PROPRIETARY AND CONFIDENTIAL

Axcient

BACKUP SOLUTIONS SYSTEM

REPORT ON AXCIENT'S SYSTEM AND ORGANIZATION CONTROLS
RELEVANT TO SECURITY AND AVAILABILITY (SOC 2)

March 1, 2019 to May 31, 2019

Moss Adams LLP
14555 Dallas Parkway, Suite 300
Dallas, TX 75254
(972) 458-2296

Table of Contents

I. INDEPENDENT SERVICE AUDITOR'S REPORT

eFolder, Inc. dba Axcient
707 17th Street, Suite 3900
Denver, CO 80202

To the Management of eFolder, Inc. dba Axcient:

Scope

We have examined Axcient's accompanying description of its Backup Solutions System in Section III titled "Axcient's Description of Its Backup Solutions System" throughout the period March 1, 2019 to May 31, 2019 (description) based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period March 1, 2019 to May 31, 2019, to provide reasonable assurance that Axcient's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Axcient uses subservice organizations Amazon Web Services, Equinix, Inc., Zayo Group, LLC Colocation Services, TeraGo Networks, Inc., and Flexential, Inc. for data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Axcient, to achieve Axcient's service commitments and system requirements based on the applicable trust services criteria. The description presents Axcient's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Axcient'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 Axcient, to achieve Axcient's service commitments and system requirements based on the applicable trust services criteria. The description presents Axcient's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Axcient'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

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of the controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our qualified opinion.

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

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

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

Inherent Limitations

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

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of our tests are listed in Section IV of this report titled "Trust Services Category, Criteria, Related Controls, and Tests of Controls."

Basis for Qualified Opinion

Axcient, Inc. states in its description of its Backup Storage System that it has controls in place to ensure proper authorization of access and timely removal of access upon termination. However, as noted on pages 51-55 of the description of test of controls and the results thereof, controls related to access provisioning of new employees and contractors and deprovisioning of existing employees and contractors were not operating effectively through the period March 1, 2019 to May 31, 2019. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion:

- *CC 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.*
- *CC 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.*

Opinion

In our opinion, except for the possible effects of the matters giving rise to the modification, in all material respects:

- the description presents Axcient's Backup Solutions System that was designed and implemented throughout the period March 1, 2019 to May 31, 2019, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period March 1, 2019 to May 31, 2019 to provide reasonable assurance that Axcient's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Axcient's controls throughout that period.

- the controls stated in the description operated effectively throughout the period March 1, 2019 to May 31, 2019 to provide reasonable assurance that Axcient'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 Axcient's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Axcient, user entities of Axcient's Backup Solutions System during some or all of the period March 1, 2019 to May 31, 2019, business partners of Axcient subject to risks arising from interactions with the Backup Solutions System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Moss Adams LLP

Denver, Colorado
March 23, 2020

II. ASSERTION OF AXCIENT'S MANAGEMENT

We have prepared the accompanying description of Axcient's Backup Solutions System in Section III titled "Axcient's Description of Its Backup Solutions System" throughout the period March 1, 2019 to May 31, 2019 (description) based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Backup Solutions System that may be useful when assessing the risks arising from interactions with Axcient's Backup Solutions System, particularly information about system controls that Axcient has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP Section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*).

Axcient uses subservice organizations Amazon Web Services, Equinix, Inc., Zayo Group, LLC Colocation Services, TeraGo Networks, Inc., and Flexential, Inc. for data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Axcient, to achieve Axcient's service commitments and system requirements based on the applicable trust services criteria. The description presents Axcient's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Axcient'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, along with controls at Axcient, to achieve Axcient's service commitments and system requirements based on the applicable trust services criteria. The description presents Axcient's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Axcient's controls.

We confirm, to the best of our knowledge and belief, that:

- the description presents Axcient's Backup Solutions System that was designed and implemented throughout the period March 1, 2019 to May 31, 2019, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period March 1, 2019 to May 31, 2019 to provide reasonable assurance that the Axcient service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout the period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Axcient's controls throughout that period.
- except for the effects of the matter described in the following paragraph, the controls stated in the description operated effectively throughout the period March 1, 2019 to May 31, 2019 to provide reasonable assurance that Axcient'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 Axcient's controls operated effectively throughout that period.

The description states on pages 51-55 that controls are in place to ensure proper authorization of access and timely removal of access upon termination. The failure to maintain sufficient documentation to support proper authorization of access and remove access timely upon termination may result in potential security risks introduced to the system. As a result, Axcient's service commitments and system requirements were not achieved based on the following trust services criteria:

- *CC 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.*
- *CC 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.*

III. AXCIENT'S DESCRIPTION OF ITS BACKUP SOLUTIONS SYSTEM

A. SERVICES PROVIDED

In 2002, Kevin Hoffman, George Welborn, Bill Gross, and John Williams founded eFolder to provide data protection services. After merging with Axcient in 2017, the combined organization became Axcient. The company subsequently chose to keep the Axcient name to move the company forward. Axcient's expansive mission today is to protect and empower business productivity. Axcient has evolved to become a leading provider of business and disaster recovery, business continuity, cloud-to-cloud backup, and file sync services, designed exclusively for the Managed Service Provider (MSP).

Originally formed as a local Value Added Reseller (VAR) serving the Atlanta market, Axcient's early years operating as an IT service provider fundamentally inspired the company's decision to exclusively serve MSP and VAR channel partners. The company's commitment to the IT channel made it possible for Axcient to develop best-in-class software and provide exceptional service to a growing community of more than 2,600 channel partners.

DESCRIPTION OF SERVICES PROVIDED

Axcient's suite of services and offerings are comprised of seven product lines, described below:

ANCHOR

Axcient Anchor ensures business data is always available via computers, servers, mobile devices, or the cloud. Anchor is an effective way for users to share and sync important data across multiple platforms, while keeping security a top priority. Teams can collaborate through Team Shares while minimizing the need for file transfer protocol (FTP) and virtual private network (VPN).

BDR CLOUD SERVICES

Backup & Disaster Recovery (BDR) enterprise-quality services ensure business continuity for mission critical servers and infrastructure. Third-party image-based backup software combined with the power of the Axcient cloud enables server virtualization anywhere in a disaster. BDR open cloud strategy allows partners to use preferred software brands with a unique, turn-key cloud environment. MSP-specific features keep costs low.

BUSINESS RECOVERY CLOUD (BRC)

BRC is a unique cloud technology that mirrors the company's entire IT infrastructure in the cloud and gives multiple recovery options from a single image-based snapshot of the system. Customers can recover data, failover servers, or virtualize the entire office with a click from a single Web-enabled interface.

CLOUDFINDER

CloudFinder ensures data stored in today's Software-as-a-Service (SaaS) applications is backed up, restorable, and protected. Safe Haven storage builds automated backup and total data protection. From a single interface, administrators can perform cross-service, instant full-text search, and rich filtering.

FUSION

Built from the ground up by Axcient using proprietary technology for today's virtual IT environments, Fusion consolidates critical non-production workloads into a single cloud platform, allowing elimination of redundant IT infrastructure, simplification and streamlining of operations, and running IT with the resilience and agility of the world's largest enterprises.

REPLIBIT

Axcient Replibit offers chain-free backup technology and offsite vaulting in the customer's data center or in the Axcient Cloud, with either pre-built BDR appliances with FastFlash™ SSD storage technology or custom-built BDR options. Axcient Replibit is an end-to-end backup and disaster recovery platform, empowering MSPs to deliver profitable, globally-managed business continuity services.

B. PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Axcient designs its processes and procedures to meet its objectives for the Backup Solutions system. These objectives are based on the service commitments that Axcient makes to user entities, the laws and regulations that govern the provision of the system, and compliance with applicable laws and regulations, while meeting the needs of the customer base.

Security and availability commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, design documentation, as well as in the description of the system provided online. Security commitments are standardized and include the use of logical and physical access controls to limit access based on roles and permissions and use of encryption technologies to protect customer data in transit. Availability commitments are standardized and include the use of policies, procedures, and internal controls designed to identify and mitigate the potential threats to the achievement of availability commitments for the Backup Solutions system.

Axcient establishes operational requirements that support the achievement of security and availability commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Axcient's system policies and procedures, system design documentation, and contracts with customers.

C. COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The System used to provide the above software and services is comprised of the following components:

- Infrastructure (facilities, equipment, and networks)
- Software (systems, applications, and utilities)
- People (developers, operators, users, and managers)
- Procedures (automated and manual)
- Data (transaction streams, files, databases, and tables)

The following sections of this description define each of these five components comprising the system.

1. INFRASTRUCTURE

DATA CENTERS

Axcient leverages a variety of data center solutions across four metro areas and three countries for storage and physical security needs. The in-scope Axcient services are physically hosted at the locations below:

Office Address	City	State	Country	Postal Code	Service Provider
1100 White Street Southwest	Atlanta	GA	USA	30310	Zayo Group, LLC
7202 S. Campus Drive	West Jordan	UT	USA	84084	Flexential, Inc.
200 Leckie Place	Kelowna	BC	Canada	V1Y7W7	TeraGo Networks, Inc.
Schepenbergweg 42	Amsterdam		Holland	1105	Equinix, Inc.

In addition to the above locations, Axcient also stores data using Amazon Web Services in the following Availability Zones:

- Ireland
- Oregon

The vendors for the above locations are responsible for all on-site staff (including data center engineers and security personnel), maintenance, monitoring, and operation of all power, cooling, and ancillary building systems and physical security. Data center services consist of physical and environmental protections including, but not limited to, the following:

- Physical security
- Heating, ventilation, and air conditioning (HVAC)
- Fire detection and fire suppression
- Power

2. SOFTWARE

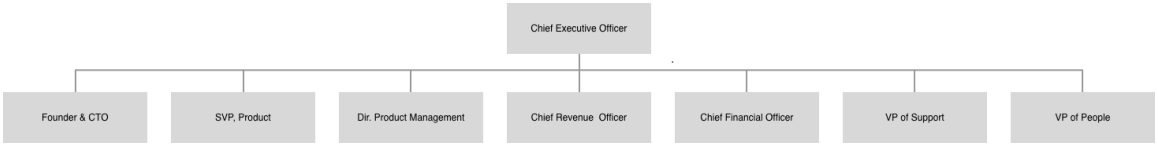
Axcient uses various monitoring solutions in the delivery of services. Enterprise monitoring tools and Axcient custom scripts are used to monitor critical system events. Upon the occurrence of an event, a ticket is created in Axcient's internal ticketing system automatically. Axcient's ticketing system is a web-based application and is the primary means of communication and method for tracking issues and requests for service.

The Axcient IT environment described herein consists of multiple applications, operating system platforms, and databases, shown in the table below:

Production Application	Business Function Description	Operating System Platform
Web Application and Database Servers	Application and database servers that support logical access systems	Linux
Firewall and Router Systems	Front-end firewalls protect the network perimeter based on rule-based access control lists	Palo Alto
VPN	Authentication for virtual private network, firewalls, and network devices	OpenVPN
Brivo	Badge Access System	N/A

3. PEOPLE

CORPORATE STRUCTURE



Axcient has employees across the world to support security and reliability for Axcient's customers. Services are provided by Axcient Cloud Engineering, Security, Support, Sales, Accounting, Product Development, Information Technology, and Executive Management teams. The majority of functions are centralized at the corporate level, though some of the staff and management work from remote locations or at specific central facilities within each in-scope country.

As Axcient grows over time, positions are added to provide additional management guidance, oversight, and structure. Organizational directory structures are available on Axcient's intranet to define clear lines of authority within the organization, and is updated frequently for new hires, promotions, or departures.

The Executive Management team meets regularly and is composed of a cross-functional group of executives to prevent domination by only one or two individuals. The Executive Management team addresses such topics as emerging trends, potential risks to the organization, and potential new strategies. Each year, the Executive Management team meets for formal business strategy and planning exercises, then multiple times weekly for tactical execution and strategic updates. These topics are then communicated to Axcient employees through the Leadership Team which is updated bi-weekly by the Executive Management Team, topical roundtables, all-hands meetings, etc. which are held at least quarterly, by the Executive Management team.

4. DATA

The data relevant to the in-scope systems include user access information, access lists, and physical and logical event logs and reports. Access to this data is limited to authorized personnel through logical access controls for the in-scope systems and treated as classified information by Axcient personnel.

Client data is managed, processed, and stored in accordance with relevant data protection and other regulations, with specific requirements formally established in customer contracts. This data is managed and stored in a range of database technologies. Only designated Axcient personnel have access to client data.

5. PROCESSES AND PROCEDURES

Procedures are used to achieve Axcient's system security and availability objectives in accordance with the defined policies. Axcient has an experienced Security team which is fully qualified to manage, design, implement, configure, and modify the infrastructure that has been deployed in a way that is consistent with the system security and availability policies.

PHYSICAL ACCESS

Physical security of the building is controlled through limited access points. Physical security of the suites in which Axcient operates is controlled through a badge reader, proximity cards, and access listings. Each non-remote employee is issued a proximity card which must be used to enter or exit areas containing Axcient data or hardware. Access to offline storage is restricted to authorized personnel only and vendor support personnel.

LOGICAL ACCESS

Procedures to restrict logical access to the Axcient system include identification and authentication of users through the use of complex passwords and multi-factor authentication (MFA). Provisioning requests or changes go through a formal approval process and are tracked in Axcient's internal ticketing system. Axcient's Security team maintains strict control over access to system configurations, super user functionality, master passwords, and security devices. Upon termination of an employee, all access is promptly removed according to established offboarding procedures.

MONITORING

In addition to procedures that allow for safely granting access to the system, Axcient has developed procedures to prevent unauthorized access to the system. Intrusion detection systems are in place on all systems and endpoints to detect any unauthorized access, changes, or abnormal behavior. Should there be an access violation or intrusion, Axcient has developed an incident response plan and all incidents and non-compliance with the security and availability policy are tracked in the Axcient internal ticketing system.

CHANGE MANAGEMENT

Documented IT change management policies and procedures are in place to guide personnel in standard change control processes for configuration management and maintenance activities to applications and infrastructure, with emphasis on change approval and communication requirements. For each proposed change, a ticket is opened for approval and assigned to the appropriate technical resource. After completing and passing relevant testing requirements, the change is then queued up for release during scheduled release windows. Downtime estimates incurred for major changes are communicated to relevant internal and external users via email prior to release deployment.

TRAINING

New personnel are required to undergo orientation training and existing personnel are required to complete annual refresher training course(s) on the above topics to ensure all employees are aware of relevant policies and procedures.

D. RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

1. CONTROL ENVIRONMENT

The control environment at Axcient is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the board of directors and operations management.

INTEGRITY AND ETHICAL VALUES

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Axcient's control environment, affecting the design, administration, and monitoring of other components.

Integrity and ethical behavior are the product of Axcient's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of Axcient's values and behavioral standards to personnel through policy statements and codes of conduct and by example. Specific control activities that Axcient has implemented in this area are described below:

- Organizational policy statements and codes of conduct are documented and communicate entity values and behavioral standards to personnel.
- The employee policy and procedures manual contains organizational policy statements and codes of conduct to which employees are required to adhere.

- Employees are required to sign an acknowledgement form indicating that they were given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- Employees are required to sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- Background checks are performed for employee candidates as a component of the hiring process (subject to local laws).

COMMITMENT TO COMPETENCE

Axcient's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Skills testing is utilized during the hiring process to qualify the skills of personnel for certain positions.
- Management has developed a security awareness training program to maintain the skill level of personnel regarding security best practices.

AUDIT COMMITTEE OVERSIGHT

Axcient's control consciousness is influenced by their Audit Committee, being controlled by the managing private equity firm's Board of Directors. Attributes include the Audit Committee's independence from management, the experience and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management, and its interaction with internal and external auditors.

Specific control activities that Axcient has implemented in this area are described below:

- An Audit Committee is in place to oversee management activities.
- An Audit Committee is in place to monitor management's compliance with the entity's objectives and performs continuous monitoring on key objectives and business processes.
- Independent external auditors conduct an annual audit of Axcient's financial transactions and statements, which is reported to and reviewed by the Audit Committee and Board of Directors.

ORGANIZATIONAL STRUCTURE AND ASSIGNMENT OF AUTHORITY AND RESPONSIBILITY

Axcient's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Axcient's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and lines of reporting. Axcient has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Axcient's assignment of authority and responsibility includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. In addition, it includes policies and communications directed at ensuring that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that Axcient has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority, responsibility, and lines of reporting to personnel. The organizational charts are communicated to employees.
- Organizational and departmental structures are used to help ensure a clear segregation of duties throughout the organization.
- Managers are responsible for encouraging training and development so that personnel continue to qualify for their functional responsibilities.

2. RISK ASSESSMENT PROCESS

Management is responsible for identifying the risks that threaten achievement of the applicable trust services criteria stated in the management's description of the organization's systems. Management has implemented a process for identifying relevant risks. This process includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding about actions to address them. However, because the applicable trust services criteria relate to risk that controls seek to mitigate, management thoughtfully identified control activities when designing, implementing, and documenting their system.

RISK IDENTIFICATION

Axcient has considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable services to its user entities. Management and operational teams meet on a regular basis to identify and review risks to the system. Management considers risks that can arise from both external and internal factors including:

EXTERNAL FACTORS

- Technological developments that could affect the nature and timing of research and development
- Changing customer needs or expectations that could affect services provided and customer service
- Competition that could alter marketing or services activities
- New legislation and regulation that could force changes in operating policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems and highlight the need for contingency planning
- Economic changes that could have an impact on decisions related to financing, capital expenditures, and expansion

INTERNAL FACTORS

- A disruption in information systems processing that could adversely affect the entity's operations
- The quality of personnel hired and methods of training and motivation that could influence the level of control consciousness within the entity
- A change in management responsibilities that could affect the way certain controls are implemented
- The nature of the entity's activities, and employee accessibility to assets, that could contribute to misappropriation of resources

The Axcient risk assessment process focuses on supporting management decisions and responding to potential threats by assessing risks and identifying important decision factors. Axcient executive management oversees risk management ownership and accountability. Senior management from different operational areas is involved in the risk identification process. Management identifies elements of business risk, including threats, vulnerabilities, safeguards, and the likelihood of a threat, to determine the actions to be taken.

RISK FACTORS

Management considers risks that can arise from both external and internal factors including the following:

EXTERNAL FACTORS

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

INTERNAL FACTORS

- Significant changes in policies, processes, or personnel
- Types of fraud
- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired and methods of training utilized
- Changes in management responsibilities

RISK ANALYSIS

Risk analysis is an essential process to the entity's success. It includes identification of key business processes where potential exposures of some consequence exist. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring, and identification of the control activities necessary to mitigate the risk. Management has identified these control activities and documented them in the Trust Services Criteria and Related Control Activities section below.

INTEGRATION WITH RISK ASSESSMENT

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security and availability criteria.

3. INFORMATION AND COMMUNICATION SYSTEMS

Axcient utilizes both formal and informal methods for corporate-wide communication. Upper management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to an appropriate higher level within the organization.

4. MONITORING CONTROLS

Management monitors controls to consider whether they are operating as intended and that the controls are modified for changes in conditions. Axcient's management performs monitoring activities to continuously assess the quality of internal control over time. Axcient management is responsible for directing and controlling operations and for establishing, communicating, and monitoring control activities and procedures. Axcient's management places emphasis on maintaining sound internal controls, as well as, ensuring integrity and ethical values to Axcient personnel.

ONGOING MONITORING

Axcient uses multiple methods to proactively monitor critical systems related to physical and logical security. With respect to security and access control, Axcient's Security personnel log and monitor access events via a suite of access-control software platforms to provide comprehensive reporting and alerting for all critical systems and endpoints.

INTERNAL AND EXTERNAL AUDITING

Axcient supports many customer entities in their efforts to meet the regulatory demands of their industry or governing agency. Axcient has assisted user entities in successfully meeting the requirements of many certifications and regulatory demands, including:

- Financial examinations
- Annual SOC 1/SOC 2 examinations on data centers

EVALUATING AND COMMUNICATING DEFICIENCIES

Identified performance deficiencies reported by a customer, third-party assessments, or the service organization's monitoring activities are logged into an incident management system for investigation and resolution. Customer complaints and comments are logged and reviewed to identify improvements in daily operations.

5. CHANGES TO THE SYSTEM DURING THE PERIOD

During the examination period, Axcient migrated all data and operations from a data center in Santa Clara, California, to the data center in Salt Lake City, Utah. Axcient management has performed risk assessments and has obtained an individual SOC report for the Santa Clara, California facility to cover the period during which it was used for Axcient services and data.

E. TRUST SERVICES CRITERIA AND RELATED CONTROLS

Although the applicable trust services criteria, related controls, and management responses to deviations, if any, are presented in Section IV of this report titled "Trust Services Category, Criteria, Related Controls, and Tests of Controls", they are an integral part of Axcient's system description throughout the period March 1, 2019 to May 31, 2019.

F. COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

Axcient's controls related to the Backup Solutions System cover only a portion of overall internal control for each user entity of Axcient. It is not feasible for the criteria related to the Backup Solutions System to be achieved solely by Axcient. Therefore, each user entity's internal controls must be evaluated in conjunction with Axcient's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

	Complementary Subservice Organization Controls	Related Criteria	Subservice Organization(s)
1	The subservice organization has implemented appropriate environmental controls including those preventing unauthorized physical access to sensitive data and equipment.	**Criteria 6.4:** Logical and Physical Access Controls	• Amazon Web Services • Zayo Group, LLC • Flexential, Inc. • TeraGo Networks, Inc. • Equinix, Inc.
2	The subservice organization has implemented controls to monitor, and manage capacity in order to meet availability commitments.	**Criteria A1.1**: Additional Criteria for Availability	• Amazon Web Services • Zayo Group, LLC • Flexential, Inc. • TeraGo Networks, Inc. • Equinix, Inc.
3	The subservice organization has implemented controls to maintain, monitor, and test recovery procedures in order to meet availability commitments.	**Criteria A1.2:** Additional Criteria for Availability	• Amazon Web Services • Zayo Group, LLC • Flexential, Inc. • TeraGo Networks, Inc. • Equinix, Inc.

G. COMPLEMENTARY USER ENTITY CONTROLS

Axcient's Backup Solutions System was designed under the assumption that certain controls would be implemented by the user entities for whom it provides its Backup Solutions System. In these situations, the application of specific controls at these customer organizations is necessary to achieve certain control objectives included in this report.

This section describes additional controls that should be in operation at the customer organizations to complement the controls at Axcient. User auditors should consider whether the following controls have been placed in operation by the customers.

Each customer must evaluate its own internal control structure to determine if the identified customer controls are in place. Users are responsible for:

Complementary User Entity Controls	
1	Ensuring compliance with contractual requirements.
2	Ensuring that user organizations adopt strong operating system and application password management procedures, including using passwords that cannot be easily compromised and require to change on a regular basis.
3	Confirming of the compatibility of software not provided by Axcient.
4	Establishing procedures for developing, maintaining, and testing their own business continuity plans (BCP).
5	Notifying Axcient in advance of any equipment or other shipments they will be sending or receiving.
6	Transmission and receipt of information not provided by Axcient.
7	Approving the telecommunications infrastructure between itself and Axcient.
8	Ensuring access is appropriately granted, reviewed periodically, and revoked as necessary.

IV. TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

This SOC 2 Type 2 Report was prepared in accordance with the AICPA attestation standards, and has been performed to examine the suitability of the design and operating effectiveness of controls to meet the criteria for the Security and Availability categories set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) throughout the period March 1, 2019 through May 31, 2019.

The trust services category for the Security and Availability criteria and related controls specified by Axcient are presented in Section IV of this report.

Test procedures performed in connection with determining the operating effectiveness of controls detailed here in Section IV are described below:

Test Procedure		Description
INQUIRIES	➤	Inquiry of appropriate personnel and corroboration with management.
OBSERVATION	➤	Observation of the application, performance or existence of the control.
INSPECTION	➤	Inspection of documents and reports indicating performance of the control.
REPERFORMANCE	➤	Reperformance of the control.

APPLICABLE TRUST SERVICES CRITERIA RELEVANT TO SECURITY AND AVAILABILITY

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 1.1	The entity demonstrates a commitment to integrity and ethical values.	New employees and contractors acknowledge the employee handbook, which also includes the ethics policy, upon hire. The ethics policy in the employee handbook includes a clause that management reserves the right to take action to resolve any conflicts of interest or ethics violations, including termination of employment.	Inquired of the VP of People about the employee handbook noting that new employees and contractors acknowledged the employee handbook, which also included the ethics policy, upon hire. Also noted that the ethics policy in the employee handbook included a clause that management reserved the right to take action to resolve any conflicts of interest or ethics violations, including termination of employment.	No exceptions noted.
			Inspected the employee handbook noting that it included the ethics policy. Also noted that the ethics policy included a clause that management reserved the right to take action to resolve any conflicts of interest or ethics violations, including termination of employment.	No exceptions noted.
			Inspected acknowledgements for randomly selected new employees and contractors during the examination period noting that new employees acknowledged the employee handbook, which also included the ethics policy, upon hire.	No exceptions noted.
		Candidates undergo multiple levels of screening, which may include a background check for employees and contractors based in countries where background checks are performed, to assess qualifications for a position.	Inquired of the VP of People about candidate screening noting that candidates underwent multiple levels of screening, which may have included a background check for employees and contractors based in countries where background checks were performed, to assess qualifications for a position.	No exceptions noted.
			Inspected background checks and evidence of screening for randomly selected new employees and contractors during the examination period noting that candidates underwent multiple levels of screening, which may have included a background check for employees and contractors based in countries where background checks were performed, to assess qualifications for a position.	No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Employees and contractors are required to take HIPAA training upon hire and annually thereafter.	Inquired of the Security & Compliance Analyst about HIPAA Training noting that employees and contractors were required to take HIPAA training upon hire and annually thereafter.	No exceptions noted.
			Inspected HIPAA training records for randomly selected new employees and contractors during the examination period noting that employees and contractors were required to take HIPAA training upon hire.	No exceptions noted.
			Inspected HIPAA training records for randomly selected current employees and contractors during the examination period noting that employees and contractors were required to take HIPAA training annually.	No exceptions noted.
		Security awareness training is completed by new employees and contractors upon hire and by current employees and contractors on an annual basis.	Inquired of the Security & Compliance Analyst about security awareness training noting that security awareness training was completed by new employees and contractors upon hire and by current employees and contractors on an annual basis.	No exceptions noted.
			Inspected security awareness training records for randomly selected new employees and contractors during the examination period noting that security awareness training was completed by new employees and contractors upon hire.	No exceptions noted.
			Inspected security awareness training records for randomly selected current employees and contractors during the examination period noting that security awareness training was completed by current employees and contractors on an annual basis.	No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Axcient's policies and procedures are approved by management and accessible by employees on Axcient's common drive to which employees have access. Company policies are reviewed at least annually and updated as necessary by senior management.	Inquired of the Chief Information Security Officer about policies and procedures noting that Axcient's policies and procedures were approved by management and accessible by employees on Axcient's common drive to which employees had access. Also noted that Company policies were reviewed at least annually and updated as necessary by senior management.	No exceptions noted.
			Inspected Axcient's common drive users noting that Company policies and procedures were accessible by employees on Axcient's common drive to which employees had access.	No exceptions noted.
			Inspected the review date for Company policies and procedures noting that Axcient's policies and procedures were reviewed by management at least annually and updated as necessary by senior management.	No exceptions noted.
CC 1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Management reports environmental, compliance, regulatory, technological changes, internal controls, and control deficiencies to Axcient's Board of Directors through a quarterly deck presentation.	Inquired of the Chief Information Security Officer about Board of Directors meetings noting that management reported environmental, compliance, regulatory, technological changes, internal controls, and control deficiencies to Axcient's Board of Directors through a quarterly deck presentation.	No exceptions noted.
			Inspected the quarterly deck presentation slides during the examination period noting that management reported environmental, compliance, regulatory, technological changes, internal controls, and control deficiencies to Axcient's Board of Directors through a quarterly deck presentation.	No exceptions noted.
		The Board of Directors operates in an advisory capacity and is independent from management and operations.	Inquired of the President about the Board of Directors' operations noting that the Board of Directors operated in an advisory capacity and was independent from management and operations.	No exceptions noted.
			Inspected the Board of Directors' meeting invite and deck presentation slides during the examination period noting that the Board of Directors operated in an advisory capacity and was independent from management and operations.	No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Axcient has a defined organizational chart which establishes the structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and requirements as they relate to security and availability.	Inquired of the VP of People about the organizational structure noting that Axcient had a defined organizational chart which established the structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and requirements as they related to security and availability. Inspected the organization chart noting that Axcient had a defined organizational chart which established the structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and requirements as they related to security and availability.	No exceptions noted. No exceptions noted.
		Management reports environmental, compliance, regulatory, technological changes, internal controls, and control deficiencies to Axcient's Board of Directors through a quarterly deck presentation.	Inquired of the Chief Information Security Officer about Board of Directors meetings noting that management reported environmental, compliance, regulatory, technological changes, internal controls, and control deficiencies to Axcient's Board of Directors through a quarterly deck presentation. Inspected the quarterly deck presentation slides during the examination period noting that management reported environmental, compliance, regulatory, technological changes, internal controls, and control deficiencies to Axcient's Board of Directors through a quarterly deck presentation.	No exceptions noted. No exceptions noted.
		Each employee and contractor has a job description that contains employee responsibilities and requirements related to education, competencies, skills, and abilities.	Inquired of the VP of People about job descriptions noting that each employee and contractor had a job description that contained employee responsibilities and requirements related to education, competencies, skills, and abilities. Inspected job descriptions for randomly selected current employees and contractors during the examination period noting that each employee had a job description that contained employee responsibilities and requirements related to education, competencies, skills, and abilities.	No exceptions noted. No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Candidates undergo multiple levels of screening, which may include a background check for employees and contractors based in countries where background checks are performed, to assess qualifications for a position.	Inquired of the VP of People about candidate screening noting that candidates underwent multiple levels of screening, which may have included a background check for employees and contractors based in countries where background checks were performed, to assess qualifications for a position. Inspected background checks and evidence of screening for randomly selected new employees and contractors during the examination period noting that candidates underwent multiple levels of screening, which may have included a background check for employees and contractors based in countries where background checks were performed, to assess qualifications for a position.	No exceptions noted. No exceptions noted.
		Security awareness training is completed by new employees and contractors upon hire and by current employees and contractors on an annual basis.	Inquired of the Security & Compliance Analyst about security awareness training noting that security awareness training was completed by new employees and contractors upon hire and by current employees and contractors on an annual basis. Inspected security awareness training records for randomly selected new employees and contractors during the examination period noting that security awareness training was completed by new employees and contractors upon hire. Inspected security awareness training records for randomly selected current employees and contractors during the examination period noting that security awareness training was completed by current employees and contractors on an annual basis.	No exceptions noted. No exceptions noted. No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Employees and contractors are required to take HIPAA training upon hire and annually thereafter.	Inquired of the Security & Compliance Analyst about HIPAA Training noting that employees and contractors were required to take HIPAA training upon hire and annually thereafter.	No exceptions noted.
			Inspected HIPAA training records for randomly selected new employees and contractors during the examination period noting that employees and contractors were required to take HIPAA training upon hire.	No exceptions noted.
			Inspected HIPAA training records for randomly selected current employees and contractors during the examination period noting that employees and contractors were required to take HIPAA training annually.	No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Candidates undergo multiple levels of screening, which may include a background check for employees and contractors based in countries where background checks are performed, to assess qualifications for a position.	Inquired of the VP of People about candidate screening noting that candidates underwent multiple levels of screening, which may have included a background check for employees and contractors based in countries where background checks were performed, to assess qualifications for a position.	No exceptions noted.
			Inspected background checks and evidence of screening for randomly selected new employees and contractors during the examination period noting that candidates underwent multiple levels of screening, which may have included a background check for employees and contractors based in countries where background checks were performed, to assess qualifications for a position.	No exceptions noted.
		Security awareness training is completed by new employees and contractors upon hire and by current employees and contractors on an annual basis.	Inquired of the Security & Compliance Analyst about security awareness training noting that security awareness training was completed by new employees and contractors upon hire and by current employees and contractors on an annual basis.	No exceptions noted.
			Inspected security awareness training records for randomly selected new employees and contractors during the examination period noting that security awareness training was completed by new employees and contractors upon hire.	No exceptions noted.
			Inspected security awareness training records for randomly selected current employees and contractors during the examination period noting that security awareness training was completed by current employees and contractors on an annual basis.	No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Employees and contractors are required to take HIPAA training upon hire and annually thereafter.	Inquired of the Security & Compliance Analyst about HIPAA Training noting that employees and contractors were required to take HIPAA training upon hire and annually thereafter.	No exceptions noted.
			Inspected HIPAA training records for randomly selected new employees and contractors during the examination period noting that employees and contractors were required to take HIPAA training upon hire.	No exceptions noted.
			Inspected HIPAA training records for randomly selected current employees and contractors during the examination period noting that employees and contractors were required to take HIPAA training annually.	No exceptions noted.
		Each employee and contractor has a job description that contains employee responsibilities and requirements related to education, competencies, skills, and abilities.	Inquired of the VP of People about job descriptions noting that each employee and contractor had a job description that contained employee responsibilities and requirements related to education, competencies, skills, and abilities.	No exceptions noted.
			Inspected job descriptions for randomly selected current employees and contractors during the examination period noting that each employee had a job description that contained employee responsibilities and requirements related to education, competencies, skills, and abilities.	No exceptions noted.

CC 1.0 Control Environment				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		New employees and contractors acknowledge the employee handbook, which also includes the ethics policy, upon hire. The ethics policy in the employee handbook includes a clause that management reserves the right to take action to resolve any conflicts of interest or ethics violations, including termination of employment.	Inquired of the VP of People about the employee handbook noting that new employees and contractors acknowledged the employee handbook, which also included the ethics policy, upon hire. Also noted that the ethics policy in the employee handbook included a clause that management reserved the right to take action to resolve any conflicts of interest or ethics violations, including termination of employment.	No exceptions noted.
			Inspected the employee handbook noting that it included the ethics policy. Also noted that the ethics policy included a clause that management reserved the right to take action to resolve any conflicts of interest or ethics violations, including termination of employment.	No exceptions noted.
			Inspected acknowledgements for randomly selected new employees and contractors during the examination period noting that new employees acknowledged the employee handbook, which also included the ethics policy, upon hire.	No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Third-party service providers undergo an annual SOC 2 Type 2 examination related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Axcient's management performs a detailed review of SOC 2 Type 2 report to evaluate the scope, testing results, and complementary user entity controls.	Inquired of the Security & Compliance Analyst about third-party service providers annual review noting that third-party service providers underwent an annual SOC 2 Type 2 examination related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient's management performed a detailed review of SOC 2 Type 2 report to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the AWS SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (October 1, 2018 through March 31, 2019) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the Equinix, Inc. SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (November 1, 2017 through October 31, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
			Inspected the zColo SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service providers underwent an annual SOC 2 Type 2 examination (November 1, 2017 through October 31, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the TeraGo SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (February 1, 2018 through November 30, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the Flexential SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (April 1, 2018 through October 31, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Vulnerability testing is performed on servers weekly. Vulnerabilities are tracked in Jira until resolved.	Inquired of the Security & Compliance Analyst about vulnerability testing noting that vulnerability testing was performed on servers weekly. Also noted that high risk vulnerabilities were tracked in Jira until resolved. Inspected vulnerability scan logs and configurations for servers during the examination period noting that vulnerability testing was performed weekly on servers. Also noted that high risk vulnerabilities were tracked in Jira until resolved.	No exceptions noted. No exceptions noted.
		Major changes are approved in a peer review and by the product owner prior to completion of the sprint.	Inquired of the IT Manager about major changes to critical systems noting that major changes to critical systems were approved in a peer review and by the product owner prior to completion of the sprint. Inspected change tickets for randomly selected major changes to critical systems during the examination period noting that major changes to critical systems were approved in a peer review and by the product owner prior to completion of the sprint.	No exceptions noted. No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Employees and contractors are required to take HIPAA training upon hire and annually thereafter.	Inquired of the Security & Compliance Analyst about HIPAA Training noting that employees and contractors were required to take HIPAA training upon hire and annually thereafter.	No exceptions noted.
			Inspected HIPAA training records for randomly selected new employees and contractors during the examination period noting that employees and contractors were required to take HIPAA training upon hire.	No exceptions noted.
			Inspected HIPAA training records for randomly selected current employees and contractors during the examination period noting that employees and contractors were required to take HIPAA training annually.	No exceptions noted.
		Security awareness training is completed by new employees and contractors upon hire and by current employees and contractors on an annual basis.	Inquired of the Security & Compliance Analyst about security awareness training noting that security awareness training was completed by new employees and contractors upon hire and by current employees and contractors on an annual basis.	No exceptions noted.
			Inspected security awareness training records for randomly selected new employees and contractors during the examination period noting that security awareness training was completed by new employees and contractors upon hire.	No exceptions noted.
			Inspected security awareness training records for randomly selected current employees and contractors during the examination period noting that security awareness training was completed by current employees and contractors on an annual basis.	No exceptions noted.
		Employees and contractors are required to read and sign the Privilege Level Access Agreement (PLAA) and confidentiality agreements upon hire.	Inquired of the VP of People about PLAA and confidentiality agreements noting that employees and contractors were required to read and sign the PLAA and confidentiality agreements upon hire.	No exceptions noted.
			Inspected PLAAs and confidentiality agreements for randomly selected new employees and contractors during the examination period noting that employees and contractors were required to read and sign the PLAA and confidentiality agreements upon hire.	No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Planned service outages are communicated to internal users by email and external users through a client status page on the login page.	Inquired of the Director of Product Management about planned service outages noting that planned service outages were communicated to internal users by email and external users through a client status page on the login page.	No exceptions noted.
			Inspected planned service outage emails for randomly selected service outages during the examination period noting that planned service outages were communicated to internal users by email.	No exceptions noted.
			Observed the login page noting that a client status page was accessible and reported planned service outages to external users.	No exceptions noted.
		Policy and procedure documents are published for significant processes, including the process and responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints. They are available on Axcient's common drive to employees and externally on Axcient's Terms of Service on the company website.	Inquired of the Chief Information Security Officer about internal policies and procedures noting that policy and procedure documents were published for significant processes, including the process and responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints. Also noted that they were available on Axcient's common drive to employees and externally within Axcient's Terms of Service on the company website.	No exceptions noted.
			Inspected the policy and procedure document noting that policy and procedure documents were published for significant processes, including the process and responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints.	No exceptions noted.
			Inspected Axcient's common drive and Axcient's Terms of Service on the company website noting that policies and procedure documents were available on Axcient's common drive to employees and externally within Axcient's Terms of Service on the company website.	No exceptions noted.

CC 2.0 Communication and Information				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Axcient's security commitments regarding the system are included in the master services agreement (MSA).	Inquired of the Senior Manager of Operations about security commitments noting that Axcient's security commitments regarding the system were included in the MSA. Inspected signed MSAs for randomly selected new clients during the examination period noting that Axcient's security commitments regarding the system were included in the MSAs.	No exceptions noted. No exceptions noted.
		Axcient's privacy policy is posted on the company's website and clients are notified when substantial updates are made.	Inquired of the Chief Information Security Officer about Axcient's privacy policy noting that Axcient's privacy policy was posted on the company's website and clients were notified when substantial updates were made. Also noted that no substantial updates were made during the examination period. Inspected the company's website noting that Axcient's privacy policy was posted on the company's website.	No exceptions noted. No exceptions noted.
		Planned service outages are communicated to internal users by email and external users through a client status page on the login page.	Inquired of the Director of Product Management about planned service outages noting that planned service outages were communicated to internal users by email and external users through a client status page on the login page. Inspected planned service outage emails for randomly selected service outages during the examination period noting that planned service outages were communicated to internal users by email. Observed the login page noting that a client status page was accessible and reported planned service outages to external users.	No exceptions noted. No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Management performs a risk assessment to identify threats to the system or environment, and communicates the risks to the Board of Directors for review.	Inquired of the Chief Information Security Officer about the risk assessment process noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review. Inspected the risk assessment performed during the examination period noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review.	No exceptions noted. No exceptions noted.
		Vulnerability testing is performed on servers weekly. Vulnerabilities are tracked in Jira until resolved.	Inquired of the Security & Compliance Analyst about vulnerability testing noting that vulnerability testing was performed on servers weekly. Also noted that high risk vulnerabilities were tracked in Jira until resolved. Inspected vulnerability scan logs and configurations for servers during the examination period noting that vulnerability testing was performed weekly on servers. Also noted that high risk vulnerabilities were tracked in Jira until resolved.	No exceptions noted. No exceptions noted.
		A security evaluation is completed for new third-party vendors whose services are integrated with Axcient.	Inquired of the IT Administrator about security evaluations noting that a security evaluation was completed for new third-party vendors whose services would be integrated with Axcient. Also noted there were no new third-party vendors during the examination period.	No exceptions noted.
		Penetration testing is performed annually by a third party and management is notified of suspicious activities. Management reviews critical risks to determine necessary action.	Inquired of the Security & Compliance Analyst about penetration testing noting that penetration testing was performed annually by a third party and management was notified of suspicious activities. Also noted that management reviewed critical risks to determine necessary action. Inspected penetration test reports during the examination period noting that penetration testing was performed annually by a third party and management was notified of suspicious activities. Also noted that there were no critical risks identified during the examination period.	No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Axcient maintains an incident response plan that documents a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure client data is secure.	Inquired of the Chief Information Security Officer about the incident response process noting that Axcient maintained an Incident Response Plan that documented a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure client data was secure. Inspected the Incident Response Plan noting that Axcient maintained an Incident Response Plan that documented a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure the client data was secure.	No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Management performs a risk assessment to identify threats to the system or environment, and communicates the risks to the Board of Directors for review.	Inquired of the Chief Information Security Officer about the risk assessment process noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review. Inspected the risk assessment performed during the examination period noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review.	No exceptions noted. No exceptions noted.
		A security evaluation is completed for new third-party vendors whose services are integrated with Axcient.	Inquired of the IT Administrator about security evaluations noting that a security evaluation was completed for new third-party vendors whose services would be integrated with Axcient. Also noted there were no new third-party vendors during the examination period.	No exceptions noted.
		Penetration testing is performed annually by a third party and management is notified of suspicious activities. Management reviews critical risks to determine necessary action.	Inquired of the Security & Compliance Analyst about penetration testing noting that penetration testing was performed annually by a third party and management was notified of suspicious activities. Also noted that management reviewed critical risks to determine necessary action. Inspected penetration test reports during the examination period noting that penetration testing was performed annually by a third party and management was notified of suspicious activities. Also noted that there were no critical risks identified during the examination period.	No exceptions noted. No exceptions noted.
		Axcient maintains an incident response plan that documents a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure client data is secure.	Inquired of the Chief Information Security Officer about the incident response process noting that Axcient maintained an Incident Response Plan that documented a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure client data was secure. Inspected the Incident Response Plan noting that Axcient maintained an Incident Response Plan that documented a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure the client data was secure.	No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Candidates undergo multiple levels of screening, which may include a background check for employees and contractors based in countries where background checks are performed, to assess qualifications for a position.	Inquired of the VP of People about candidate screening noting that candidates underwent multiple levels of screening, which may have included a background check for employees and contractors based in countries where background checks were performed, to assess qualifications for a position. Inspected background checks and evidence of screening for randomly selected new employees and contractors during the examination period noting that candidates underwent multiple levels of screening, which may have included a background check for employees and contractors based in countries where background checks were performed, to assess qualifications for a position.	No exceptions noted. No exceptions noted.
		Management performs a risk assessment to identify threats to the system or environment, and communicates the risks to the Board of Directors for review.	Inquired of the Chief Information Security Officer about the risk assessment process noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review. Inspected the risk assessment performed during the examination period noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review.	No exceptions noted. No exceptions noted.
		A security evaluation is completed for new third-party vendors whose services are integrated with Axcient.	Inquired of the IT Administrator about security evaluations noting that a security evaluation was completed for new third-party vendors whose services would be integrated with Axcient. Also noted there were no new third-party vendors during the examination period.	No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Management performs a risk assessment to identify threats to the system or environment, and communicates the risks to the Board of Directors for review.	Inquired of the Chief Information Security Officer about the risk assessment process noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review. Inspected the risk assessment performed during the examination period noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review.	No exceptions noted. No exceptions noted.
		Vulnerability testing is performed on servers weekly. Vulnerabilities are tracked in Jira until resolved.	Inquired of the Security & Compliance Analyst about vulnerability testing noting that vulnerability testing was performed on servers weekly. Also noted that high risk vulnerabilities were tracked in Jira until resolved. Inspected vulnerability scan logs and configurations for servers during the examination period noting that vulnerability testing was performed weekly on servers. Also noted that high risk vulnerabilities were tracked in Jira until resolved.	No exceptions noted. No exceptions noted.
		A security evaluation is completed for new third-party vendors whose services are integrated with Axcient.	Inquired of the IT Administrator about security evaluations noting that a security evaluation was completed for new third-party vendors whose services would be integrated with Axcient. Also noted there were no new third-party vendors during the examination period.	No exceptions noted.
		Penetration testing is performed annually by a third party and management is notified of suspicious activities. Management reviews critical risks to determine necessary action.	Inquired of the Security & Compliance Analyst about penetration testing noting that penetration testing was performed annually by a third party and management was notified of suspicious activities. Also noted that management reviewed critical risks to determine necessary action. Inspected penetration test reports during the examination period noting that penetration testing was performed annually by a third party and management was notified of suspicious activities. Also noted that there were no critical risks identified during the examination period.	No exceptions noted. No exceptions noted.

CC 3.0 Risk Assessment				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Management reports environmental, compliance, regulatory, technological changes, internal controls, and control deficiencies to Axcient's Board of Directors through a quarterly deck presentation.	Inquired of the Chief Information Security Officer about Board of Directors meetings noting that management reported environmental, compliance, regulatory, technological changes, internal controls, and control deficiencies to Axcient's Board of Directors through a quarterly deck presentation. Inspected the quarterly deck presentation slides during the examination period noting that management reported environmental, compliance, regulatory, technological changes, internal controls, and control deficiencies to Axcient's Board of Directors through a quarterly deck presentation.	No exceptions noted. No exceptions noted.

CC 4.0 Monitoring Activities				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Security incidents are tracked in Jira, rated by severity, with P0/P1's being resolved within 72 hours.	Inquired of the Chief Information Security Officer about incident tracking noting that security incidents were tracked in Jira, rated by severity, with P0/P1's being resolved within 72 hours. Also noted that there were no P0/P1 incidents identified during the examination period.	No exceptions noted.
		Vulnerability testing is performed on servers weekly. Vulnerabilities are tracked in Jira until resolved.	Inquired of the Security & Compliance Analyst about vulnerability testing noting that vulnerability testing was performed on servers weekly. Also noted that high risk vulnerabilities were tracked in Jira until resolved. Inspected vulnerability scan logs and configurations for servers during the examination period noting that vulnerability testing was performed weekly on servers. Also noted that high risk vulnerabilities were tracked in Jira until resolved.	No exceptions noted. No exceptions noted.
		Penetration testing is performed annually by a third party and management is notified of suspicious activities. Management reviews critical risks to determine necessary action.	Inquired of the Security & Compliance Analyst about penetration testing noting that penetration testing was performed annually by a third party and management was notified of suspicious activities. Also noted that management reviewed critical risks to determine necessary action. Inspected penetration test reports during the examination period noting that penetration testing was performed annually by a third party and management was notified of suspicious activities. Also noted that there were no critical risks identified during the examination period.	No exceptions noted. No exceptions noted.
		A security evaluation is completed for new third-party vendors whose services are integrated with Axcient.	Inquired of the IT Administrator about security evaluations noting that a security evaluation was completed for new third-party vendors whose services would be integrated with Axcient. Also noted there were no new third-party vendors during the examination period.	No exceptions noted.

CC 4.0 Monitoring Activities				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Management performs a risk assessment to identify threats to the system or environment, and communicates the risks to the Board of Directors for review.	Inquired of the Chief Information Security Officer about the risk assessment process noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review. Inspected the risk assessment performed during the examination period noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review.	No exceptions noted. No exceptions noted.
		Axcient maintains an incident response plan that documents a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure client data is secure.	Inquired of the Chief Information Security Officer about the incident response process noting that Axcient maintained an Incident Response Plan that documented a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure client data was secure. Inspected the Incident Response Plan noting that Axcient maintained an Incident Response Plan that documented a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure the client data was secure.	No exceptions noted. No exceptions noted.
		Security incidents are tracked in Jira, rated by severity, with P0/P1's being resolved within 72 hours.	Inquired of the Chief Information Security Officer about incident tracking noting that security incidents were tracked in Jira, rated by severity, with P0/P1's being resolved within 72 hours. Also noted that there were no P0/P1 incidents identified during the examination period.	No exceptions noted.
		Management reports environmental, compliance, regulatory, technological changes, internal controls, and control deficiencies to Axcient's Board of Directors through a quarterly deck presentation.	Inquired of the Chief Information Security Officer about Board of Directors meetings noting that management reported environmental, compliance, regulatory, technological changes, internal controls, and control deficiencies to Axcient's Board of Directors through a quarterly deck presentation. Inspected the quarterly deck presentation slides during the examination period noting that management reported environmental, compliance, regulatory, technological changes, internal controls, and control deficiencies to Axcient's Board of Directors through a quarterly deck presentation.	No exceptions noted. No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Vulnerability testing is performed on servers weekly. Vulnerabilities are tracked in Jira until resolved.	Inquired of the Security & Compliance Analyst about vulnerability testing noting that vulnerability testing was performed on servers weekly. Also noted that high risk vulnerabilities were tracked in Jira until resolved. Inspected vulnerability scan logs and configurations for servers during the examination period noting that vulnerability testing was performed weekly on servers. Also noted that high risk vulnerabilities were tracked in Jira until resolved.	No exceptions noted. No exceptions noted.
		Separate environments are in place for test, development, and production activities.	Inquired of the Chief Information Security Officer about the test, development, and production environments noting that separate environments were in place for test, development, and production activities. Inspected environments for each in-scope application noting that separate environments were in place for test, development, and production activities.	No exceptions noted. No exceptions noted.
		Access to the application database test, development, and production servers is restricted to authorized personnel.	Inquired of the Chief Information Security Officer about access to the application database test, development, and production servers noting that access was restricted to authorized personnel. Inspected Axcient's application user access listings noting that access to the application database test, development, and production servers was restricted to authorized personnel.	No exceptions noted. No exceptions noted.
		Management performs a risk assessment to identify threats to the system or environment, and communicates the risks to the Board of Directors for review.	Inquired of the Chief Information Security Officer about the risk assessment process noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review. Inspected the risk assessment performed during the examination period noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review.	No exceptions noted. No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Management performs a risk assessment to identify threats to the system or environment, and communicates the risks to the Board of Directors for review.	Inquired of the Chief Information Security Officer about the risk assessment process noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review. Inspected the risk assessment performed during the examination period noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review.	No exceptions noted. No exceptions noted.
		A security evaluation is completed for new third-party vendors whose services are integrated with Axcient.	Inquired of the IT Administrator about security evaluations noting that a security evaluation was completed for new third-party vendors whose services would be integrated with Axcient. Also noted there were no new third-party vendors during the examination period.	No exceptions noted.
		Laptop reset procedures are in place for the removal of data from any laptops that will no longer be used by the organization.	Inquired of the IT Administrator about laptop data noting that laptop reset procedures were in place for the removal of data from any laptops that would no longer be used by the organization. Also noted that there were no laptops that would no longer be used by the organization identified during the examination period. Inspected the laptop reset procedures noting that the laptop reset procedures were in place for the removal of data from any laptops that would no longer be used by the organization.	No exceptions noted. No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Data management and removal procedures are in place for the retention and removal of data from user laptops upon termination.	Inquired of the IT Administrator and the Security & Compliance Analyst about data management noting that data management and removal procedures were in place for the retention and removal of data from user laptops upon termination.	No exceptions noted.
			Inspected the laptop reset procedures noting that the laptop reset procedures were in place for the retention and removal of data from user laptops upon termination.	No exceptions noted.
			Inspected termination checklists for randomly selected employee terminations during the examination period noting that data management and removal procedures were in place for the retention and removal of data from user laptops upon termination.	No exceptions noted.
		Access to the application database test, development, and production servers is restricted to authorized personnel.	Inquired of the Chief Information Security Officer about access to the application database test, development, and production servers noting that access was restricted to authorized personnel.	No exceptions noted.
			Inspected Axcient's application user access listings noting that access to the application database test, development, and production servers was restricted to authorized personnel.	No exceptions noted.

CC 5.0 Control Activities				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Axcient's policies and procedures are approved by management and accessible by employees on Axcient's common drive to which employees have access. Company policies are reviewed at least annually and updated as necessary by senior management.	Inquired of the Chief Information Security Officer about policies and procedures noting that Axcient's policies and procedures were approved by management and accessible by employees on Axcient's common drive to which employees had access. Also noted that Company policies were reviewed at least annually and updated as necessary by senior management. Inspected Axcient's common drive users noting that Company policies and procedures were accessible by employees on Axcient's common drive to which employees had access. Inspected the review date for Company policies and procedures noting that Axcient's policies and procedures were reviewed by management at least annually and updated as necessary by senior management.	No exceptions noted. No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Applications with backend data are configured to enforce complex passwords.	Inquired of the Security & Compliance Analyst about password configurations noting that applications with backend data were configured to enforce complex passwords. Inspected application password configurations for Ancient's products noting that applications with backend data were configured to enforce complex passwords.	No exceptions noted. No exceptions noted.
		Password management is in place and used for the management, administration, and enforcement of passwords complexity requirements for access to critical systems.	Inquired of the Security & Compliance Analyst about password management noting that password management was in place and used for the management, administration, and enforcement of passwords complexity requirements for access to critical systems. Observed the password management application noting that password management was in place and used for the management, administration, and enforcement of passwords complexity requirements for access to critical systems.	No exceptions noted. No exceptions noted.
		Axcient maintains an Employee Handbook, which contains security policies including the Personnel Acceptable Use Policy, Password Policy, and Incident Response Policy. The Employee Handbook is made available to employees and contractors on Axcient's common drive.	Inquired of the VP of People about location of the Employee Handbook noting that Axcient maintained an Employee Handbook, which contained security policies including the Personnel Acceptable Use Policy, Password Policy, and Incident Response Policy. Also noted that the Employee Handbook was made available to employees and contractors on Axcient's common drive. Inspected the Employee Handbook noting that Axcient maintained an Employee Handbook, which contained security policies including the Personnel Acceptable Use Policy, Password Policy, and Incident Response Policy. Inspected Axcient's common drive noting that the Employee Handbook was made available to employees and contractors on Axcient's common drive.	No exceptions noted. No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Access for new employees and contractors to the system and applications is designed based on job roles and responsibilities.	Inquired of the IT Manager about new employee access noting that access for new employees and contractors to the system and applications was designed based on job roles and responsibilities. Inspected access tickets for randomly selected new employees and contractors during the examination period noting that access for new employees and contractors to the system and applications was designed based on job roles and responsibilities.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Access for new employees and contractors to the system and applications is designed based on job roles and responsibilities.	Inquired of the IT Manager about new employee access noting that access for new employees and contractors to the system and applications was designed based on job roles and responsibilities. Inspected access tickets for randomly selected new employees and contractors during the examination period noting that access for new employees and contractors to the system and applications was designed based on job roles and responsibilities.	No exceptions noted. No exceptions noted.
		During the termination process, physical and logical access of terminated users is deactivated within one business day and are tracked on a termination checklist.	Inquired of the VP of People about access termination noting that during the termination process, physical and logical access of terminated users was deactivated within one business day and were tracked on a termination checklist. Inspected termination checklists for randomly selected terminated employees and contractors during the examination period noting that during the termination process, physical and logical access of terminated users was deactivated within one business day and were tracked on a termination checklist.	No exceptions noted. Two of five randomly selected terminated employees did not have logical access terminated within one business day. Per the termination checklist, access was terminated within three business days. *Management Response:* All staff have access removed immediately upon termination. Because the process is not centralized with identity management, and requires manually verifying the task was completed, evidence produced was contrary to actual process and results.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Access provisioning is requested and approved by the employee's manager, via email or Smartsheet submission to the IT Infrastructure team.	Inquired of the Security & Compliance Analyst about user access provisioning noting that access provisioning was requested and approved by the employee's manager, via email or Smartsheet submission to the IT infrastructure team. Inspected emails and the Smartsheet access provisioning request log for randomly selected new employees and contractors during the examination period noting that access provisioning was requested and approved by the employee's manager, via email or Smartsheet submission to the IT Infrastructure team.	No exceptions noted. Eight of 10 randomly selected new employees and contractors during the examination period did not have evidence of the request and approval of access provisioning by the employee's manager via email or Smartsheet submission to the IT Infrastructure team. *Management Response:* Access Management can only be granted by a request to a manager. Unfortunately, due to turnover, a record of those requests was not memorialized. New processes were put in place post-audit to make the review process more streamlined in the future.
		Access changes are requested by the end user through JIRA and approved/granted by the appropriate Engineering team. Requests for privileged access are also reviewed by the Security team prior to completion.	Inquired of the IT Manager about access change noting that access changes were requested by the end user through JIRA and approved/granted by the appropriate Engineering team. Also noted that requests for privileged access were reviewed by the Security team prior to completion. Inspected access tickets for randomly selected access changes during the examination period noting that access changes were requested by the end user through JIRA and approved/granted by the appropriate Engineering team. Also noted that requests for privileged access were reviewed by the Security team prior to completion.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Access provisioning is requested and approved by the employee's manager, via email or Smartsheet submission to the IT Infrastructure team.	Inquired of the Security & Compliance Analyst about user access provisioning noting that access provisioning was requested and approved by the employee's manager, via email or Smartsheet submission to the IT infrastructure team. Inspected emails and the Smartsheet access provisioning request log for randomly selected new employees and contractors during the examination period noting that access provisioning was requested and approved by the employee's manager, via email or Smartsheet submission to the IT Infrastructure team.	No exceptions noted. Eight of 10 randomly selected new employees and contractors during the examination period did not have evidence of the request and approval of access provisioning by the employee's manager via email or Smartsheet submission to the IT Infrastructure team. *Management Response:* Access Management can only be granted by a request to a manager. Unfortunately, due to turnover, a record of those requests was not memorialized. New processes were put in place post-audit to make the review process more streamlined in the future.
		Separate environments are in place for test, development, and production activities.	Inquired of the Chief Information Security Officer about the test, development, and production environments noting that separate environments were in place for test, development, and production activities. Inspected environments for each in-scope application noting that separate environments were in place for test, development, and production activities.	No exceptions noted. No exceptions noted.
		Access to the application database test, development, and production servers is restricted to authorized personnel.	Inquired of the Chief Information Security Officer about access to the application database test, development, and production servers noting that access was restricted to authorized personnel. Inspected Axcient's application user access listings noting that access to the application database test, development, and production servers was restricted to authorized personnel.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Access for new employees and contractors to the system and applications is designed based on job roles and responsibilities.	Inquired of the IT Manager about new employee access noting that access for new employees and contractors to the system and applications was designed based on job roles and responsibilities. Inspected access tickets for randomly selected new employees and contractors during the examination period noting that access for new employees and contractors to the system and applications was designed based on job roles and responsibilities.	No exceptions noted. No exceptions noted.
		Access changes are requested by the end user through JIRA and approved/granted by the appropriate Engineering team. Requests for privileged access are also reviewed by the Security team prior to completion.	Inquired of the IT Manager about access change noting that access changes were requested by the end user through JIRA and approved/granted by the appropriate Engineering team. Also noted that requests for privileged access were reviewed by the Security team prior to completion. Inspected access tickets for randomly selected access changes during the examination period noting that access changes were requested by the end user through JIRA and approved/granted by the appropriate Engineering team. Also noted that requests for privileged access were reviewed by the Security team prior to completion.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		During the termination process, physical and logical access of terminated users is deactivated within one business day and are tracked on a termination checklist.	Inquired of the VP of People about access termination noting that during the termination process, physical and logical access of terminated users was deactivated within one business day and were tracked on a termination checklist. Inspected termination checklists for randomly selected terminated employees and contractors during the examination period noting that during the termination process, physical and logical access of terminated users was deactivated within one business day and were tracked on a termination checklist.	No exceptions noted. Two of five randomly selected terminated employees did not have logical access terminated within one business day. Per the termination checklist, access was terminated within three business days. *Management Response:* All staff have access removed immediately upon termination. Because the process is not centralized with identity management, and requires manually verifying the task was completed, evidence produced was contrary to actual process and results.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Access to the Axcient office is secured during business and non-business hours with badge access. Visitors are given a sticker badge with their picture and are escorted.	Inquired of the IT Manager about access to the Axcient office noting that access to the Axcient office was secured during business and non-business hours with badge access. Also noted that visitors were given a sticker badge with their picture and were escorted. Observed access to the Axcient office noting that access to the Axcient office was secured during business and non-business hours with badge access. Also noted that visitors were given a sticker badge with their picture and were escorted.	No exceptions noted. No exceptions noted.
		A security evaluation is completed for new third-party vendors whose services are integrated with Axcient.	Inquired of the IT Administrator about security evaluations noting that a security evaluation was completed for new third-party vendors whose services would be integrated with Axcient. Also noted there were no new third-party vendors during the examination period.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Third-party service providers undergo an annual SOC 2 Type 2 examination related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Axcient's management performs a detailed review of SOC 2 Type 2 report to evaluate the scope, testing results, and complementary user entity controls.	Inquired of the Security & Compliance Analyst about third-party service providers annual review noting that third-party service providers underwent an annual SOC 2 Type 2 examination related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient's management performed a detailed review of SOC 2 Type 2 report to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the AWS SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (October 1, 2018 through March 31, 2019) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the Equinix, Inc. SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (November 1, 2017 through October 31, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
			Inspected the zColo SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service providers underwent an annual SOC 2 Type 2 examination (November 1, 2017 through October 31, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the TeraGo SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (February 1, 2018 through November 30, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the Flexential SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (April 1, 2018 through October 31, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Laptop reset procedures are in place for the removal of data from any laptops that will no longer be used by the organization.	Inquired of the IT Administrator about laptop data noting that laptop reset procedures were in place for the removal of data from any laptops that would no longer be used by the organization. Also noted that there were no laptops that would no longer be used by the organization identified during the examination period. Inspected the laptop reset procedures noting that the laptop reset procedures were in place for the removal of data from any laptops that would no longer be used by the organization.	No exceptions noted. No exceptions noted.
		Data management and removal procedures are in place for the retention and removal of data from user laptops upon termination.	Inquired of the IT Administrator and the Security & Compliance Analyst about data management noting that data management and removal procedures were in place for the retention and removal of data from user laptops upon termination. Inspected the laptop reset procedures noting that the laptop reset procedures were in place for the retention and removal of data from user laptops upon termination. Inspected termination checklists for randomly selected employee terminations during the examination period noting that data management and removal procedures were in place for the retention and removal of data from user laptops upon termination.	No exceptions noted. No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	NextGen firewalls are in place and protect the network perimeter with a default deny policy blocking unnecessary ports. Advanced sandboxing technology is used for intrusion prevention to protect Axcient's web application.	Inquired of the Chief Information Security Officer about application protection noting that NextGen firewalls were in place and protected the network perimeter with a default deny policy blocking unnecessary ports. Also noted that advanced sandboxing technology was used for intrusion prevention to protect Axcient's web application. Inspected firewall configurations and advanced sandboxing technology logs noting that NextGen firewalls were in place and protected the network perimeter with a default deny policy blocking unnecessary ports. Also noted that advanced sandboxing technology was used for intrusion prevention to protect Axcient's web application.	No exceptions noted. No exceptions noted.
		Security settings are enabled for wireless networks which includes encryption and user authentication.	Inquired of the IT Manager about wireless network encryption noting that security settings were enabled for wireless networks which included encryption and user authentication. Inspected the wireless network configuration settings noting that security settings were enabled for wireless networks which included encryption and user authentication.	No exceptions noted. No exceptions noted.
		White-listing configuration settings are in place that restrict access to the systems using approved IP addresses for remote sessions.	Inquired of the Chief Information Security Officer about white-listing noting that white-listing configuration settings were in place that restricted access to the systems using approved IP addresses for remote sessions. Inspected white-listing configuration settings noting that white-listing configuration settings were in place that restricted access to the systems using approved IP addresses for remote sessions.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Data management and removal procedures are in place for the retention and removal of data from user laptops upon termination.	Inquired of the IT Administrator and the Security & Compliance Analyst about data management noting that data management and removal procedures were in place for the retention and removal of data from user laptops upon termination. Inspected the laptop reset procedures noting that the laptop reset procedures were in place for the retention and removal of data from user laptops upon termination. Inspected termination checklists for randomly selected employee terminations during the examination period noting that data management and removal procedures were in place for the retention and removal of data from user laptops upon termination.	No exceptions noted. No exceptions noted. No exceptions noted.
		Disk encryption is installed on servers to ensure data is encrypted at rest.	Inquired of the IT Manager about encryption at rest noting that disk encryption was installed on servers to ensure data was encrypted at rest. Inspected encryption key configurations noting that disk encryption was installed on servers to ensure data is encrypted at rest.	No exceptions noted. Although encryption key configurations were provided, evidence was not available to determine the operational effectiveness during the examination period. *Management Response:* Evidence, as requested, was provided to the auditors. Being a HIPAA compliant company, we are required to have full disk encryption on all our partner storage to adhere to the regulations. Evidence was requested and provided outside of the audit window, but was in place at the time of the audit.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Security settings are enabled for wireless networks which includes encryption and user authentication.	Inquired of the IT Manager about wireless network encryption noting that security settings were enabled for wireless networks which included encryption and user authentication. Inspected the wireless network configuration settings noting that security settings were enabled for wireless networks which included encryption and user authentication.	No exceptions noted. No exceptions noted.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Vulnerability testing is performed on servers weekly. Vulnerabilities are tracked in Jira until resolved.	Inquired of the Security & Compliance Analyst about vulnerability testing noting that vulnerability testing was performed on servers weekly. Also noted that high risk vulnerabilities were tracked in Jira until resolved. Inspected vulnerability scan logs and configurations for servers during the examination period noting that vulnerability testing was performed weekly on servers. Also noted that high risk vulnerabilities were tracked in Jira until resolved.	No exceptions noted. No exceptions noted.
		Users' laptops are required to be in compliance with Axcient's Security Policy regarding anti-virus.	Inquired of the Security & Compliance Analyst about user laptop compliance noting that users' laptops were required to be in compliance with Axcient's Security Policy regarding anti-virus. Inspected the Axcient Security Policy noting that users' laptops were required to be in compliance with Axcient's Security Policy regarding anti-virus. Inspected workstation anti-virus logs for randomly selected current employees during the examination period noting that users' laptops were in compliance with Axcient's Security Policy regarding anti-virus.	No exceptions noted. No exceptions noted. Thirty-one of 40 randomly selected employees and contractors did not have evidence of compliance with Axcient's Security policy regarding anti-virus installed on their workstations. *Management Response:* While our previous endpoint security solution did not provide a practical way to report on protected devices, evidence was provided after the examination period of 20 of the 31 having current security installed. We have since switched to a new endpoint security solution as well as updated our remote monitoring and management (RMM) to ensure all devices are corrected going forward.

CC 6.0 Logical and Physical Access Controls				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Penetration testing is performed annually by a third party and management is notified of suspicious activities. Management reviews critical risks to determine necessary action.	Inquired of the Security & Compliance Analyst about penetration testing noting that penetration testing was performed annually by a third party and management was notified of suspicious activities. Also noted that management reviewed critical risks to determine necessary action. Inspected penetration test reports during the examination period noting that penetration testing was performed annually by a third party and management was notified of suspicious activities. Also noted that there were no critical risks identified during the examination period.	No exceptions noted. No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Vulnerability testing is performed on servers weekly. Vulnerabilities are tracked in Jira until resolved.	Inquired of the Security & Compliance Analyst about vulnerability testing noting that vulnerability testing was performed on servers weekly. Also noted that high risk vulnerabilities were tracked in Jira until resolved. Inspected vulnerability scan logs and configurations for servers during the examination period noting that vulnerability testing was performed weekly on servers. Also noted that high risk vulnerabilities were tracked in Jira until resolved.	No exceptions noted. No exceptions noted.
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Vulnerability testing is performed on servers weekly. Vulnerabilities are tracked in Jira until resolved.	Inquired of the Security & Compliance Analyst about vulnerability testing noting that vulnerability testing was performed on servers weekly. Also noted that high risk vulnerabilities were tracked in Jira until resolved. Inspected vulnerability scan logs and configurations for servers during the examination period noting that vulnerability testing was performed weekly on servers. Also noted that high risk vulnerabilities were tracked in Jira until resolved.	No exceptions noted. No exceptions noted.
		NextGen firewalls are in place and protect the network perimeter with a default deny policy blocking unnecessary ports. Advanced sandboxing technology is used for intrusion prevention to protect Axcient's web application.	Inquired of the Chief Information Security Officer about application protection noting that NextGen firewalls were in place and protected the network perimeter with a default deny policy blocking unnecessary ports. Also noted that advanced sandboxing technology was used for intrusion prevention to protect Axcient's web application. Inspected firewall configurations and advanced sandboxing technology logs noting that NextGen firewalls were in place and protected the network perimeter with a default deny policy blocking unnecessary ports. Also noted that advanced sandboxing technology was used for intrusion prevention to protect Axcient's web application.	No exceptions noted. No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Security incidents are tracked in Jira, rated by severity, with P0/P1's being resolved within 72 hours.	Inquired of the Chief Information Security Officer about incident tracking noting that security incidents were tracked in Jira, rated by severity, with P0/P1's being resolved within 72 hours. Also noted that there were no P0/P1 incidents identified during the examination period.	No exceptions noted.
		Axcient maintains Security Policies which document the security requirements for authorized users and detail the requirements outlining the classification of data and use thereof.	Inquired of the Chief Information Security Officer about security policies noting that Axcient maintained Security Policies which documented the security requirements for authorized users and detailed the requirements outlining the classification of data and use thereof.	No exceptions noted.
			Inspected the Company Policies folder in the company common drive noting that Axcient maintained Security Policies.	No exceptions noted.
			Inspected the Access Control Monitoring Policy and the Data Classification Policy noting that Axcient maintained Security Policies which documented the security requirements for authorized users and detailed the requirements outlining the classification of data and use thereof.	No exceptions noted.
		Axcient maintains an incident response plan that documents a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure client data is secure.	Inquired of the Chief Information Security Officer about the incident response process noting that Axcient maintained an Incident Response Plan that documented a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure client data was secure.	No exceptions noted.
			Inspected the Incident Response Plan noting that Axcient maintained an Incident Response Plan that documented a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure the client data was secure.	No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Axcient maintains an incident response plan that documents a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure client data is secure.	Inquired of the Chief Information Security Officer about the incident response process noting that Axcient maintained an Incident Response Plan that documented a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure client data was secure. Inspected the Incident Response Plan noting that Axcient maintained an Incident Response Plan that documented a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure the client data was secure.	No exceptions noted. No exceptions noted.
		Security incidents are tracked in Jira, rated by severity, with P0/P1's being resolved within 72 hours.	Inquired of the Chief Information Security Officer about incident tracking noting that security incidents were tracked in Jira, rated by severity, with P0/P1's being resolved within 72 hours. Also noted that there were no P0/P1 incidents identified during the examination period.	No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Penetration testing is performed annually by a third party and management is notified of suspicious activities. Management reviews critical risks to determine necessary action.	Inquired of the Security & Compliance Analyst about penetration testing noting that penetration testing was performed annually by a third party and management was notified of suspicious activities. Also noted that management reviewed critical risks to determine necessary action. Inspected penetration test reports during the examination period noting that penetration testing was performed annually by a third party and management was notified of suspicious activities. Also noted that there were no critical risks identified during the examination period.	No exceptions noted. No exceptions noted.
		Policy and procedure documents are published for significant processes, including the process and responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints. They are available on Axcient's common drive to employees and externally on Axcient's Terms of Service on the company website.	Inquired of the Chief Information Security Officer about internal policies and procedures noting that policy and procedure documents were published for significant processes, including the process and responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints. Also noted that they were available on Axcient's common drive to employees and externally within Axcient's Terms of Service on the company website. Inspected the policy and procedure document noting that policy and procedure documents were published for significant processes, including the process and responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints. Inspected Axcient's common drive and Axcient's Terms of Service on the company website noting that policies and procedure documents were available on Axcient's common drive to employees and externally within Axcient's Terms of Service on the company website.	No exceptions noted. No exceptions noted. No exceptions noted.

CC 7.0 System Operations				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Axcient maintains an incident response plan that documents a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure client data is secure.	Inquired of the Chief Information Security Officer about the incident response process noting that Axcient maintained an Incident Response Plan that documented a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure client data was secure. Inspected the Incident Response Plan noting that Axcient maintained an Incident Response Plan that documented a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure the client data was secure.	No exceptions noted. No exceptions noted.
		Security incidents are tracked in Jira, rated by severity, with P0/P1's being resolved within 72 hours.	Inquired of the Chief Information Security Officer about incident tracking noting that security incidents were tracked in Jira, rated by severity, with P0/P1's being resolved within 72 hours. Also noted that there were no P0/P1 incidents identified during the examination period.	No exceptions noted.

CC 8.0 Change Management				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Access to the application database test, development, and production servers is restricted to authorized personnel.	Inquired of the Chief Information Security Officer about access to the application database test, development, and production servers noting that access was restricted to authorized personnel. Inspected Axcient's application user access listings noting that access to the application database test, development, and production servers was restricted to authorized personnel.	No exceptions noted. No exceptions noted.
		Major changes are approved in a peer review and by the product owner prior to completion of the sprint.	Inquired of the IT Manager about major changes to critical systems noting that major changes to critical systems were approved in a peer review and by the product owner prior to completion of the sprint. Inspected change tickets for randomly selected major changes to critical systems during the examination period noting that major changes to critical systems were approved in a peer review and by the product owner prior to completion of the sprint.	No exceptions noted. No exceptions noted.
		Separate environments are in place for test, development, and production activities.	Inquired of the Chief Information Security Officer about the test, development, and production environments noting that separate environments were in place for test, development, and production activities. Inspected environments for each in-scope application noting that separate environments were in place for test, development, and production activities.	No exceptions noted. No exceptions noted.

CC 9.0 Risk Mitigation				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from business disruption.	Management reports environmental, compliance, regulatory, technological changes, internal controls, and control deficiencies to Axcient's Board of Directors through a quarterly deck presentation.	Inquired of the Chief Information Security Officer about Board of Directors meetings noting that management reported environmental, compliance, regulatory, technological changes, internal controls, and control deficiencies to Axcient's Board of Directors through a quarterly deck presentation. Inspected the quarterly deck presentation slides during the examination period noting that management reported environmental, compliance, regulatory, technological changes, internal controls, and control deficiencies to Axcient's Board of Directors through a quarterly deck presentation.	No exceptions noted. No exceptions noted.
		Management performs a risk assessment to identify threats to the system or environment, and communicates the risks to the Board of Directors for review.	Inquired of the Chief Information Security Officer about the risk assessment process noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review. Inspected the risk assessment performed during the examination period noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review.	No exceptions noted. No exceptions noted.
		Axcient maintains an incident response plan that documents a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure client data is secure.	Inquired of the Chief Information Security Officer about the incident response process noting that Axcient maintained an Incident Response Plan that documented a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure client data was secure. Inspected the Incident Response Plan noting that Axcient maintained an Incident Response Plan that documented a risk mitigation strategy by assessing potential risks and vulnerabilities to help ensure the client data was secure.	No exceptions noted. No exceptions noted.

CC 9.0 Risk Mitigation				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
CC 9.2	The entity assesses and manages risks associated with vendors and business partners.	Axcient's security commitments regarding the system are included in the master services agreement (MSA).	Inquired of the Senior Manager of Operations about security commitments noting that Axcient's security commitments regarding the system were included in the MSA. Inspected signed MSAs for randomly selected new clients during the examination period noting that Axcient's security commitments regarding the system were included in the MSAs.	No exceptions noted. No exceptions noted.
		Axcient's privacy policy is posted on the company's website and clients are notified when substantial updates are made.	Inquired of the Chief Information Security Officer about Axcient's privacy policy noting that Axcient's privacy policy was posted on the company's website and clients were notified when substantial updates were made. Also noted that no substantial updates were made during the examination period. Inspected the company's website noting that Axcient's privacy policy was posted on the company's website.	No exceptions noted. No exceptions noted.

CC 9.0 Risk Mitigation				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Third-party service providers undergo an annual SOC 2 Type 2 examination related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Axcient's management performs a detailed review of SOC 2 Type 2 report to evaluate the scope, testing results, and complementary user entity controls.	Inquired of the Security & Compliance Analyst about third-party service providers annual review noting that third-party service providers underwent an annual SOC 2 Type 2 examination related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient's management performed a detailed review of SOC 2 Type 2 report to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the AWS SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (October 1, 2018 through March 31, 2019) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the Equinix, Inc. SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (November 1, 2017 through October 31, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.

CC 9.0 Risk Mitigation				
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
			Inspected the zColo SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service providers underwent an annual SOC 2 Type 2 examination (November 1, 2017 through October 31, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the TeraGo SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (February 1, 2018 through November 30, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the Flexential SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (April 1, 2018 through October 31, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
		A security evaluation is completed for new third-party vendors whose services are integrated with Axcient.	Inquired of the IT Administrator about security evaluations noting that a security evaluation was completed for new third-party vendors whose services would be integrated with Axcient. Also noted there were no new third-party vendors during the examination period.	No exceptions noted.

A.0	Additional Criteria for Availability			
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
A 1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Axcient uses monitoring tools for capacity planning and the data is used to forecast trends. Alerts are sent to notify Axcient of any issue requiring further investigation.	Inquired of the Chief Information Security Officer and the Linux System Administrator and Architect (Cloud Engineering) about monitoring tools noting that Axcient used monitoring tools for capacity planning and the data was used to forecast trends. Also noted that alerts were sent to notify Axcient of any issue requiring further investigation.	No exceptions noted.
			Observed monitoring tools noting that Axcient used monitoring tools for capacity planning and the data was used to forecast trends.	No exceptions noted.
			Inspected the alert configurations and an alert notification received during the examination period noting that alerts were sent to notify Axcient of any issue requiring further investigation.	No exceptions noted.
		Axcient leadership meets on a quarterly basis to discuss system performance, availability, capacity, and security concerns and trends. In this meeting, control improvements are identified and status updates provided on the progress toward remediation.	Inquired of the VP of People about quarterly leadership meetings noting that Axcient leadership met on a quarterly basis to discuss system performance, availability, capacity, and security concerns and trends. Also noted that in this meeting, control improvements were identified and status updates provided on the progress toward remediation.	No exceptions noted.
			Inspected Product Council slide decks during the examination period noting that Axcient leadership met on a quarterly basis to discuss system performance, availability, capacity, and security concerns and trends. Also noted that in this meeting, control improvements were identified and status updates provided on the progress toward remediation.	No exceptions noted.

A.0	Additional Criteria for Availability			
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
A 1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Management performs a risk assessment to identify threats to the system or environment, and communicates the risks to the Board of Directors for review.	Inquired of the Chief Information Security Officer about the risk assessment process noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review. Inspected the risk assessment performed during the examination period noting that management performed a risk assessment to identify threats to the system or environment, and communicated the risks to the Board of Directors for review.	No exceptions noted. No exceptions noted.
		Management monitors information regarding the latest technical, security, and compliance threats. Security notifications received are evaluated.	Inquired of the Chief Information Security about technical, security, and compliance threats noting that management monitored information regarding the latest technical, security, and compliance threats. Also noted that security notifications received were evaluated. Inspected email notifications from monitoring systems during the examination period noting that management monitored information regarding the latest technical, security, and compliance threats. Inspected incident analysis for notifications from the monitoring systems during the examination period noting that technical, security, and compliance threats notifications received were evaluated.	No exceptions noted. No exceptions noted. No exceptions noted.

A.0	Additional Criteria for Availability			
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Third-party service providers undergo an annual SOC 2 Type 2 examination related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Axcient's management performs a detailed review of SOC 2 Type 2 report to evaluate the scope, testing results, and complementary user entity controls.	Inquired of the Security & Compliance Analyst about third-party service providers annual review noting that third-party service providers underwent an annual SOC 2 Type 2 examination related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient's management performed a detailed review of SOC 2 Type 2 report to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the AWS SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (October 1, 2018 through March 31, 2019) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the Equinix, Inc. SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (November 1, 2017 through October 31, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.

A.0	Additional Criteria for Availability			
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
			Inspected the zColo SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service providers underwent an annual SOC 2 Type 2 examination (November 1, 2017 through October 31, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the TeraGo SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (February 1, 2018 through November 30, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the Flexential SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (April 1, 2018 through October 31, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.

A.0	Additional Criteria for Availability			
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Critical systems are configured to back-up using in-house solutions.	Inquired of the Chief Technology Officer about system back-up noting that critical systems were configured to back-up using in-house solutions. Inspected backup configuration, schedule, and backup logs for critical systems noting that critical systems were configured to back-up using in-house solutions.	No exceptions noted. Although back-up configurations were later provided, evidence was not available to determine the operational effectiveness during the examination period. *Management Response:* Backups are retained for a 30-day window. At auditor's request, the configuration of backups and a screenshot of the previous 30 days were provided showing its operational effectiveness. The request was made well outside the audit window, which didn't allow us to provide proof we had backups in place at the time of the audit.

A.0	Additional Criteria for Availability			
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
A 1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Third-party service providers undergo an annual SOC 2 Type 2 examination related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Axcient's management performs a detailed review of SOC 2 Type 2 report to evaluate the scope, testing results, and complementary user entity controls.	Inquired of the Security & Compliance Analyst about third-party service providers annual review noting that third-party service providers underwent an annual SOC 2 Type 2 examination related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient's management performed a detailed review of SOC 2 Type 2 report to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the AWS SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (October 1, 2018 through March 31, 2019) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the Equinix, Inc. SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (November 1, 2017 through October 31, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.

A.0	Additional Criteria for Availability			
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
			Inspected the zColo SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service providers underwent an annual SOC 2 Type 2 examination (November 1, 2017 through October 31, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the TeraGo SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (February 1, 2018 through November 30, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.
			Inspected the Flexential SOC 2 Type 2 report, bridge letter, and management's review for the third-party service provider noting that the third-party service provider underwent an annual SOC 2 Type 2 examination (April 1, 2018 through October 31, 2018) related to the platform over Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality. Also noted that Axcient performed a detailed review of the SOC 2 Type 2 report and bridge letter (May 31, 2019) to evaluate the scope, testing results, and complementary user entity controls.	No exceptions noted.

A.0	Additional Criteria for Availability			
	Trust Services Criteria Related to Security and Availability	Controls Specified by Axcient	Tests Performed by Moss Adams LLP	Test Results
		Critical systems are configured to back-up using in-house solutions.	Inquired of the Chief Technology Officer about system back-up noting that critical systems were configured to back-up using in-house solutions. Inspected backup configuration, schedule, and backup logs for critical systems noting that critical systems were configured to back-up using in-house solutions.	No exceptions noted. Although back-up configurations were later provided, evidence was not available to determine the operational effectiveness during the examination period. *Management Response:* Backups are retained for a 30-day window. At auditor's request, the configuration of backups and a screenshot of the previous 30 days were provided showing its operational effectiveness. The request was made well outside the audit window, which didn't allow us to provide proof we had backups in place at the time of the audit.