Axonius, Inc.

Independent Service Auditor’s SOC 3 Report For the Axonius Cybersecurity Asset Management Platform System

For the Period of June 1, 2021, to November 30, 2021

Attestation and Compliance Services
INDEPENDENT SERVICE AUDITOR’S REPORT

To Axonius, Inc.:

Scope
We have examined Axonius, Inc.’s (“Axonius”) accompanying assertion titled “Assertion of Axonius, Inc. Service Organization Management” (“assertion”) that the controls within the Axonius Cyber Security Asset Management Platform system (“system”) were effective throughout the period June 1, 2021, to November 30, 2021, to provide reasonable assurance that Axonius’ service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Axonius uses a subservice organization for cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Axonius, to achieve Axonius’ service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system 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.

Service Organization’s Responsibilities
Axonius 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 Axonius’ service commitments and system requirements were achieved. Axonius has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Axonius is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

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

Our examination included:
- Obtaining an understanding of the system and the service organization’s service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve Axonius’ service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Axonius’ service commitments and system requirements based on the applicable trust services criteria.

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

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

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

Opinion

In our opinion, management’s assertion that the controls within the Axonius Cybersecurity Asset Management Platform system were effective throughout the period June 1, 2021, through November 30, 2021, to provide reasonable assurance that Axonius’ service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Scheiman & Company, LLC

Columbus, Ohio
December 13, 2021
We are responsible for designing, implementing, operating, and maintaining effective controls within the Axonius Cybersecurity Asset Management Platform system ("system") throughout the period June 1, 2021, to November 30, 2021, to provide reasonable assurance that Axonius’ service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2021, to November 30, 2021, to provide reasonable assurance that Axonius’ service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Axonius’ objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements related to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period June 1, 2021, to November 30, 2021, to provide reasonable assurance that Axonius’ service commitments and systems requirements were achieved based on the applicable trust services criteria.
DESCRIPTION OF THE BOUNDARIES OF THE AXONIUS CYBERSECURITY ASSET MANAGEMENT PLATFORM SYSTEM

Company Background

Founded in June 2017, Axonius offers a cybersecurity asset management platform that gives organizations a comprehensive asset inventory, uncovers gaps, and automatically validates and enforces policies. This cyber asset attack surface management (CAASM) solution integrates with hundreds of data sources to give customers the confidence to control complexity by mitigating threats, navigating risk, decreasing incidents, automating response actions, and informing business-level strategy.

Description of Services Provided

The Axonius Cybersecurity Asset Management Platform is a Software as a Service (SaaS) application that allows customers to manage IT assets with a focus on cybersecurity. The platform connects to customers’ existing data sources and tools and consolidates and correlates the data to provide a unified inventory of assets and their configurations. Customers can create custom, complex queries against all the sources of data and are able to take both automated and ad hoc actions upon the listings and information, such as quarantining a system from its network or opening a ticket for further investigation.

The Axonius Cybersecurity Asset Management Platform integrates with hundreds of security, management, and business solutions including Active Directory, cloud providers such as Amazon Web Services (AWS), endpoint protection tools, network access control solutions, mobile device management tools, vulnerability management tools, and many more. These adapters allow customers to feed data from various sources all into one location to make asset management seamless.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principal Service Commitments and System Requirements

Axonius designs its processes and procedures related to the Axonius Cybersecurity Asset Management Platform to meet its objectives for its cybersecurity and asset management services. Those objectives are based on the service commitments that Axonius makes to user entities, the laws and regulations that govern the provision of the Platform, and the financial, operational, and compliance requirements that Axonius has established for the services. Security commitments are documented and communicated in customer contracts, privacy policy, terms and conditions, and public website. The principal security commitments are standardized and include, but are not limited to, the following:

- Axonius will take all steps reasonably necessary to ensure that customer data is treated securely.
- Axonius employs administrative, physical, and technical measures in accordance with industry standards to protect data.
- Axonius has a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of data.

Axonius establishes policies and procedures as well as operational requirements that support the achievement of the principal service commitments (security), relevant laws and regulations, and other system requirements. These are achieved through controls including, but not limited to, implementing physical and technical safeguards, user access reviews, encryption technologies to protect system user authorization, and the documentation, testing, and approval of system changes.
Axonius cybersecurity policies define an organization-wide approach to how systems and data are protected. These include policies around how the system operates, how the internal business systems and networks are managed, and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Axonius platform.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure

The Axonius production environment is supported by infrastructure hosted by AWS. Only authorized Axonius personnel have the ability to log into the production environment via the roles assigned. End users access their Axonius Cybersecurity Asset Management Platform instance using encrypted web sessions. Axonius has implemented a single tenant SaaS and infrastructure environment to provide each customer with independent and separate servers and databases, as well as customizable virtual private cloud (VPC) security groups.

AWS is responsible for providing the physical safeguarding of the IT infrastructure to help ensure that unauthorized access to the IT infrastructure does not occur, as well as providing environmental safeguards (e.g., power supply, temperature control, fire suppression, etc.) against certain environmental threats. AWS is also responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Axonius platform resides.

People

The various personnel and teams involved in the operation and use of the system are as follows:

- **Executive Management** – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- **Security & IT (led by the CISO)** – responsible for creating and managing the company’s cybersecurity program including the identification of risks, compliance inspections, security monitoring, and the deployment and management of technological cybersecurity controls at Axonius. It also provides the Corporate IT function and includes the Cloud Infrastructure function, which manages cloud resources with the exception of Axonius-hosted product instances, which are handled by DevOps.
- **DevOps, Asset Group, and Solutions Architecture (SA)** – responsible for managing cloud resources and implementing information technology and security practices for Axonius’ product development and delivery infrastructure consistent with the Axonius’ cybersecurity program and the corresponding policies and procedures.
- **Customer Support** – responsible for supporting Axonius customers in their use of the Axonius product.
- **R&D and Product Teams** – responsible for maintaining a cybersecurity mindset when developing the Axonius application and engaging with the Security & IT Team as part of the system development lifecycle (SDLC) process.
- **People Team** – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
Procedures

HR and Training

Job descriptions are documented and utilized to outline the required skills needed and employee responsibilities for the job. As part of the hiring process, employment candidates are interviewed for the required skillset of the job position the employment candidate is applying for and identity verification procedures are performed. Upon hire, employees are required to sign an agreement including an acknowledgment of the standards of employee conduct, as well as a non-disclosure agreement. Additionally, an employee discipline procedure is documented that outlines employees may be disciplined up to termination for violation of the standards of employee conduct or other company policies.

New hires are required upon hire, and existing employees on at least an annual basis, to complete a security awareness training to understand their obligations and responsibilities to comply with the corporate and business unit security policies. Ongoing training is also provided and available for employees to maintain and further develop their proficiency. In addition to the optional and required trainings for all employees, development, product, and engineering personnel are required to complete developer training on an annual basis to understand security considerations when developing software. This includes reviewing when to include security team members in the change management process, as well as controls in place to help ensure code is developed and implemented in a secure manner and follows the defined change management process.

Access, Authentication, and Authorization

In order to connect to production systems, employees must first authenticate to the single sign on (SSO) which enforces two-factor authentication. Once authenticated, the SSO provides authorization to production systems and infrastructure based on preconfigured and preassigned roles. The ability to administer access to the SSO, AWS utilities, and underlying infrastructure is restricted to authorized personnel with administrative privileges via SSO roles.

Access Requests and Access Revocation

Policies, procedures, and workflows have been established for provisioning and removal of access. User access reviews are performed on at least an annual basis to help ensure that roles and access to data are restricted to authorized personnel and conform with job responsibilities.

When an employee is terminated, People personnel notify Security & IT of the termination. Upon receipt of the termination notification, Security & IT personnel complete a termination checklist to help ensure that specific elements of the termination process are consistently executed. As part of the termination process, Security & IT personnel revoke the terminated employee’s access privileges to the production systems.

Customers may request changes to their own AWS instances that may include additional administrator access, password resets, changes to security group rulesets, or other unique configuration changes. These change requests are made via a ticketing system and Customer Support personnel verify that change requests are made from an authorized customer contact and obtain approval prior to implementing the change. Customers are responsible for removing users from their Axonius application instance when they are terminated or when access is no longer appropriate.

System Security

Policies and procedures are in place that govern baseline protection standards for company software, network devices, servers, and workstations and security policies and procedures are in place to guide personnel in system security practices; these include, but are not limited to, cybersecurity policies, access control policies, acceptable use policies, and technical operations procedures. AWS is responsible for ensuring a secure network in which the Axonius production systems reside. Security groups are in place providing for a virtual firewall for AWS instances to control incoming and outgoing traffic. External network traffic must be authorized by a security group rule; otherwise, the traffic is dropped and not permitted to communicate with the internal environment.
Encryption
To protect data while in transit, web servers utilize transport layer security (TLS) encryption for web communication sessions. Employee sessions via the SSO and end-user sessions via the Axonius application are encrypted using TLS.

System Monitoring
Axonius monitors its production systems through daily business operations as well as separate assessments that occur periodically throughout the year. Continuous system monitoring of the production environment and company assets is performed utilizing various tools for security threat monitoring, infrastructure monitoring, and network malicious activity monitoring. Utilizing a combination of pre-defined rules and thresholds, as well other criteria based on user behavior and expected system activity, the tools have established baselines that will alert security personnel when unauthorized or potentially malicious activity is detected. To help ensure that there are periodic checks on the Axonius’ security posture, security assessments are performed.

Additionally, management monitors the security impact of emerging technologies and threats and the impact of applicable laws or regulations for the Axonius services which are considered by management. This helps ensure continued system security and compliance with regulatory requirements and commitments made to customers.

Incident Response
A documented incident response plan for reporting security incidents is provided to employees to guide the identification and reporting of failures, potential or confirmed incidents, concerns, and other complaints. Communication of incidents is performed over secure communication channels internally, and guidelines for communicating with external parties in accordance with regulations and applicable laws is documented within the response plan. There is a group called the Security Working Group (SWG) participating in security governance activities, provide cybersecurity leadership, and contribute to the cybersecurity awareness culture. To help ensure that overall trends are monitored and address, the SWG discusses incidents as part of their quarterly meetings.

Media Handling and Disposal
A media handling and disposal policy is in place to guide personnel in Axonius’ requirements for the secure disposal of media when no longer required. This can include the destruction of non-electronic media, or the physical and data destruction related to electronic media such as of personal computers, network equipment, hard drives, and handheld devices. The Corporate IT team is responsible for adhering to the disposal and destruction policy for assets at end of life. For cloud infrastructure components, Axonius uses the infrastructure destruction method that is native to the hosting platform.

Vendor Management
To address risks associated with vendors, management maintains the vendor security risk assessment procedure which provides guidelines for managing risk during vendor onboarding, annual reassessment, and offboarding. Vendor contracts are in place to communicate security commitments between the vendor and Axonius. Monitoring procedures over existing vendors are performed as a part of ongoing day-to-day operations and formally to help ensure compliance by vendors and business partners with Axonius’ expectations.

Business Continuity and Disaster Recovery
To mitigate the risks of business disruptions, a business continuity and disaster recovery plan is in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. The disaster recovery plan is tested formally on an annual basis and as a component of regular maintenance.

Change Management
Documented change management policies and procedures are in place to guide personnel in executing the change management process. This includes the process to identify and plan for application and infrastructure changes, assigning responsibilities to evaluate the change based on risk, impact, and business need; as well as reviewing the change via testing and documented approvals. A development platform is utilized to centrally maintain, manage, and monitor application and infrastructure development and maintenance activities through implementation.
Data

The Axonius platform receives, processes, and retains information related to the asset inventory, device configurations, and users that authenticate to, and use, each device. This information is aggregated within the platform via the use of client-configured adapter connections which integrate with a wide array of security and IT management solutions within the client’s environment to collect and correlate information about devices, cloud instances, and users. This information is retained within each client’s separate instance, and the client manages access to their instance. Data may be reported for use via custom queries, dashboards, and reports for viewing and managing assets, configurations, and user activity. The following table describes the information used and supported by the system.

<table>
<thead>
<tr>
<th>Data Description</th>
<th>Data Reporting</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information collected and correlated about an organization’s users, asset inventory, and system configurations via pre-built adapter integrations within the Axonius platform.</td>
<td>Data is available to authorized client Axonius users via the web application. Access to data is managed by the client.</td>
<td>Confidential/Limited</td>
</tr>
<tr>
<td>Dashboards, charts, and asset query results generated on-demand from the Axonius application.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Subservice Organizations

The cloud hosting services provided by AWS were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, alone or in combination with controls at Axonius, and the types of controls expected to be implemented at AWS to achieve Axonius’ service commitments and system requirements based on the applicable trust services criteria.

<table>
<thead>
<tr>
<th>Control Activity Expected to be Implemented by AWS</th>
<th>Applicable Trust Services Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS is responsible for managing and monitoring logical access to the underlying network and virtualization management software for its cloud hosting services where production systems reside.</td>
<td>CC6.1, CC6.2, CC6.3, CC6.5</td>
</tr>
<tr>
<td>AWS is responsible for restricting and monitoring physical access to data center facilities, backup media, and other system components for its cloud hosting services where the production systems reside.</td>
<td>CC6.4, CC6.5, CC7.2</td>
</tr>
</tbody>
</table>

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security are applicable to the Axonius Cybersecurity Asset Management Platform system.