the Managed-infrastructure and Enterprise IT Services system; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

### *Inherent Limitations*

Due to the nature and inherent limitations of controls, Atomic Data's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

### *Opinion*

In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on the AICPA an CPA Canada trust services security, availability, and confidentiality criteria.

*Wipfli LLP*

Wipfli LLP

May 5, 2017  
St. Paul, Minnesota

# **Section 3**

## **Description of the Managed- infrastructure and Enterprise IT Services Provided by Atomic Data, LLC**

---



## General Overview

Atomic Data, LLC (“Atomic Data” or the “Company”) is a privately owned Minnesota company with headquarters located at 615 North Third Street in Minneapolis, Minnesota. Atomic Data has additional office locations located at 250 Marquette Avenue South in Minneapolis, Minnesota, and 750 B Street in San Diego, California. Jim Wolford and Larry Patterson founded Atomic Data in 2001. They continue to 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 customers, Atomic Data has grown to manage nine data center facilities worldwide, with a core group of three world-class 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 MPLS wide-area network. This flexibility allows Atomic Data to host high-availability websites, applications, enterprise WAN networks, and VoIP services for its customers.

Atomic Data monitors and manages its services from its 24/7 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 24/7 managed help desk services and other custom management services.

Atomic Data has a dedicated Security and Compliance team, 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 of proposed changes including services, policies, organizational changes, risk acceptance or remediation, and changes to the control environment.



## Description of Services

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

1. The Atomic Cloud®
2. Data Center Colocation
3. Enterprise Architecture and Implementation
4. Compliance as a Service
5. 24/7 Network Monitoring and Management
6. 24/7 Technical Support
7. Orange Book—Annual IT Asset Review and Budget Planning
8. Server and Workstation Management
9. Remote Data Backup and Disaster Recovery Products
10. Connectivity and ISP Services
11. Hosted Solutions
12. Web and Software Development
13. Software and Platform Optimization Services
14. Voice Solutions

### The Atomic Cloud®

Atomic Data can help customers build the perfect cloud solution that leverages existing IT resources and aligns seamlessly with a customer'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. Customers may purchase Atomic Data monitoring and Atomic Data patch-management services for their virtual servers. Atomic Data patches, monitors, and manages Windows virtual servers with Kaseya enterprise management software. Atomic Data patches, monitors, and manages Linux virtual servers with Opsview and other enterprise management software.

### Data Center Colocation

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

Available from 1U to multi-rack and private cage configurations, colocation allows 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 as a subservice provider for facility infrastructure.

## **Description of Services (Continued)**

### **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. Systems Engineering and Network Engineering teams provide network and application architecture, design, and implementation for customers. Enterprise implementations include WAN design, LAN design, cloud architecture and migration planning, storage evaluation and recommendations, disaster recovery playbooks, and more. Enterprise implementation services are tailored to meet specific customer technology needs.

### **Compliance as a Service**

The safety and security of customer data is Atomic Data's highest priority. Whether it's PCI, HIPAA, SOC 2 or SOC 3, Atomic Data's industry-certified security and compliance experts can help customers safeguard their data by preparing for and passing a multitude of industry-specific security and compliance audits. Engineers and security specialists will assist customers in implementing managerial oversight, comprehensive policies and procedures, physical and logical access controls, computing/software/network controls, data destruction techniques, and more.

### **24/7 Network Monitoring and Management**

Atomic Data's Network Operations Center (NOC) provides remote monitoring, utilizes management tools, identifies, and resolves network issues to prevent downtime for customer and internal networks. Using tools such as Zenoss, Nagios, Splunk, Kaseya, and Opsview, Atomic Data's highly trained and experienced NOC technicians monitor customer networks 24/7 and are just a call, email, or Web portal ticket away. In addition to monitoring data centers, routers, switches, servers, applications, storage networks, and websites, Atomic Data can also manage incident response, serving as the first line of defense when network issues arise.

### **24/7 Technical Support**

Operating from redundant Minneapolis locations, Atomic Data offers 24/7 email, phone, and Web portal-based support for a customer's employees, executives, and even their customers. Atomic Data's Service Desk and On-Site Support 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, and peripherals to 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 customers. For more complex issues or those which cannot be resolved remotely, the Service Desk will escalate the issue to the On-Site Support department for resolution.

Operating desk-side as well as remotely, the On-Site Services department is composed of field-based engineers who provide customer support including but not limited to business application server support, email management and support, desktop management and support, network directory services, LAN/WAN security management, and more. In addition to regularly scheduled maintenance and support, On-Site Services also provides LAN/WAN technical support on a time-and-materials basis or as prepaid services.

## **Description of Services (Continued)**

### **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 customer'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 customers a useful first step in defining a custom maintenance regime, future-state upgrades, and IT-related financial planning that fit their network's specific components and complement their business plan.

### **Server and Workstation Management**

Atomic Data will take on the burden of patching, securing, monitoring, and auditing servers and workstations to save customers time and money, using advanced management tools like Kaseya. Customers 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 24/7 Network Operations Center (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 customers' critical data. Multi-level backup options for workstations, laptops, and servers at file or block levels allow customers to configure a secure, cost-effective backup scheme tailored to their specific business needs. Atomic Data also offers disaster recovery options tailored to balance the customer's budget and risk management requirements. From off-site data backup to a fully equipped secondary site, Atomic Data's data security consultants help customers choose the option that best meets their needs.

### **Connectivity and 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 customers 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 metro-Ethernet circuits from 10 mbps up to 1000 mbps and beyond, traditional circuits such as DS3s and T1s, 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 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 remove the burden of server maintenance and administration.

## **Description of Services (Continued)**

### **Web and Software Development**

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

Atomic Data's senior software architects and business analysts engage with customers at the front end of the software development life cycle (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 customer timeline and budget goals. Atomic Data provides flexible application development options, including complete software development services, hybrid development teams that include internal customer employees, and simplified leadership and mentoring of customer development teams by senior Atomic Data software architects.

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

### **Software and Platform Optimization Services**

Atomic Data provides infrastructure as a service for large software platforms and customers 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 customers in managing the deployment and ongoing monitoring and maintenance of customer 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 and Systems Engineering teams ensure that customer applications are running at their peak efficiency within Atomic Data's shared infrastructure at all times.

### **Voice Solutions**

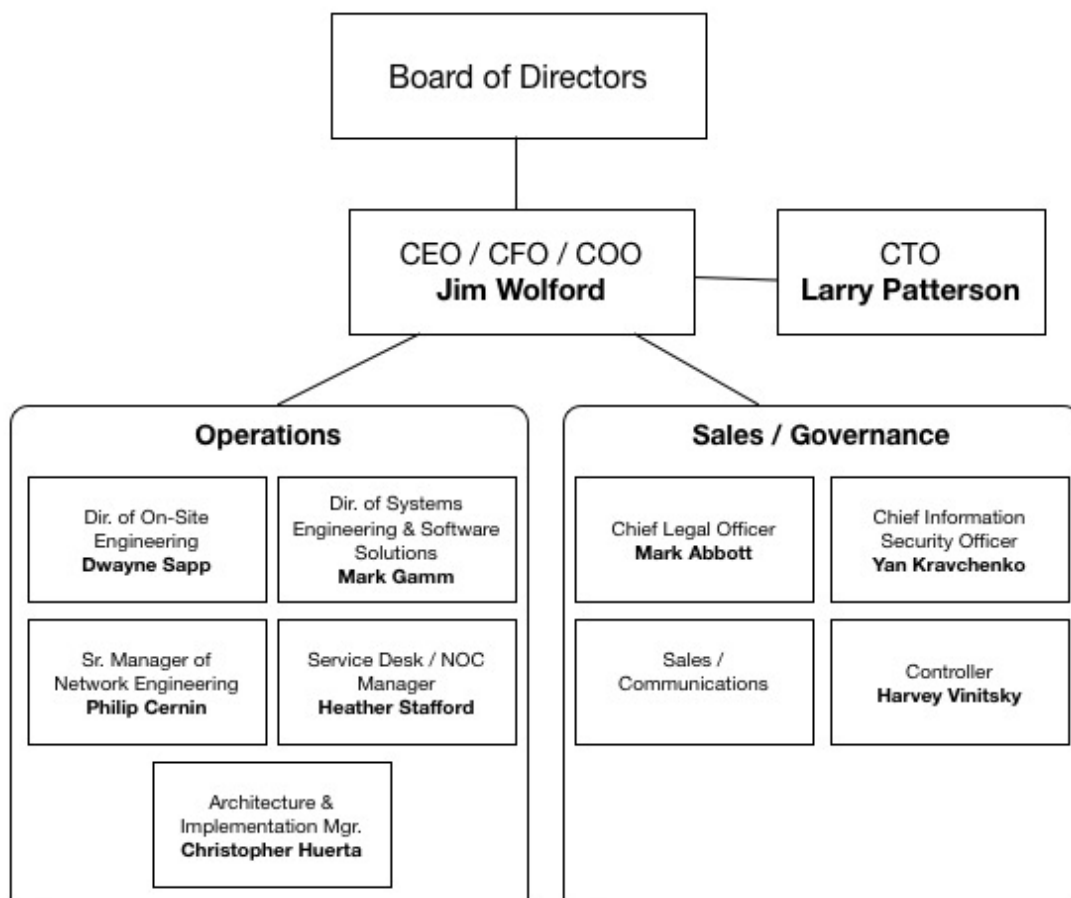
Atomic Data's hosted VoIP offerings are built on top of a combination of Session Initiation Protocol (SIP) trunks, Public Relay Interfaces (PRI), and a ShoreTel VoIP system. A hosted VoIP solution combined with Atomic Data bandwidth over an MPLS network provides customers an enterprise VoIP solution without requiring an equipment investment and ongoing system management and maintenance. With SIP trunks and PRIs residing within an enterprise data center facility, a customer'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 its hosted VoIP products, Atomic Data also provides colocation of ShoreTel and other voice systems owned by customers, as well as on-premise ShoreTel implementations.

## Organization, Management, and Functional Responsibilities

Atomic Data is organized into functional areas supporting general business administration and technical operations under the executive leadership of CEO Jim Wolford. Sales/Governance teams include Security and Compliance, Communications, Sales, Accounting, Operations, and Human Resources. Technical Operations teams include Account Management, Service Desk, NOC, On-Site Services, Network Engineering, Systems Engineering, and Software Solutions. This organizational structure is depicted here:



## **Organization, Management, and Functional Responsibilities (Continued)**

### **Leadership Team**

Overall operations of Atomic Data are under the direction of a senior executive management team that reports directly to Mr. Wolford. The senior executive management team of Atomic Data includes:

#### Jim Wolford, Chief Executive Officer, Chief Financial Officer, and Chief Operations Officer

As CEO/CFO/COO, Mr. Wolford is responsible for providing the leadership necessary to position Atomic Data at the forefront of the industry. This includes developing a strategic plan to advance Atomic Data's mission and objectives and to promote revenue, profitability, and growth as an organization. Mr. Wolford works with the leadership team to establish long-range goals, strategies, plans, and policies.

For the greater part of the last 17 years, Mr. Wolford has assisted Minneapolis-based corporations with their strategic Internet plans and has assisted in the project management of their business systems. Working on projects from hardware architecture to full supply chain management software tools, he has gained valuable experience in all facets of the new digital economy. Mr. Wolford's skill set lies in his understanding of traditional business processes and the capabilities of the new digital age. Combining these two understandings allows him to weigh all aspects of the decision-making process in regard to design, architecture, development, implementation, and post-development strategies. Mr. Wolford attended St. John's University in Collegeville, Minnesota, and obtained a bachelor of arts degree in political science and history.

#### Larry Patterson, Chief Technology Officer

As CTO, Mr. Patterson's responsibilities include overseeing all technical aspects of Atomic Data. He works with the leadership team to apply the use of technological resources and actively participates in day-to-day network services as a Level III Engineer for external and internal customers. Mr. Patterson directs employees involved in program development and deployment to attain the customer's expectations and satisfaction.

Mr. Patterson served as the Chief Network Engineer at ORIGIX, a startup network service provider in Minneapolis. Prior to ORIGIX, he was a consultant with 3M Corporation where he designed health care information systems currently used in medical manufacturing. Mr. Patterson attended the University of Minnesota Institute of Technology.

#### Mark Abbott, Chief Legal Officer

As CLO, Mr. Abbott oversees all legal matters for the Company. He is responsible for negotiating, managing, and enforcing contracts; maintaining regulatory compliance; and responding to emerging business and legal issues internally and with Atomic Data's partners and customers. Mr. Abbott works with other members of the executive leadership team to develop and advise on strategic goals, assess risks from contemplated business decisions, and proactively resolve nascent issues that could evade organizational controls.

Mr. Abbott possesses an extensive legal and technical background in operating security, compliance, and organization controls for cloud and data center service providers. His leadership career began in the early 1990s when he served as service manager and then senior solutions integrator for Minnesota-based Cybernet Systems, Inc. In 2001, Mr. Abbott founded his own corporation, Abbott Systems, Inc., where he focused on integrating high-volume data networks with efficient business processes for the printing and publishing industries. He joined Atomic Data, LLC in 2007, when he began work as Director of Special Projects. Mr. Abbott was promoted to Chief Information Officer in 2010 and CLO in 2015.

## **Organization, Management, and Functional Responsibilities (Continued)**

### **Leadership Team (Continued)**

Mr. Abbott received a B.A. from Macalester College with majors in mathematics and computer science. In 2006, he was awarded a J.D., cum laude, from the University of Minnesota Law School and an M.B.A. from the University of Minnesota, Carlson School of Management.

#### Yan Kravchenko, Chief Information Security Officer

As CISO, Mr. Kravchenko is responsible for managing the Security and Compliance resources. He confronts the evolving and ever-present data security challenges facing Atomic Data and its customers.

Mr. Kravchenko brings more than 19 years of technology and information security experience to Atomic Data, the last six of which he served as compliance advisory practice lead at NetSPI. He primarily addressed unique security and compliance challenges in the health care space during that time. In addition, Mr. Kravchenko has six years of experience in the payment card industry as a practicing QSA. Mr. Kravchenko received a B.S. degree in Information Systems Management from Regis University. He also holds a wide array of industry certifications including CISSP, CSSLP, CISA, and CISM.

#### Harvey Vinitsky, Controller

As Controller, Mr. Vinitsky assists the CFO with the financial affairs of Atomic Data and with preparation of financial analyses of operations, including financial statements with supporting schedules for the guidance of management. He is responsible for management of day-to-day accounting operations, including payables and receivables, and oversees internal controls, ensuring accuracy, timely deliverables, and compliance.

Mr. Vinitsky brings over 50 years of experience in the accounting and finance industries to Atomic Data. For nearly 35 years, he worked as credit manager for a floor covering distributor. During this time, Mr. Vinitsky's main responsibilities included extending credit lines and collecting payments on accounts. He served as controller for a retail furniture company for six years before joining Atomic Data.

#### Mark Gamm, Director of Systems Engineering and Software Solutions

As Director of Systems Engineering and Software Solutions, Mr. Gamm is responsible for managing the Systems Engineering and Software Solutions resources. He also oversees the management and maintenance of Atomic Data's hosted products, delivery of Systems and Software customer projects, and architecture and design decisions of products and custom customer solutions.

Prior to joining Atomic Data, Mr. Gamm was a Senior Software Architect and Practice Lead with 1543AD, now a part of Atomic Data. He also spent considerable time with Appolis, Inc., PolarFab, Inetium, Inc., and VTC, Inc., working his way up from development technician to senior solutions developer and product manager. Mr. Gamm is a graduate of Anoka-Hennepin Technical College.

#### Dwayne Sapp, Director of On-Site Services

As Director of On-Site Services, Mr. Sapp is responsible for managing the On-Site Engineering, Project Coordination, and Account Management resources dedicated to Atomic Data's On-Site customers.

Prior to joining Atomic Data, Mr. Sapp held positions in engineering, sales engineering, and strategic sales for telecom carriers and equipment manufacturers. He is a veteran of the U.S. Army.

## **Organization, Management, and Functional Responsibilities (Continued)**

### **Leadership Team (Continued)**

#### Christopher Huerta, Architecture and Implementation Manager

As Architecture and Implementation Manager, Mr. Huerta manages a group of expert resources who are committed to architecting and implementing solutions tailored to meet the needs of our customers.

Mr. Huerta has been building, supporting, and managing IT environments and professionals for almost 20 years. His IT experience reaches across several markets including banking, retail, supply chain, and disability services. Mr. Huerta is a graduate of Capella University.

#### Heather Stafford, Manager of Service Desk and NOC

As Manager of Service Desk and NOC, Ms. Stafford is responsible for managing the Service Desk and NOC resources. She also manages the relationship between the Atomic Data Service Desk and several partner Service Desks.

Prior to joining Atomic Data, Ms. Stafford was customer support supervisor for OneNeck IT Solutions, formally VISI. She also spent time with ipHouse as a service desk technician. Prior to working as customer support supervisor, Ms. Stafford worked her way up from a customer support technician Level I. She holds an ITIL Foundations certification.

#### Philip Cernin, Senior Manager of Network Engineering

As Senior Manager of Network Engineering, Mr. Cernin is responsible for managing and leading a team of Network and Data Center Engineers who maintain the health and integrity of hundreds of customers' networks. He also works closely with the Data Center Engineering team, ensuring the stability and security of the Company's data centers.

Mr. Cernin brings 15 years of telecom and IT experience to Atomic Data. He has worked primarily on the MSP side of technology/telecommunications over his IT career, focused on managing professional services resources, engagements, and deployment services across all Cisco architectures. Mr. Cernin is a graduate of St. Olaf College with a BA in Sociology and Management Studies and he holds the ITIL v3 certification.

### **Functional Responsibilities**

Atomic Data assigns personnel to departments organized around technical and professional responsibilities, as indicated by the organizational chart above. 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.



## **Organization, Management, and Functional Responsibilities (Continued)**

### **Functional Responsibilities (Continued)**

#### 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's computing infrastructure.

The Security and Compliance department is also responsible for ongoing management and governance of Atomic Data's compliance initiatives in coordination with Human Resources and the CEO. This includes management of the Service Organization Control (SOC) program and oversight of the supporting controls. Examples of these responsibilities include performing security testing; performing security incident investigation and analysis; developing and conducting security awareness training; 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; analyzing the control impact of Change Impact Summaries (CIS) for the Change Advisory Board (CAB); 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, email 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 prepares responses to Requests for Information (RFI) and Requests for Proposal (RFP) and is also responsible 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 customers, evaluating the existing customer base for additional sales opportunities, and preparing and delivering all eQuotes, proposals, and completed responses to RFIs and RFPs. In addition, the Atomic Data 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 have to be entered into the system to be fulfilled and also require proper senior management authorization.

The Sales department maintains customer relations and develops and maintains strategic partnerships and relationships with complementary vendors and strategic resellers in order 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 preparation of 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.

## **Organization, Management, and Functional Responsibilities (Continued)**

### **Functional Responsibilities (Continued)**

#### Human Resources

The Human Resources (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 and outline and maintain job descriptions and facilitates candidate searches through recruiting activities and the interview process. 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. Annual background checks are conducted and maintained on file by the HR department for all employees and contractors. A key element supporting recruiting, development, and retention activities is HR's benefits development and administration in coordination with the CEO.

#### 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 customers. In addition, the Software Solutions department provides full-service development, testing, deployment, and support as part of the software development life cycle.

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 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 customer project plans, timelines, and events and obtaining customer feedback upon the implementation of products and/or services.

#### Service Desk

The Service Desk provides 24/7 troubleshooting of customer technical issues received via phone, email, 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 whether the issue can be resolved at their level or whether the issue needs to be escalated to a Level II or Level III Engineer for resolution.

## **Organization, Management, and Functional Responsibilities (Continued)**

### **Functional Responsibilities (Continued)**

#### Network Operations Center

The Network Operations Center (NOC) is responsible for responding to any potential issues related to Atomic Data's 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 customers and as such helps management monitor company trends. The NOC department is responsible for the day-to-day monitoring, maintenance, and administration of all Atomic Data and customer circuits, internal networking devices, NOC management systems, and Linux-based servers. The Service Desk and Network Operations Center share a common heritage at Atomic Data, so many NOC and Service Desk personnel are cross-trained for duties within the other department.

#### On-Site Services

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

#### Network Engineering

The Network Engineering department manages Atomic Data's IP transit network, IP allocations, ISP services, colocation facilities, physical colocation services, and all customer move-ins at the data centers. In addition, the Network Engineering team receives Level I, II, and III Cisco escalations from the NOC and Service Desk.

#### Systems Engineering

The Systems Engineering department is responsible for meeting the demands of customers with sophisticated Linux and Windows systems administration needs, including complex database integration, application clustering and availability engineering, code development and performance optimization, and enterprise LAN and WAN network architecture. The Systems Engineering department also is responsible for the architecture and maintenance of Atomic Data's virtual server infrastructure, including VMware clusters, SAN storage, tape backup services, firewalls, and load balancers. Systems Engineering also manages Atomic Data's Kaseya product, which provides patch management, monitoring, and antivirus for Atomic Data and customer resources as well as Atomic Data's Black Box product, which provides for backup and disaster recovery of critical customer server systems.

The Systems Engineering and Network Engineering departments share a common heritage at Atomic Data, so engineers from either group are often cross-trained for duties within the other department.

## Relevant Aspects of the Control Environment

The control environment is the foundation for all other areas of internal controls. As such, the control environment of Atomic Data sets the tone for the Company and influences control conscientiousness and discipline of employees. Atomic Data management emphasizes the importance of controls and ethical behavior throughout the Company.

In addition, Atomic Data has instituted oversight and governance committees that are responsible for managing change throughout the organization, assessing risk, and promoting growth while sustaining the control environment. These committees consist of the Change Advisory Board and the Security Advisory Board.

### Change Advisory Board

The Atomic Data Change Advisory Board (CAB) is responsible for overseeing and monitoring the overall company operating environment, including risk identification and management, internal control monitoring, and review and approval of architectural changes that could significantly impact Atomic Data's control environment or the safety of customer data.

The CAB meets on a monthly basis and is composed of Atomic Data leadership and senior staff representing administrative, operating, and customer-facing areas of the Company. The CAB reviews and approves planned and proposed changes to the organization, technology infrastructure, and control environment to assess potential risks and impact to the control environment. The CAB also reviews the collection of identified and completed Atomic Data events over the previous month to determine whether any continuing risks are emerging. The CAB identifies any items requiring additional investigation or work performed and identifies the appropriate resource for completion.

### Security Advisory Board

The Atomic Data Security Advisory Board (SAB) is responsible for identifying, evaluating, mitigating, and monitoring security risks to the organization, customer data, and the control environment. Functioning in a security steering committee capacity, the SAB:

- Reviews change requests with impact to information security.
- Evaluates security threats/vulnerabilities.
- Monitors security metrics.
- Prioritizes security risks.
- Reviews results of internal/external audits and security assessments.
- Owns the design of the Atomic Data's control network environment.
- Evaluates all information security incidents.

The SAB meets on a weekly basis and is composed of a diverse selection of personnel who represent a comprehensive breadth of expertise and organizational interests. Whenever necessary, the SAB reviews proposed control environment changes for security impact on behalf of the CAB. This includes network security changes that are designated for SAB-controlled change management. These changes may be presented and approved during the weekly SAB meeting. The SAB reports to the CAB on a monthly basis, which includes updates on security initiatives, security risks, and technical risk decisions.

## **Relevant Aspects of the Control Environment (Continued)**

### **Additional Operational Procedures**

In addition to the formalized committees outlined above, all management and supervisory personnel continuously evaluate and monitor internal control performance as a routine part of the quality control process. On a daily and weekly basis, core departments produce key-indicator management reports, which measure the performance and effectiveness of the various functions involved in providing customer services and products. These reports are distributed to the management team and reviewed individually and collectively to allow collaborative and proactive identification of risks and deficiencies and corrective action as needed.

Atomic Data uses additional information assembled and gathered from financial, operational, compliance-related, and relevant external sources to inform decision making and control the business. Formalized policies and procedures are stored in a location readily accessible to those responsible for their execution and easily updated by their owners. Organic and tacit controls and business processes are formalized and refined whenever appropriate. Customer-specific information and processes are stored securely for easy retrieval and review. All employees are empowered to document and internally publish their experiential operational knowledge and to review, comment on, and learn from the knowledge shared by other employees. Individual internal and customer-facing activities are documented in a structured ticketing system that allows simple content searching for issue recognition and correlation.

### **Roles and Responsibilities**

Atomic Data uses various means of communication to ensure that all employees understand their individual roles and responsibilities for providing services to customers and promoting timely notification of significant events. Continuous communications and hands-on training help ensure that employees are aware of important policy and organizational events and changes. 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. Furthermore, employees receive written job descriptions that clearly define roles, responsibilities, and expectations.

The HR department maintains written job descriptions for all Atomic Data employees. Written job descriptions are reviewed periodically and revised as necessary by HR and the appropriate department head. Written policy requires all potential employees to consent to Atomic Data performing a background check at an appropriate point in the hiring process. After hire, Atomic Data performs annual background checks on all employees. Atomic Data's vacation policy is structured to encourage employees to take vacation in the calendar year in which it is earned.

All supervisors are required to annually provide a written performance evaluation of each of their direct reports. These reviews are based on employee-stated goals and objectives that are prepared and reviewed with the employee's supervisor. The employee's performance is assessed on the basis of his or her compliance with the policies, procedures, and other controls that apply generally to all employees, as well as those which apply to the individual employee based on his or her functional and departmental area. Completed appraisals are reviewed by senior management and become a permanent part of the employee's personnel file.

## **Roles and Responsibilities (Continued)**

### **Organization Monitoring and Risk Assessment**

Atomic Data utilizes a variety of organizational monitoring methods and risk assessment processes that help identify, analyze, and manage risks which could affect Atomic Data's ability to provide reliable services for its customers. Collectively, these processes continuously assess changing internal, operational, and external conditions.

### **Quality Control and Management Oversight**

Atomic Data management utilizes several risk assessment processes to identify and manage risks that could affect the Company's ability to provide reliable services for their customers. One of those processes is the Service Desk Dashboard Report, which is prepared and reviewed daily by the Operations Management team and other personnel. The Service Desk Dashboard Report contains information regarding issues that are due to be resolved, issues submitted, issues completed, the priority and status of issues, issue type, and resources assigned to issues. The Operations Management team reviews these reports so they are aware of any ongoing issues and can follow up on any outstanding items, if necessary.

### **External and Internal Risk Assessment**

Atomic Data has implemented an ongoing risk management methodology by which risks are evaluated in weekly and monthly governance meetings. Risks are identified by a combination of internal and external security assessments as well as changes in the overall threat and technology landscape. In addition, Atomic Data collects information about security incidents and suspicious activities, which are used to identify and remediate vulnerabilities. Operations management performs periodic and on-demand reviews of any recent events involving its major data centers and service providers to help identify areas for improvement. Leadership regularly reviews the Company as a whole and in the context of the broader industry and economic environment to anticipate and plan against future risks.

### **Communications**

Service Desk and NOC reports are prepared on a twice-daily basis. These reports include important information about products and services, alerts, customers, and internal tasks relevant for the past 24 hours. Other departments review these reports daily and are expected to communicate perceived possible risks and offer recommendations toward resolution, prevention, or mitigation. Management uses these collective, ongoing reports as major inputs to Atomic Data's internal quality control.

## Subservice Organizations and Facilities

In addition to the office facilities, Atomic Data operates at the following data center facilities:

- MSP250: 250 Marquette Avenue South, Minneapolis, Minnesota 55401
- MSP511: 511 11th Avenue South, Minneapolis, Minnesota 55415
- MSP7700: 7700 France Avenue South, Edina, Minnesota 55435
- DFW400: 400 South Akard Street, Dallas, Texas 75202

### MSP250 Data Center Infrastructure

#### *Atomic Data*

Atomic Data assumed operational responsibility for the facility in early 2014. The facility provides secure, highly controlled space and redundant network access for colocation equipment. Customers may choose from a wide range of space offerings including rack, multi-rack, dedicated cage, and dedicated suite solutions. 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. Two-factor authentication is required for access to cages and perimeter facility doors. The facility is equipped with raised floors, multiple UPS units for A/B-style redundant power delivery, generator, pre-action dry-pipe fire suppression, and an independent HVAC system with redundant air handlers. The MSP250 data center is part of a multi-tenant building at 250 Marquette Avenue South in Minneapolis, Minnesota. In tandem with building management, this facility provides 24/7 physical security, including security cameras, individually locking cabinets and cages, card key access, and on-site security guards.

### MSP511 Data Center Infrastructure

#### *Cologix*

Atomic Data utilizes Cologix as a colocation and network service provider for the MSP511 data center. 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 that 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 24/7 and monitored by security cameras. Cologix provides security at the suite, room, and rack level, ensuring no unauthorized access is permitted.

Atomic Data uses MSP511 to enhance services already available in the MSP market and add on to existing 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.

## **Third-Party Organizations and Facilities (Continued)**

### **MSP7700 and DFW400 Data Center Infrastructure**

#### *DataBank*

Atomic Data utilizes DataBank as a subservice provider for the MSP7700 and DFW400 data center facilities.

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 provides infrastructure protection to its colocation customers through use of a secure data center, with environmental conditions monitoring, failover capabilities, and 24-hour availability of its personnel to respond to customer inquiries.

DataBank offers carrier-class facilities designed to meet industry standards. Multiple high-speed fiber entrances to their facilities and redundant cooling and power systems are standard.

DataBank offers suites, cages, and full or partial cabinet options to meet customer needs. Support services and equipment are available on an "as needed" basis, allowing customers to outsource only the services they really need.

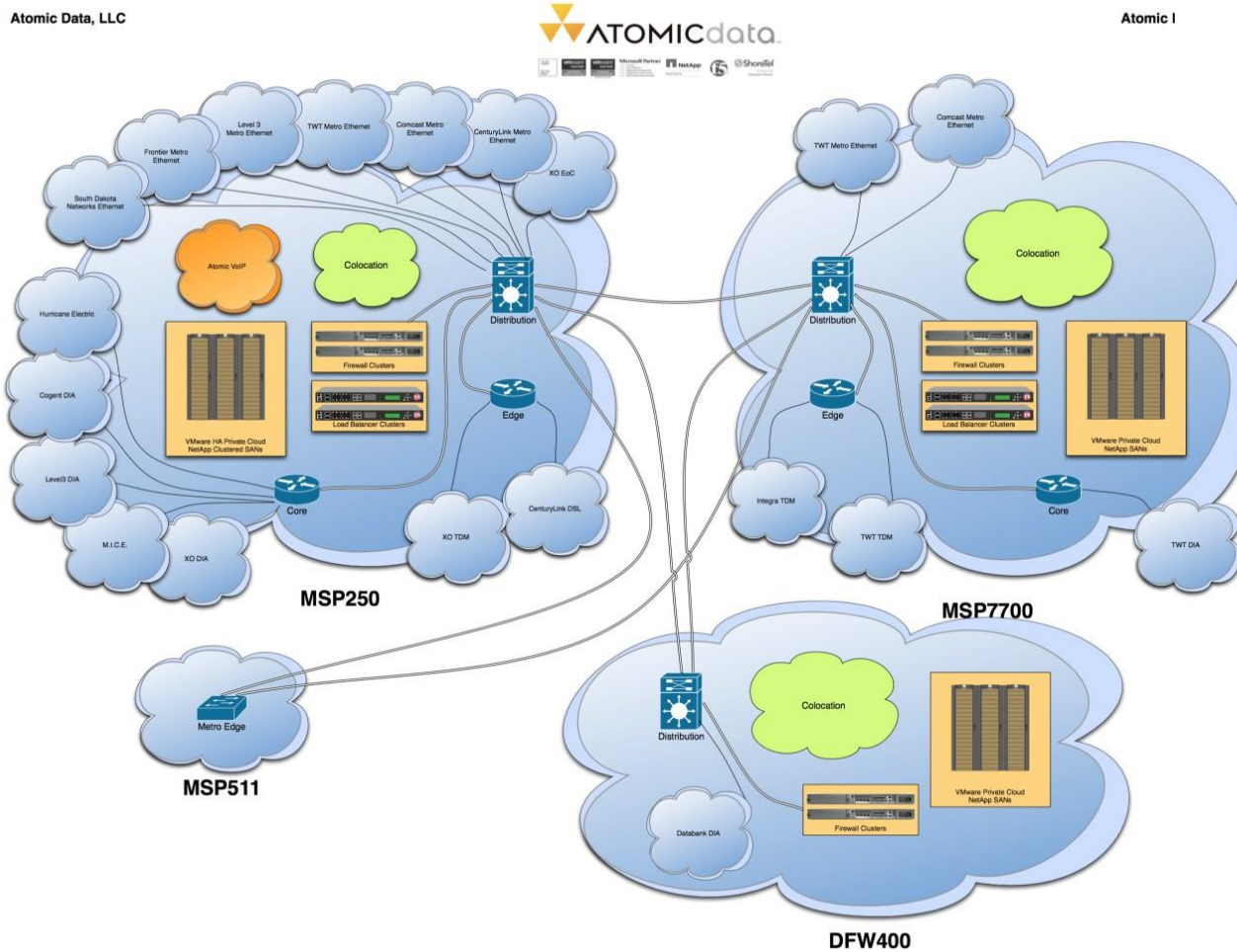
Atomic Data utilizes dedicated cages at this facility, extending its standard access control, environmental monitoring, and video surveillance infrastructures to facilitate best-of-class products and services. Access to cages requires two-factor authentication independent from DataBank and controlled by the same system used at MSP250. Camera recording provides close-in recording throughout both cages. Independent environmental probes are monitored 24/7 by the NOC. Customers 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.

DataBank operates multiple 24/7/365 commercial data centers throughout the United States. Atomic Data utilizes space within two of these facilities: 7700 France Avenue South, Edina, Minnesota, and 400 South Akard Street, Dallas, Texas. Both of these data centers are part of multi-tenant buildings.



# Atomic Data Network Overview

This is a high-level view of the services provided by Atomic Data:



Rev: 2016.03.25.1

## Atomic Data Security Controls

### Overview of the Control Environment

Atomic Data, LLC organizes its control environment around three general principles of control: human, physical, and logical. By identifying and controlling risk according to the best practices of the professional disciplines falling within each principle, the internal control system is able to comprehensively meet and exceed the applicable criteria of common audit and attestation standards, including the Trust Service Principles of Security, Confidentiality, and Availability common to the SOC 2 and SOC 3 reporting frameworks. Because of the relationships maintained with its subservice organizations, Atomic Data is able to implement complementary controls that normalize each independent facility toward a set of common expectations.

### Organizing Control Principles

Atomic Data identified the organizing principles of human, physical, and logical control as a natural result of the principles of role separation. While these areas do overlap, pragmatically, this method provides clear enough lines to promote the intuitive understanding of the system of internal control by the widest range of system members and allow for targeted application of relevant professional expertise.

#### Human

Human controls encompass a class of internal controls that aim to provide assurance that personnel acting within and in proximity to the control environment are properly identified, vetted, and authorized, from the time they first make contact with Atomic Data until after the association has ended.

For Atomic Data personnel, operating policies and procedures stress the importance of maintaining the confidentiality, security, and availability of customer data and services. These policies also require disclosure by an employee of relationships that could impair the employee's ability to act in the best interests of Atomic Data or otherwise constitute a conflict of interest. Atomic Data's policy is that all information obtained from Atomic Data-owned systems or stored on Atomic Data-owned equipment remains the property of Atomic Data or the originating customer. Employees do not have any privacy or proprietary interest in such information. Common understanding of these principles is ensured through new employee orientation training and by requiring existing employees to sign a confidentiality and nondisclosure agreement on an annual basis. This is also reinforced through regularly scheduled security awareness training.

#### Physical

Physical controls aim to ensure the integrity of the physical environments involved in generating the service provided by Atomic Data. At Atomic Data's offices, these protections include 24-hour video surveillance and recording, proximity-card controlled perimeter doorways, glass-break detection, and punch-code-secured interior doorways, which limit access to key storage areas to appropriate personnel. At the data centers, Atomic Data implements best-practice controls and policies that can function standalone at sites where it is in sole control and as a complement to the controls of a subservice provider 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 customers, comprehensive monitoring of internal and external environmental conditions, and extensive video surveillance.

## **Atomic Data Security Controls (Continued)**

### **Logical**

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 Atomic Login Account (ALA), which is required to gain access to any privileged network within the office or 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.

### **Control as Applied to the Operating Environment and Subservice Organizations**

Atomic Data ensures the security, confidentiality, and availability of customer and Company information at its networks and data centers through the appropriate, predictable application of all three principles. Effective control at locations where data is stored necessitates a strong, collaborative relationship with the provider. Thus, the relationship between Atomic Data and any of its subservice organizations is necessarily collaborative so Atomic Data is able to independently verify the operational readiness of each facility.

### **Control Model as Applied to the General Environment**

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 24/7 by the NOC and Service Desk, 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, the internal and customer service availability through intelligent application checks, and televised and automatic weather reporting for the local area and for the specific geographic locations of customer 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.

### **MSP250 Data Center – Atomic Data**

#### *Building and Perimeter*

This facility maintains high security standards for building access and perimeter monitoring. All inter-building area access is monitored and enforced by proximity card key access. Cameras are located at the entrances, around the data center suite, and in other key locations within the facility. The cameras are digital and operate 24/7. The facility provides, through its contractor, additional 24/7 monitoring for:

- Illegal entry at windows or doors
- Glass breakage
- Fire alarms

All access information and video surveillance is logged and available to customers for review upon request. The building is patrolled by on-site security personnel 24/7.

## **Atomic Data Security Controls (Continued)**

### *Environmental*

The facility space is heating, cooling, and humidity controlled via a commercial system developed for rooms containing electrical equipment. Failures in the HVAC system are monitored by the NOC, which operates on a 24/7 basis. If an alarm is received, processes are in place within the NOC to send notification to the appropriate person. All air handlers have drip pans in case of a leak. If water is detected in the drip pan, an alarm is sent. If the room temperature in the colocation space reaches or exceeds 75 degrees, an alarm is sent. In addition, the chilled water infrastructure is monitored for anomalies to aid in early detection of temperature fluctuation. Maintenance of these systems is performed on a quarterly basis.

### *Fire Protection*

The facility utilizes very early smoke detection alarms. Fire suppression occurs via a dry pipe, pre-action-based sprinkler system. The pipes are activated only if two sensors detect smoke in the facility. Water is released only if a specific sprinkler head is triggered because of heat. The colocation space is divided into several pre-action zones. Handheld fire extinguishers are located throughout facility spaces and maintained on a regular basis.

### *Power*

The facility includes two independent UPS systems and a generator system sufficient to run all of the facility's critical loads should utility power be interrupted. All power circuits supporting colocation equipment are connected to the UPS and generator. The facility provides protected, UPS-diverse circuits for customers that require redundant power to the rack or continuous power during a transition from utility to emergency power. The generator system is large enough to provide power to all hardware, lights, access systems, and HVAC in the case of a utility power outage. The facility maintains enough diesel fuel to operate for a minimum of seven days. This operational period can be extended depending on the load on the generator and the availability of fuel. The generator is run-tested monthly, and overall system maintenance is completed on an annual basis.

## **MSP7700 Data Center – DataBank**

### *Building and Perimeter*

The physical security of the building in which DataBank resides is monitored by a third-party security provider 24/7. Third-party personnel perform daily patrols of the facility and document incidents in a daily log. The DataBank suite is monitored on a daily basis by the DataBank Operations Manager to identify any suspicious activity of the security access system. All results of monitoring are documented within a daily log. Facility security personnel monitor the surveillance cameras 24/7. Digital surveillance cameras record access to and throughout the facility common areas. The records are stored for a period of 90 days. A security access system is utilized to restrict access to the data center facility. The door to the data center is restricted via a biometric hand geometry reader and PIN code. In addition, the data center can be accessed only through a two-door mantrap. The first door leading to the colocation room requires a biometric scan, while a second door requires a proximity key that may be used only when the first door is secured. The security access system logs forced door entries. A forced door entry generates an audible alarm throughout the facility.

## Atomic Data Security Controls (Continued)

### *Environmental*

Environmental conditions are monitored by both DataBank and building management. Building management monitors the building's chilled water loop, smoke alarms, and fire suppression systems, while Databank monitors air-handling units, water detection, air temperature, humidity levels, and as its own dedicated chilled water loop. Notifications are sent to building management and DataBank personnel in the event that predefined thresholds are exceeded. Environmental conditions within the DataBank data center are monitored using a software monitoring tool. DataBank personnel are notified whenever environmental conditions exceed predefined thresholds. Multiple air handlers, connected to redundant cooling towers, redundant cooling loops, and heat exchange systems, are in place to maintain environmental settings in the data center and provide failover capabilities in the event of a hardware outage. The building environmental monitoring system is configured to monitor the cooling towers, chilled water loops, and heat exchange systems. Alerts are configured on predefined temperature thresholds to notify building management and DataBank personnel. DataBank utilizes an environmental monitoring system to systematically monitor the data center's environmental conditions. Personnel are notified via email and on-call paging when levels exceed predefined minimum and maximum thresholds.

### *Fire Protection*

The data center facility is protected by fire detection and suppression controls that include the following: fire alarms, two-stage pre-action dry pipe sprinkler systems, automated FM200 extinguisher system, handheld fire extinguishers, and smoke detectors. Systems and equipment are maintained within the data center. There are water detection devices and smoke detectors located beneath raised floors and within the air handlers.

### *Power*

- DataBank ensures environmentally protected hosting environments through the use of redundant utilities and redundant generator systems implemented in a failover architecture. DataBank utilizes automated switch gear to feed three UPS systems to provide uninterrupted and redundant power to the data center floor, where colocation equipment resides.
- Preventative maintenance on the UPS systems and supporting battery subsystems is performed as follows:
  - Check performance logs daily.
  - Check batteries' electrolyte level and cases weekly.
  - Change air filters quarterly.
  - Check light bulbs and LEDs semiannually.
  - Check major connections every five years.
  - Perform infrared (IR) scans every six months.
- Two 2.1-megawatt diesel generators are in place to provide power to the facility in the event of a power outage. Internal generator tests are conducted weekly to verify the generators are in proper working order.

## Atomic Data Security Controls (Continued)

### DFW400 Data Center - DataBank

#### *Location*

DataBank's Downtown Dallas facility is designed to meet the highest industry standards of the telecom and enterprise IT businesses. The facility's robust mechanical plant systems are completely scalable and designed to serve the entire building easily, even under 100% occupancy by the most demanding high-density tenants. The entire electrical system is built out to true (2N) redundancy, which ensures DataBank customers will have continuous operations even during a complete grid blackout. In addition, the property is over three acres, with full-perimeter fencing encompassing all facility parking, loading docks, and building entrances. The entire 150,000-square-foot facility is designed to include multilevel physical security, as well as have secure freight delivery and storage/staging areas:

- Downtown Dallas Business district
- Over 130,000 square feet of raised floor
- Property of over three acres of secured area
- Structure of hardened steel frame with concrete slabs and granite/limestone/marble facades
- High-wind concrete deck with waterproof membrane construction
- 4,000-pound capacity freight elevator and a secured, dock-high loading/staging area
- 250 parking spaces in a secure, access-controlled parking lot

#### *Redundancy*

In downtown Dallas, DataBank offers customers a Tier III+ facility capable of providing complete redundancy in power, cooling, and network infrastructure:

- Multi-MegaWatt utility feeding a (2N) redundant configuration with capacity of over 30MW
- 10 generators providing over 19MW power generation, with additional expansion available
- Facility is fed by seven 500-ton cooling towers with a redundant cooling and power design
- Dual-fed high-efficiency CRAC units
- 80,000-gallon reserve water cooling tank
- Diverse secure service provider entries
- Meet-Me-Room offering network-neutral fiber interconnection to 22 service providers

#### *Additional Controls Provided by Atomic Data*

Atomic Data provides additional levels of monitoring and control independent of DataBank. The Atomic Data NOC monitors Atomic Data-operated security cameras inside its secured areas, 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. All Atomic Data and customer equipment is secured within Atomic Data-owned cages, which are protected by a two-factor authentication system controlled exclusively by Atomic Data.