Axonius

NIST 800-53
Compliance Review

How Axonius Can Help Your Organization
Reach FISMA or FedRAMP Compliance

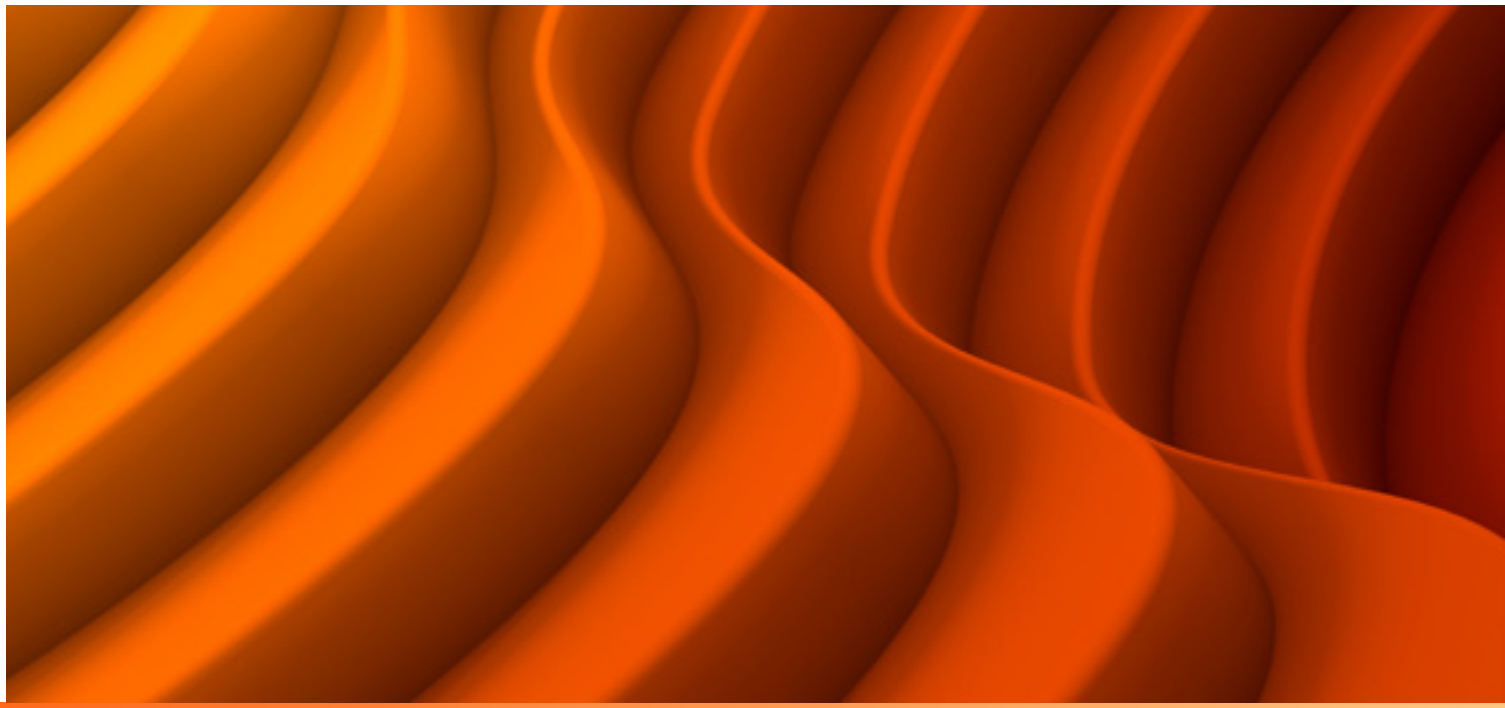


Table of Contents

Executive Summary

Overview

Axonius engaged Tevora, an independent, third-party information security and risk management consulting firm, to conduct an in-depth evaluation of Axonius against the National Institute of Science and Technology's (NIST) SP 800-53 Revision 5 requirements, high impact. Tevora is a leading security consulting firm specializing in enterprise risk, compliance, information security solutions, and threat research. Tevora offers a comprehensive portfolio of information security solutions and services to clients in all industries.

Tevora is also an accredited Third-Party Assessment Organization (3PAO) under the American Association for Laboratory Accreditation (A2LA), which is required to perform qualified assessments against NIST SP 800-53 for FedRAMP and GovRAMP compliance and is highly recommended for assessing FISMA compliance. Tevora partnered with the Axonius product and technical team to test Axonius features and capabilities mapping to NIST 800-53 Revision 5. Tevora was also granted access to the Axonius demo environment in order to conduct further testing and confirmation of capabilities.

Axonius transforms asset intelligence into intelligent action that security, IT, and governance, risk, and compliance teams can use to strengthen cybersecurity postures. The Axonius Asset Cloud allows organizations to preemptively tackle hard-to-spot threat exposures, misconfigurations, and operational challenges from one place. The Axonius Asset Cloud works in tandem with Axonius's market-leading Adapter Network, which features bi-directional integrations with more than 1,200 security and IT tools. Axonius uses its platform and network to build a complete, accurate, and always up-to-date model of agencies' attack surfaces, help teams prioritize critical actions, and make smart, effective, and data-driven decisions.

This whitepaper will navigate readers through the NIST 800-53 Revision 5 standard, the importance of NIST 800-53 compliance, and highlight applicable Axonius product capabilities.

NIST SP 800-53

Background

NIST Special Publication 800-53 Revision 5 provides a catalog of security and privacy controls for organizational information systems to be more resilient to a diverse range of threats, including malicious attacks, human error, natural disasters, structural failings, and foreign intelligence surveillance. The controls can be customized and implemented as part of an organization-wide process to manage risk and to meet business objectives more systematically.

The objective of NIST SP 800-53 is to set a basic standard for information security policies and controls for federal agencies or organizations contracted with federal agencies. The latest version, Revision 5, was released on September 23, 2020, to strengthen and modernize both security and privacy controls to better meet requirements set forth by the Federal Information Security Modernization Act (FISMA). The changes introduced are directly linked to the current state of the threat landscape (i.e., capabilities, intentions, and targeted activities of adversaries) and the attack data collected and analyzed over a three-year period.

Control Families

NIST SP 800-53 Rev. 5 requires organizations to comply with a robust set of criteria, which are broken down into 20 control families:

1. Access Control (AC)
2. Awareness and Training (AT)
3. Audit and Accountability (AU)
4. Assessment, Authorization, and Monitoring (CA)
5. Configuration Management (CM)
6. Contingency Planning (CP)
7. Identification and Authentication (IA)
8. Incident Response (IR)
9. Maintenance (MA)
10. Media Protection (MP)
11. Physical and Environmental Protection (PE)
12. Planning (PL)
13. Program Management (PM)
14. Personnel Security (PS)
15. Personally Identifiable Information Processing and Transparency (PT)
16. Risk Assessment (RA)
17. System and Services Acquisition (SA)
18. System and Communications Protection (SC)
19. System and Information Integrity (SI)
20. Supply Chain Risk Management (SR)

Each control family includes a range of controls that are further segmented according to the security baseline for which each control would be required.

Security Baselines

Federal Information Processing Standards Publication 199 (FIPS 199) establishes the standard for security baseline categorization of all federal information systems and information. NIST SP 800-53 relies on the following categorizations based on FIPS 199:

- Low – loss of confidentiality, integrity, or availability; would be expected to have a limited adverse effect on organizational operations, assets, or individuals
- Moderate – loss of confidentiality, integrity, or availability; would be expected to have a serious adverse effect on organizational operations, assets, or individuals
- High – loss of confidentiality, integrity, or availability; would be expected to have a severe or catastrophic adverse effect on organizational operations, assets, or individuals

FIPS 200 establishes minimum security requirements by relating NIST SP 800-53 security controls and control enhancements to the appropriate baseline defined in FIPS 199. Since FIPS documentation only establishes baseline requirements for security controls, the privacy controls identified in NIST SP 800-53 are not included within the baseline categorization. The privacy controls NIST determines as required must be implemented regardless of baseline levels.

Organizations NIST SP 800-53 Applies To

NIST SP 800-53 was originally designed for federal information systems and any applicable organizations that are contracted with federal agencies. Although these systems have requirements to comply with these security and privacy standards to safeguard government information, many non-governmental organizations can benefit from aligning their security program with NIST SP 800-53's comprehensive catalog of controls.

FISMA

FISMA is a United States legislation that made it a requirement for federal agencies to develop, document, and implement an information security protection program. FISMA was introduced in 2002 as part of the E-Government Act (Public Law 107-347). FISMA 2002 was amended by FISMA 2014, providing several modifications that modernize federal security practices to address evolving security concerns. FISMA 2014 defined the Department of Homeland Security's role in administering the implementation of information security policies for Federal Executive Branch civilian agencies, overseeing agencies' compliance with those policies, and assisting in developing those policies. The law aims to reduce the security risk to sensitive federal information. FISMA established a set of guidelines and cybersecurity standards that federal agencies must meet. Federal agencies need to provide information security protections commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of:

- information collected and maintained by or on behalf of an agency
- information systems that are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

Also, federal agencies need to "com[ply] with the information security standards", guidelines, and mandatory required standards developed by NIST.

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) was designed to enable easier contracting for federal agencies with cloud service providers (CSP). Like FISMA, the controls outlined in FedRAMP are based on the controls within NIST 800-53. The process of a FedRAMP certification requires a 3PAO to assess security controls of the CSP's service by completing a Security Assessment Plan (SAP), performing initial and periodic assessments, and producing a Security Assessment Report (SAR). The SAP, SAR, and CSP's System Security Plan are then submitted to the Joint Authorization Board (JAB) for an agency review. If authorized, the CSP's services are placed on the FedRAMP marketplace for other agencies to find services that meet their needs.

GovRAMP

GovRAMP provides a comprehensive security framework designed to improve cloud security for state and local governments. Like FedRAMP, GovRAMP aims to deliver a uniform approach to verifying that CSPs meet the standards and regulations needed to conduct business with state and local governments.

GovRAMP's goals are to help state and local governments:

- Protect the data of its citizens residing in the state
- Save taxpayer and service provider dollars with a "verify once, serve many" model
- Promote education and best practices in cybersecurity among those it services in industry and government communities

Commercial

NIST 800-53 is the most comprehensive set of cataloged controls. The different sets of controls map easily to many other frameworks such as PCI DSS, CIS Controls, SOC 2, and others. This overlap in control requirements allows organizations to easily tailor their program using relevant controls and baselines that best fit their organizational and business goals.

Challenges Implementing Controls

Complexity in Federal Information Technology

Movement toward Zero Trust architectures, secure cloud environments (including SaaS, IaaS, and PaaS), centralized and streamlined access to cybersecurity data, and increased incident response collaboration has significantly accelerated over the past several years. Axonius supports this momentum by providing:

- A single source of truth and total visibility into all cyber and software assets, SaaS applications, user identities, and more
- A complete, accurate, and continuously updated model of an agency's entire technology footprint
- Integration with thousands of systems across devices, applications, and identities—eliminating data conflicts and empowering teams with a unified operational platform
- Actionable insights that enable teams to prioritize their cybersecurity responses for greater efficiency and effectiveness
- Deep intelligence to uncover and address coverage gaps, critical vulnerabilities, misconfigurations, and excessive spending before they become issues
- Automated, comprehensive, and precise analysis and reporting to support NIST and FISMA compliance

Drafting a System Security Plan

A system security plan (SSP) is a formal document that provides an overview of the security requirements for an information system and describes both the security controls already in place or those planned to meet those requirements (Plan of Action and Milestones

(POA&M)). If an organization participates in contracts with the DoD, the contract requires an organization to have an SSP in place. The purpose of the SSP is to give anyone looking into an organization's cybersecurity posture a readable overview of security and controls that are in place to meet requirements. An SSP is a working and living document; as an organization matures

its security posture, the SSP will become larger and include more details.

Agencies should engage a third-party expert to assess and execute an SSP. However, Axonius can help organizations easily map security tools to requirements by identifying gaps and controls to safeguard Controlled Unclassified Information (CUI).

Maintaining a Plan of Action and Milestones

SSP and POA&M often work hand in hand. Each organization's POA&M is likely to defer in each organization because it includes information about weaknesses and gaps according to NIST 800-171 standards. The risk posture, gaps, weaknesses, and mitigating steps an organization intends to make should be documented within the POA&M. While an SSP is a working and living document that evolves over time, the POA&M document should become smaller as an organization implements mitigating controls.

Axonius for NIST 800-53 *Compliance*

Axonius helps federal government agencies safeguard their operations by bringing truth to action in their cybersecurity programs. The Axonius Asset Cloud platform uses a comprehensive asset data model that unifies formerly disparate information on devices, identities, applications, infrastructure, and more to provide agencies with complete, accurate, and always up-to-date information.

With total visibility into their entire asset ecosystem, agencies can uncover even the most difficult to spot threat exposures, risky misconfigurations, and resolve issues—before they become real threats.

Meanwhile, the Axonius Adapter Network includes integrations with more than 1,200 powerful business, IT, and security management tools. This allows Axonius to accurately collect data on all assets, users, vulnerabilities, and more, giving organizations a comprehensive picture of their asset landscape. Axonius uses this data to identify both known and unknown assets and build complete, accurate, and current models of agencies' attack surfaces.

Key Features for NIST 800-53:

Cybersecurity Asset Management: Accurate asset tracking and management requires continuous assessment, as organizations' IT ecosystems are in constant flux. Axonius allows organizations to obtain dynamic asset intelligence through continued visibility, actionability, and an always up-to-date, comprehensive asset inventory.

SaaS Management: Axonius allows organizations to discover all known and unknown SaaS applications and achieve full lifecycle management of all installed software. Agencies can see data interconnectivity between applications, identify risk, and optimize costs by eliminating problematic, redundant, or unused tools.

Exposure Management: Axonius unifies exposure findings and correlates and ranks risks so organizations can prioritize and efficiently execute mitigation efforts to minimize exposures. Organizations can benefit from continuous asset discovery, intelligent assessments, and streamlined remediation workflows.

Identity Management: Axonius simplifies and strengthens how IT and security teams collectively manage and secure identities. Axonius breaks down silos to ensure every identity is accounted for and Identity Access Management policies (IAM) are continuously enforced.

Cloud Asset Compliance: FedRAMP and FISMA require CSPs to conduct compliance assessments for inclusion on FedRAMP's marketplace. Axonius connects to organizations' cloud platforms to map the state of their cloud instances against industry standards and benchmarks. This capability allows teams to identify issues of non-compliance and reduce the time for manual assessments.

Policy Enforcement: The Axonius Policy Enforcement Center allows organizations to execute automated response actions to immediately address assets that do not adhere to company policies or have vulnerabilities that may put the organization at risk.

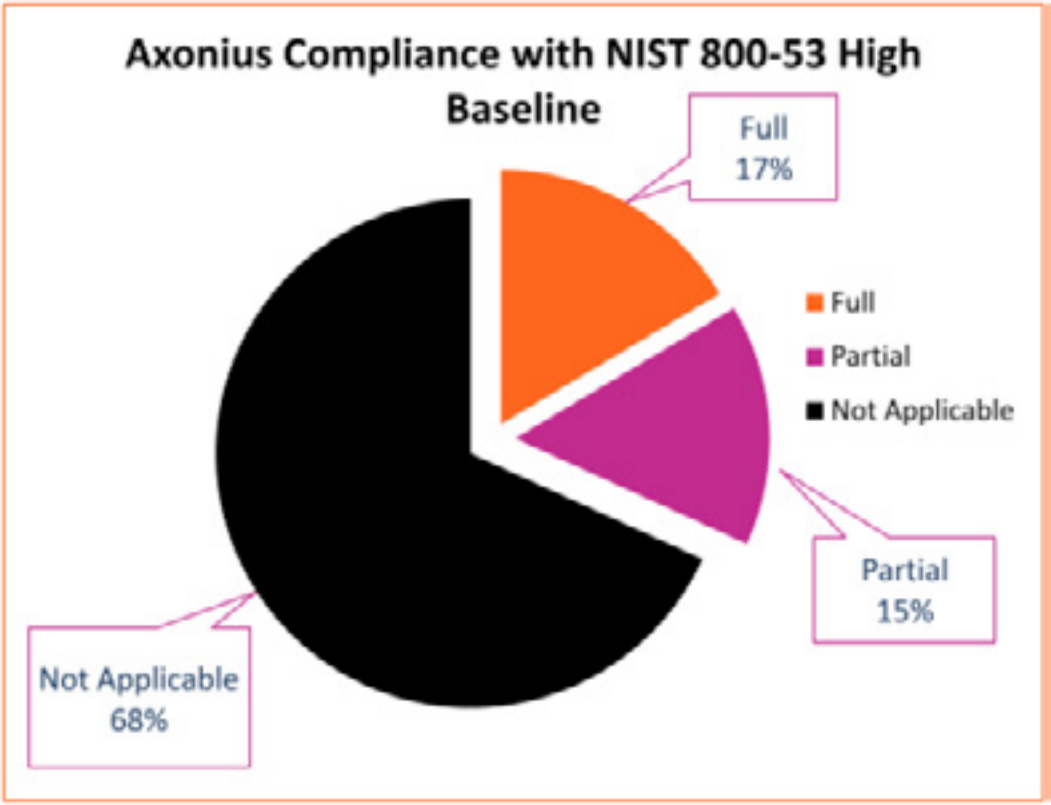
Vulnerability and Incident Management: Attack security, vulnerability management, and incident response teams must have advance warning of evolving threats to reduce the likelihood of compromise. Axonius turns threat intelligence into intelligent action, providing teams with the information they need to proactively target and prioritize threat response for an efficient yet strong security posture.

Flexible Deployment Options:

- Customer-hosted (on-premises/private cloud): deployed on a virtual appliance that is part of an organization's internal network
- Axonius-hosted (SaaS): deployed on an AWS EC2 instance that is fully separated from other customers' environments. The AWS EC2 instance can be hosted on any of the available Amazon EC2 regions

Axonius Capability Charts

Below is a chart that displays the compliance capabilities Axonius provides to organizations that want to achieve compliance with NIST 800-53 Revision 5. The complete guide includes over 1,200 security controls. For the High Baseline, NIST requires organizations to implement 371 specific controls, and Axonius either fully or partially supports 118 (31%) of these High Baseline requirements.

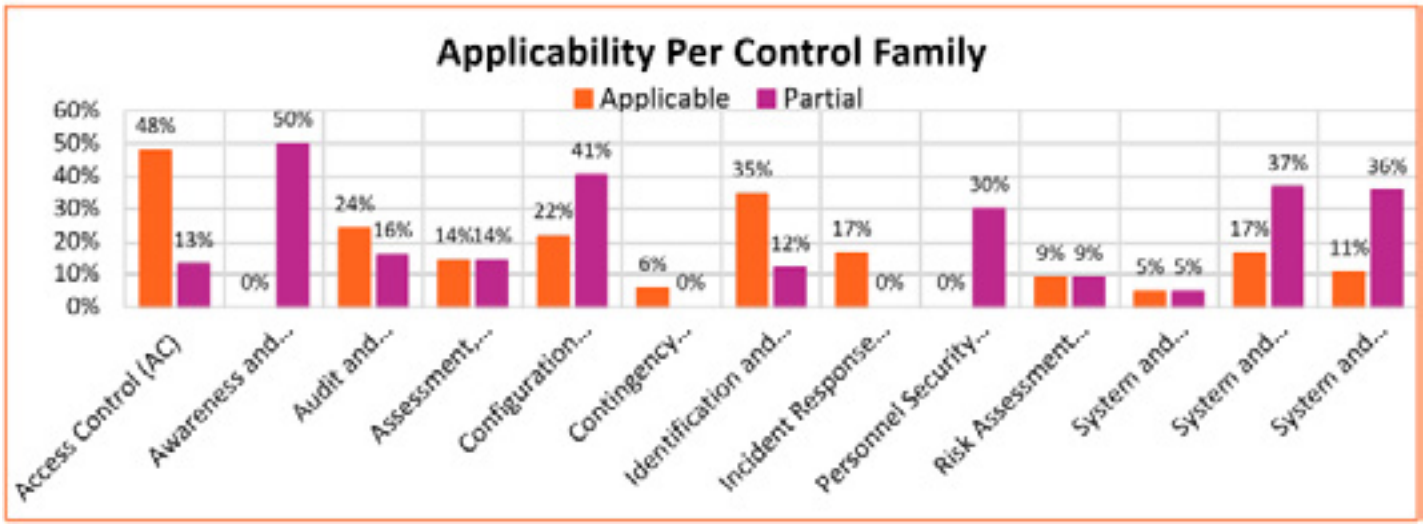


Control Summary Table

Status	Number of Controls
Full Applicability	61
Partially Applicability	57
Not Applicable	253

Axonius Capability Charts

Below is a chart showing the Axonius compliance percentages when it comes to mapping capabilities with applicable NIST 800-53 controls. Of the controls relevant to meeting NIST 800-53 compliance, fully implemented controls are marked as "Applicable" and controls that have partially been implemented are marked "Partially."



Compliance Capabilities

Below is the compliance applicability table that highlights how Axonius can help organizations meet NIST 800-53 controls.

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
AC - Access Control		
AC-2: Account Management	Axonius's adapters for identity management solutions like Active Directory, Entra ID, and Okta enable organizations to understand the full scope of accounts, devices, permissions and more. Using the Enforcement Center, organizations can also take action on accounts, such as adding/removing users from groups or assigning specific roles.	Yes
AC-2 (1): Account Management | Automated System Account Management	Axonius has adapters with identity management solutions like Microsoft Active Directory, Entra ID, and Okta to help organizations automate account management. Using the Enforcement Center, organizations can use AD and Okta to create, enable, modify, disable, and remove accounts.	Yes
AC-2 (2): Account Management | Automated System Account Management	Within identity solutions, organizations can set defined time periods for the removal of temp accounts. Axonius can help organizations conduct user access reviews by verifying if temporary and emergency accounts have been disabled or removed and if not, take the appropriate action to remove access.	Yes
AC-2 (3): Account Management | Disable Accounts	Using Axonius Workflows, organizations can deactivate or suspend users in their identity platform or HR source (e.g. Workday).	Yes
AC-2 (4): Account Management | Automated Audit Actions	Axonius provides out-of-box dashboards and a query wizard that customers can use to review account detail across their identity platforms. Auditing account management can be done via AD by enabling the "audit user account management" audit policy. User logs are generated within Axonius and can be configured with additional adapters such as Splunk to monitor account management. Capabilities include automatically auditing account creation, modification, enabling, disabling, and removal actions.	Yes

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
AC - Access Control		
AC-2 (12): Account Management | Account Monitoring for a Typical Usage	Axonius can be configured to support implemented network access monitoring, security incident and event management (SIEM), and identity and access management (IAM) solutions by sending emails or generating log events when a user attempts to access a device they typically would not require access to.	Yes
AC-2 (13): Account Management | Disable Accounts for High-Risk Individuals	Organizations using AD as an adapter within Axonius can disable accounts that prove to be of high risk within a set defined time period. The access removal would remove any user's access across all systems that have integrations with AD.	Partial
AC-3: Access Enforcement	Organizations can configure access to various adapters within Axonius via AD in conjunction with the organization's Access Control policy.	Yes
AC-4: Information Flow Enforcement	Axonius supports boundary device management interfaces, in which organizations can set information flow policies within, through adapter connections.	Yes
AC-4 (4): Information Flow Enforcement | Flow Control of Encrypted Information	Axonius has adapters for data loss prevention products such as Netskope which can help prevent encrypted information from being exfiltrated by decrypting and inspecting the information before it leaves organizational assets. Additionally, Axonius can help identify gaps in coverage and deployment of adapters.	Partial
AC-6: Least Privilege	Axonius offers various adapters for organizations to leverage when it comes to the management of least privilege. An example is CyberArk Endpoint Privilege Manager which enforces the least privilege, providing credential theft protection and application control at scale. Microsoft AD can be used for Identify and Access Management (IAM) to manage PAM (Privileged Access Management) which authenticates and authorizes users and workstations. Organizations can use Axonius to help verify members of critical groups such as Domain Administrators and monitor new entries. Axonius can help identify gaps in the coverage provided by these tools.	Yes

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
AC - Access Control		
AC-6 (1): Least Privilege | Authorize Access to Security Functions	Axonius has adapters for identity solutions such as Microsoft Active Directory, Entra ID and Okta that provide insights into account management practices. Organizations can gain insight into whether users have administrative rights while comparing the naming convention of the account (e.g., jsmith_admin vs. jsmith). Axonius Identities enables companies to build joiner, mover, leaver processes for account management, and gives companies visibility into user risks and permissions.	Yes
AC-6 (2): Least Privilege | Non-Privileged Access for Nonsecurity Functions	Axonius supports AD and Entra ID adapter connections to manage an organization's users and ensure all users are provisioned with nonprivileged accounts to manage day-to-day functionality while also ensuring those with privileged accounts use them only when necessary (e.g., accessing security functionality).	Yes
AC-6 (5): Least Privilege | Privileged Accounts	Organizations can leverage Axonius Identities to understand identity security posture, including actionable insights into MFA coverage gaps, weak access controls, excessive permissions, policy conflicts, and more to help remediate misconfigurations and exposures before they become exploits. Additionally, Axonius Identities provides recommendations for right-sizing excessive access permissions.	Yes
AC-6 (7): Least Privilege | Review of User Privileges	Axonius Identites provides recommendations for right-sizing excessive access permissions.	Yes
AC-6 (9): Least Privilege | Log Use of Privileged Functions	Axonius has various adapters for logging and monitoring, organizations can utilize Axonius to help identify gaps and add any unseen systems via the enforcement center to the logging and monitoring tool to enforce visibility. Axonius allows for integrating adapters such as Splunk for log collection. Organizations can review logs and configure alerts according to their logging and monitoring policies and procedures.	Yes

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
AC - Access Control		
AC-6 (10): Least Privilege | Prohibit Nonprivileged Users from Executing Privileged Functions	Microsoft AD can be used for Identify and Access Management (IAM) to manage PAM (Privileged Access Management) which authenticates and authorizes users and workstations. Axonius can help identify gaps and allow organizations to add any unseen systems via the enforcement center to the logging tool being used by the organization.	Yes
AC-17 (1): Remote Access | Monitoring and Control	Axonius takes a comprehensive approach to identifying user accounts and installed software for all devices in the environment simply by connecting to all the IT and security tools and organizations already in use. By connecting data sources such as EDR/EPP agents, configuration and patch management tools, network infrastructure, vulnerability scanners, and more, it's easy to quickly identify which remote access tools exist in your environment.	Yes
AC-17 (3): Remote Access | Managed Access Control Points	Axonius can be used to display all network devices that provide access to external devices. Depending on the specific device, Axonius also supports adapter connections that allow additional configuration management through the Axonius environment.	Yes
AC-17 (4): Remote Access | Privileged Commands and Access	Axonius can employ privileged access management (PAM) solutions to restrict access to remote access program execution to only those stipulated with job functions authorized by the enterprise. The following are examples of PAM adapters Axonius support: CyberArk: Provides privileged access management, session recording, and least privilege enforcement to control access to systems and applications within an enterprise/agency. BeyondTrust: Privileged management solution that allows application and system access controls to be configured based on an enterprise's needs. PrivX: Allows organizations to configure privileged access controls to on-premise and cloud environments to control sensitive or critical infrastructure.	Partial

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
AC - Access Control		
AC-18: Wireless Access	Axonius can integrate with leading network and wireless technology providers such as Cisco Meraki and Aruba Airwave to report on assets accessing wireless networks. It can also easily identify unmanaged devices that are accessing specific network interfaces. Using the Axonius Query Wizard, organizations can easily search for unknown, unmanaged, and rogue devices on specific network interfaces across the connected network infrastructure.	Yes
AC-18 (1): Wireless Access | Authentication and Encryption	Axonius integrates with leading network and wireless technology providers such as Cisco Meraki, Aruba Airwave, and Ubiquiti UniFi Controller to report on assets accessing wireless networks. It can also easily identify unmanaged devices that are accessing specific network interfaces. Using the Axonius Query Wizard, organizations can easily search for unknown, unmanaged, and rogue devices on specific network interfaces across the connected network infrastructure.	Partial
AC-18 (3): Wireless Access | Disable Wireless Networking	Organizations can manage devices connected to the wireless network via integrations such as Cisco Meraki, Aruba Airwave, and Ubiquiti Networks to control wireless access.	Yes
AC-18 (4): Wireless Access | Restrict Configuration by Users	Organizations can manage devices connected to the wireless network via integrations such as Cisco Meraki, Aruba Airwave, and Ubiquiti Networks to control wireless access.	Yes

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
AC - Access Control		
AC-19: Access Control for Mobile Devices	Axonius allows visibility into all devices managed through mobile device management (MDM) solutions while also providing direct connections to many common MDM interfaces through adapter connections. The following are a few examples of supported MDM solutions in the Axonius platform: Blackberry Unified Endpoint Management: MDM solution that delivers endpoint management and policy control for both small formfactor devices and workstations endpoints. Citrix Endpoint Management (XenMobile): Endpoint management solution that provides support for mobile device management and mobile application management. IBM MaaS 360: Unified endpoint management solution that extends to mobile devices and allows configurations for apps, content, and stored data. VMWare Workspace ONE (AirWatch): Enterprise mobility management software to manage mobile devices for content, applications, and email.	Yes
AC-19 (5): Access Control for Mobile Devices | Full Device or Container-based Encryption	Axonius has an adapter for Microsoft BitLocker Administration and Monitoring (MBAM) that provides a simplified administrative interface to implement full-device encryption through BitLocker.	Yes
AC-20: Use of External Systems	Axonius has sanitizing data features. An adapter may pull in more assets or information than an organization is comfortable with. Such examples can include devices in extraneous subnets or user fields containing potential PII. In these cases, Ingestion Rules may be an appropriate feature to limit that data in a customization way. The result is a unified approach across all adapters to simplify post-fetch filtering.	Partial
AC-21: Information Sharing	Axonius has data security integrations with platforms such as Box and Citrix Sharefile which help users make information sharing and collaboration decisions based on information classifications configured within these applications.	Yes

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
AT – Awareness Training		
AT-2: Literacy Training and Awareness	Axonius integrates with KnowBe4, a tool used to monitor users enrolled in security awareness as well as provide training and awareness from a vast library of interactive content including modules, games, newsletters, and more.	Partial
AT-2 (2): Literacy Training and Awareness | Insider Threat	While Axonius does not actively provide training on recognizing and reporting indicators of threats, the platform does support UEBA, DLP tools that can monitor, prevent, and provide alerts for potential insider threat activities.	Partial
AT-4: Training Records	Organizations using Axonius's integration with KnowBe4 and other training-related tools can retrieve training records including records such as test results, user risk score, phish prone percentage status, and training completion.	Partial
AU – Audit and Accountability		
AU-2: Event Logging	Within its list of adapters, Axonius offers Splunk which can index and correlate real-time data in a searchable repository. Other solutions such as Devo, IBM QRadar, LogRhythm, Rapid7 InsightIDR, Exabeam, and Datadog are available as well.	Partial
AU-3: Content of Audit Records	Organizations can specify the content of audit records via supported adapter connections Additionally, Axonius can identify locations that are not being monitored and assets that are not integrated with the SIEM tool.	Yes
AT-3 (1): Content of Audit Records | Additional Audit Information	Axonius has various SIEM adapters to choose from. Organizations can customize their audit record content based on organizational needs and requirements. Axonius makes it easy to create queries and search for audit-specific information as needed.	Yes
AU-6: Audit Record Review, Analysis, and Reporting	Axonius has the ability for log analysis through integrations such as Splunk. This allows the platform to identify where audit recording is not taking place.	Partial

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
AU – Audit and Accountability		
AC-7 (1): Audit Record Reduction and Report Generation | Automatic Processing	Axonius provides a wide variety of query options to search audit records for events of interest based on specified fields.	Partial
AU-8: Time Stamps	When records are generated in Axonius, they are stamped with the following data field: Last Generated - the timestamp of the last time the report was generated.	Yes
AU-9: Protection of Audit Information	Axonius Role-based Access Control (RBAC) Management can be utilized to control who has access to audit information and prevention from unauthorized access, modification, and deletion.	Yes
AU-11: Audit Record Retention	Axonius allows organizations to query back in time ("display by date") and obtain a snapshot of how the environment was configured in the past.	Yes
AC-11 (1): Audit Record Retention | Long Term Retrieval Capability	Audit records can be retrieved by the Report function. The Display by Date function allows searching for a specified period.	Yes
AU-12: Audit Record Generation	The Axonius Query Wizard can be used to filter for event types from many different information system components. Using the Report function, audit records can be generated for the event types defined in AU-2c and AU-3.	Partial

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
CA – Assessment, Authorization, and Monitoring		
CA-2: Control Assessments	Axonius can assess security controls as having an accurate and up-to-date asset inventory allows for more accurate and comprehensive security control validation. The solution integrates with all the security controls, showing how they relate to all IT assets in one central view. It can also validate whether security controls exist and are working correctly for all assets continuously.	Partial
CA-7: Continuous Monitoring	Axonius supports continuous monitoring through the pre-built adapters (third-party IT integrations). Sample adapters include Obsidian Security and ConnectWise Automate.	Partial
AC-7 (4): Continuous Monitoring | Risk Monitoring	Axonius supports risk monitoring by connecting adapters to critical sources which provide detailed information on devices, users, and cloud assets. Administrators can query to identify risks, implement risk controls, and validate against them.	Yes
CA-8: Penetration Testing	Axonius has two pre-built adapters that allow penetration testing abilities: BurpSuite and Edgescan. Organizations can leverage either adapter to meet penetration testing requirements.	Yes
CM – Configuration Management		
CM-2 (2): Baseline Configuration | Automation Support for Accuracy and Currency	Axonius provides organizations with detailed insight into their enterprise/agency devices to help maintain compliance with security configuration baselines. Devices that do not meet configuration baselines can be identified and prioritized using alerting and dashboards in the Axonius platform.	Partial
CM-2 (3): Baseline Configuration | Retention of Previous Configurations	Axonius cannot directly control a rollback of assets to previous configuration baselines; however, if those configuration baselines are retained elsewhere in an organization's systems, administrators are able to use Axonius to validate and ensure all devices on their network are rolled back effectively.	Partial

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
CM – Configuration Management		
CM-2 (7): Baseline Configuration | Configure Systems and Components for High-risk Areas	Administrators can granularly control, monitor, and manage specific IT devices within their organization's scope by using Axonius and adapters that support applicable CMDB solutions.	Partial
CM-3: Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes	While organizations may need to manage manual documentation for change control processes separately, Axonius can be used to enhance visibility and oversight during change implementation, recordkeeping, and scheduled updates. It helps enterprises more effectively manage their devices throughout the change process. Enforcement policies in Axonius can be configured to alert administrators when scheduled changes—sourced from a connected CMDB—fail on any device. This supports faster response times and provides clear evidence of successful or failed changes.	Partial
CM-3 (1): Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes	Notifications of configuration deviations can be configured within the Enforcement Center of the Axonius platform, but documentation and approval processes cannot be automated within the tool directly.	Partial
CM-3 (2): Configuration Change Control | Testing, Validation, and Documentation of Changes	The Axonius asset summary dashboards display details of applications, operating system versions, and other key configurations that can be used to validate changes to devices.	Partial
CM-4 (1): Impact Analyses | Separate Test Environments	Axonius can be used to monitor a separate test environment (whether cloud-based or on premises) and ensure it is configured appropriately for security analysis before the changes are formally made in a production environment.	Partial

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
CM – Configuration Management		
CM-4 (2): Impact Analyses | Verification of Controls	Axonius gives organizations insight into the configurations (operating systems, installed agents, connected devices) of all assets within their network perimeter, which allows for streamlined verification of changes to devices. Any misconfigured devices that do not meet expected parameters can be queried for identification and targeted remediation.	Yes
CM-5 (1): Access Restrictions for Change | Automated Access Enforcement and Audit Records	Axonius supports various adapter connections to IAM and account management tools to support access restrictions, enforcement, and documentation of actions for auditing.	Yes
CM-6: Configuration Settings	Axonius can provide verification evidence of configuration settings and changes through the visibility the asset summary dashboard offers.	Partial
CM-6 (1): Configuration Settings | Automated Management, Application, and Verification	Axonius can be configured, using the Enforcement Center, to generate automated notifications based on desired criteria (e.g., missing agents or devices that are not meeting change requirements).	Partial
CM-7: Least Functionality	By collecting and correlating asset data from multiple sources, Axonius creates a comprehensive inventory of the enterprise. This inventory can be searched to identify unauthorized or unnecessary ports, services, processes, and software running in the environment. Through the Enforcement Center, these items can be automatically disabled, removed, or flagged for administrative review and further action.	Partial

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
CM – Configuration Management		
CM-7 (1): Least Functionality | Periodic Review	Organizations can review queries and data within the Axonius environment to identify unnecessary or nonsecure functions, ports, protocols, installed software, or services. Once detected, it is the organization's responsibility—using their chosen tools—to remove any unnecessary or insecure functionality. Axonius can then be used to verify that these components have been successfully removed.	Partial
CM-7 (2): Least Functionality | Prevent Program Execution	Axonius can ensure applications to prevent unwanted program execution, such as VMware Carbon Black App Control (formerly Carbon Black CB Protection), are installed on all devices but the platform cannot directly determine what programs to exclude. This would require manual configurations in the chosen solution to fully meet implementation compliance.	Partial
CM-8: System Component Inventory	Axonius provides a single point of reference for a network inventory to include what is installed on each asset. By using multiple sources and the ability to use WMI for data enrichment, Axonius guarantees the most accurate inventory available, which is easy to query and generate reports with.	Yes
CM-8 (1): System Component Inventory | Updates During Installation and Removal	Axonius generates a full asset inventory with each data pull, ensuring the component inventory is always up to date. It also allows users to compare the current inventory with any previous snapshot for change tracking and analysis.	Yes
CM-8 (2): System Component Inventory | Automated Maintenance	By connecting to multiple security and management tools in the environment, Axonius can provide the single source of truth for an up-to-date component inventory, including details on machines that may be temporarily unavailable.	Yes
CM-8 (3): System Component Inventory | Automated Unauthorized Component Detection	Notifications can be configured through the Enforcement Center to alert administrators when software that is not part of the configured baseline is installed on any device within an organization's network.	Yes

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
CM – Configuration Management		
CM-11: User-Installed Software	Using the Axonius Query Wizard, admins can search by software name, version, or description. A simple way to find unsanctioned software is to reference unsanctioned software-defined percompany/agency policy. Peer to Peer Networks: Tor, Torrent, TikTok, WeChat, PopcornTime Cracking Tools: AirCrack, L0phtcrack, Brutus Protocol Analysis Tools: winpcap, Wireshark, mergcap, mergecap, npcap Vulnerability mapping and pentest tools: dsniff, Metasploit, Nessus, Nikto, nmap Cryptocurrency Wallets and Miners: btcminer, bfgminer, cgminer Gaming: Pokerstars, Discord, Steam, etc. Native applications that can be used for malicious purposes: Nmap, mimikatz, dsniff, Wireshark, Metasploit Keyloggers / Password crackers: davegrohl Remote Access Tools (RATs): Poison Ivy, Sakula, KjWorm, Havex, Dark Comet, AlienSpy Unsanctioned IT & Security tools: any unsanctioned platforms including VPN, Antivirus, Cloud storage, and more.	Yes
CM-12 (1): Information Location | Automated Tools to Support Information Location	Axonius can support information location by tracking deployed asset location in the asset's detail record and ensuring that tracking agents are installed on all deployed devices.	Partial

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
CP - Contingency Planning		
CP-2: Contingency Plan	Axonius helps secure and recover assets that are in scope for organizations. Although Axonius doesn't create specific contingency plans, it can track assets in scope which will lead to efficiency in recovery of those same assets, if needed. Commvault enables data protection, backup and recovery, and information management solutions. Dell EMC Avamar is a backup and recovery solution that enables daily backups of physical and virtual environments, NAS servers, enterprise applications, remote offices, and desktops/laptops. Zerto is a data loss protection solution that provides disaster recovery, backup, and workload mobility software for virtualized infrastructures and environments. Nutanix AHV is a hypervisor included with the Enterprise Cloud OS. AHV delivers flexible migrations, security hardening, automated data protection and disaster recovery, and analytics. Rubrik provides data security and data protection on a single platform, including Zero Trust Data Protection, ransomware investigation, incident containment, sensitive data discovery, and orchestrated application recovery.	Yes
CP-9: System Backup	Axonius integrates with the CommVault data backup solution. CommVault enables data protection, backup and recovery, and information management solutions. It provides end-to-end encryption, including data-at-rest and data-in-flight encryption, to ensure data is secure.	Yes
IA – Identification and Authentication		
IA-2: Identification and Authentication (Organizational Users)	Once Axonius is deployed, adapters like Microsoft AD can be integrated to manage users, groups, and monitor account activity across the organization. The Enforcement Center can support security policies from applicable adapters, such as Okta, to manage MFA. SAML login is used to authenticate users. AD consists of remote and wireless accesses.	Yes

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
IA – Identification and Authentication		
IA-2 (1): Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts	Axonius provides visibility into privileged user accounts that an organization may have. Organizations can leverage Axonius's capability via connecting to identity and access management tools like Okta, Duo, Ping Identity, and more to implement multifactor authentication for access to privileged accounts. Sample adapter: BeyondTrust Privileged Identity.	Yes
IA-2 (2): Identification and Authentication (Organizational Users) | Multifactor Authentication to Nonprivileged Accounts	Organizations can obtain user account data via Axonius. Axonius offers visibility into user data including but not limited to usernames, user titles, user managers, user departments, MFA enrollment, and MFA enforcement. The user department section can help identify domain ownership distinguishing between privileged and non-privileged accounts. Axonius can connect to identity and access management tools like Okta, Duo, Ping Identity, and more to implement multifactor authentication for access to nonprivileged accounts.	Yes
IA-3: Device Identification and Authentication	Axonius identifies interconnected devices via device descriptions and details. Axonius offers the ability to uniquely identify and authenticate devices based on different scenarios: 1. Through exact hostnames, if the device entity does not have any MAC or IP address. 2. With ServiceNow adapter, based on MAC address only. 3. If enabled, Axonius only correlates assets from Microsoft Azure AD adapter connection based on asset name. If disabled, Axonius correlates assets from Azure AD adapter connection based on several parameters such as MAC address, hostname, and others.	Partial
IA-4: Identifier Management	Organizations deploying Axonius can identify and assign identifiers pertaining to individuals, groups, roles, and devices used within the organization. Organizations can use adapters such as Microsoft AD to facilitate this.	Yes

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
IA – Identification and Authentication		
IA-4 (4): Identifier Management | Identify User Status	Axonius has pre-built adapters for directory services such as Microsoft AD and Okta where user status can be queried. For example, in the Axonius AD adapter, users can be identified using specific fields that indicate whether they are contractors or external (non-organizational) users.	Yes
IA-5: Authenticator Management	By connecting Axonius to account management and IAM tools like AD or Okta, organizations can enforce authentication requirements across their environment. This ensures that all authenticators meet the strength and security standards defined by organizational policy. Physical authenticators cannot be token-based authentication and passwords can be configured through these adapters.	Partial
IA-5 (1): Authentication Management | Password-based Authentication	Organizations using Axonius can utilize various adapters for authentication management. The Password Policy Settings address password complexity, brute-forced protection, expiration settings, and more. Enterprise Password Management vaults like AWS Secrets Manager, Cyberark, and BeyondTrust Privileged Identity are available for storing and securing passwords.	Partial
IA-5 (2): Authenticator Management | Public Keybased Authentication	DigiCert CertCentral consolidates tasks for issuing, installing, inspecting, remediating, and renewing certificates. DigiCert PKI Platform (formerly Symantec Managed PKI) provides a cloud-based enterprise solution for issuing and managing digital certificates used to enable strong authentication and encryption. Venafi secures and protects cryptographic keys and digital certificates.	Yes
IA-7: Cryptographic Module Authentication	Axonius has been added to the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Program Approved Products List (APL) and has received the Cryptographic Algorithm Validation Program (CAVP) certification for its product's use of the OpenSSL FIPS Object Module. Additional details can be found here.	Yes

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
IA – Identification and Authentication		
IA-8: Identification and Authentication (non-organizational Users)	Axonius can help identify users accessing systems who are not listed in the organization's user directories, such as Microsoft AD or Okta. AD allows organizations to manage users, groups, and monitor accounts—including guest or non-organizational users. Using LDAP connections and the Axonius Enforcement Center, organizations can manage multi-factor authentication (MFA) and AD access through Okta. User authentication is handled via SAML login.	Yes
IA-11: Reauthentication	Axonius supports adapter connections to Active Directory for configuring authentication policies, along with a wide range of identity and access management (IAM) solutions such as Okta, Keycloak, PingOne, and SailPoint. Organizations can define device locks and re-authentication of individuals via adapters.	Yes
IR – Incident Response		
IR-4 (4): Incident Handling | Information Correlation	Axonius integrates with tools like WMI or OSQuery, which can be exceptionally useful by looking for services, local accounts, processes, or other artifacts across the enterprise that are related to an incident. Other adapters include: Code42: a next-gen DLP solution used to detect insider threats, satisfy regulatory compliance, and accelerate incident response investigations. Proofpoint ObserveIT Insider Threat Management (ITM) platform: a cloud-based solution that provides insider risk detection, incident response, and unified visibility across user activity, data interaction, and threat context. VMware Carbon Black EDR (formerly Carbon Black CB Response): a threat hunting and incident response solution that delivers continuous visibility in offline, air-gapped, and disconnected environments using threat intel and customizable detections. Wazuh: an open-source and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response, and compliance.	Yes

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
IR – Incident Response		
IR-7: Incident Response Assistance	Organizations using Axonius can utilize Axonius to help prepare, identify, and contain incidents. Axonius can creating dashboards identifying critical data points to use in incident response. The enforcement center allows organizations to use existing tools to isolate target devices with Carbon Black, Crowdstike and others. If the investigation is user based, creating and using an incident response dashboard chart will allow identification. Additional information can be found here: Incident Response User Dashboards	Yes
IR-7 (1): Incident Response Assistance | Automation Support for Availability of Information and Support	Organizations can use Axonius to support the preparation, identification, and containment of security incidents. It offers customizable dashboards that highlight critical data points relevant to incident response teams. Through the Enforcement Center, Axonius integrates with tools like Carbon Black, CrowdStrike, and others, enabling teams to isolate affected devices quickly. If the investigation is user-focused, incident response dashboards and charts can be used to identify and track user-related activity.	Yes
PS – Personnel Security		
PS-4: Personnel Termination	Axonius integrates with HR software such as ADP and BambooHR, which can be used to verify if the access privileges of terminated personnel has been revoked across the environment.	Partial
PS-4 (2): Personnel Termination | Automated Actions	Axonius integrates with HR software such as ADP and BambooHR, which can be used to verify if the access privileges of terminated personnel has been revoked across the environment.	Partial
PS-5: Personnel Transfer	Axonius can integrate with various Human Resources Information Systems (HRIS) and Identity Management (IDM) systems that facilitate employee transfer protocols. This data can then be compared to other sources to ensure completeness and validate current access across the network. Enforcements can be used to automatically add or remove users from specific Active Directory groups, ensuring they have appropriate access based on attributes like their division or job title.	Partial

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
RA – Risk Assessment		
RA-5: Vulnerability Monitoring and Scanning	Axonius provides users the ability to understand the presence and impact of all observed vulnerabilities. Organizations can manage vulnerabilities across the fleet of devices, prioritize vulnerabilities via contextual device data, enriched data from external threat databases, and third-party threat intelligence, to better understand and assess the urgency, relevancy, and importance of security weaknesses. Axonius integrates with various vulnerability scanning/ management tools to help organizations find and remediate applications or assets at risk. Axonius identifies gaps in coverage related to Vulnerability scanning. It also pulls CVEs from NIST as another source to verify the results of the vulnerability scanner.	Partial
RA-5 (2): Vulnerability Monitoring and Scanning | Update Vulnerabilities to be Scanned	Axonius pulls vulnerability information from multiple sources allowing verification that an organization's vulnerability monitoring platform is current with the latest vulnerabilities.	Yes
SA – System and Services Acquisition		
SA-16: Developer-Provided Training	Axonius provides general security awareness training, social engineering, phishing awareness, and threat simulations for employees by correlating with tools such as KnowBe4 and Cofense PhishMe.	Yes
SA-22: Unsupported System Components	Within the Axonius dashboard, metrics are displayed for operating system versions, software versions installed on systems, and more, helping organizations understand what system components may be unsupported.	Partial

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
SC – System and Communications Protection		
SC-2: Separation of System and User Functionality	Axonius allows organizations to leverage Data Scope Management. Organizations can use data scopes to control the sets of data different groups of users have access to. After defining a data set using special asset scope saved queries, the organization can assign that scope to a role and then assign users to that role to control access accordingly. This enables groups of users to see only data that is relevant to them or that they are allowed to see.	Yes
SC-3: Security Function	To protect the integrity of the hardware, software, and firmware that performs security functions, organizations can combine Axonius with a tool like Eclypsium_adapter which can identify where protections are not in place. The tool can be used to ensure that hardware is not being modified.	Partial
SC-5: Denial-of-Service Protection	Axonius adapters allow agencies to manage their boundary protection devices (e.g., firewall, web-application firewall), update IDS/IPS to filter DoS or volumetrics traffic, or manage cloud-based protection if they are using a cloud service provider such as Cloudflare, AWS Shield, or Azure. Within the firewall rules, organizations can allow/deny access, view the direction of users' movements (i.e., ingress, egress), targets, and protocols.	Partial
SC-7: Boundary Protection	Axonius integrates with various firewall solutions: Check Point Infinity: protects against cyber threats across networks, endpoint, cloud, and mobile devices. This adapter supports the entire Infinity platform, including Check Point firewalls. Fortinet FortiGate:a next-generation firewall providing security and visibility for end-to-end protection across the entire network. Skybox Firewall Assurance: provides automation of firewall management tasks across different firewall vendors and complex rulesets. Tufin SecureTrack:a firewall management solution that delivers security, compliance, and connectivity across physical networks and hybrid cloud.	Partial

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
SC – System and Communications Protection		
SC-7 (5): Boundary Protection | Deny by Default – Allow by Exception	Organizations can use Axonius supported adapters to connect to their firewall management platforms and update configurations - including the deny all, allow by default rules. Axonius can show cloud configurations and the firewall rules being utilized.	Partial
SC-7 (8): Boundary Protection | Route Traffic to Authenticated Proxy Servers	Organizations can view firewall rules for cloud based devices to identify traffic routes (ingress or egress) and if the traffic is being allowed or denied.	Partial
SC-7 (21): Boundary Protection | Isolation of System Components	Axonius supports various firewall adapter connections to allow information flow configuration management through portals supported through adapters.	Partial
SC-8: Transmission Confidentiality and Integrity	Axonius supports various adapters to manage DLP configurations, including encryption, for an enterprise's/agency's assets: Symantec DLP: central interface to manage DLP configurations and enforced policies to reduce information leakage risks. Also supports reporting and IT analytics. PKWARE: monitors and remediates all instances of unprotected data traversing an organization's network.	Yes
SC-10: Network Disconnect	While organizations can set time periods of inactivity, Axonius can help identify and pass information to a SOAR such as Swimlane, Phantom, and XSOAR.	Partial

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
SC – System and Communications Protection		
SC-12: Cryptographic Key Establishment and Management	Axonius does not support adapters that provide full coverage for an organization's encryption key management; however, some adapter connections do support encryption key management within their interface: KeyCloak: open-source identity brokering service that provides an administrative console to manage applicable encryption key life cycles within. Venafi: SaaS-based encryption key and certificate management solution for mixed IT environments. Symantec Endpoint Encryption: organizations can manage full-disk and removable media encryption policies on their endpoint devices through a centralized management platform.	Partial
SC-13: Cryptographic Protection	Once an organization has formally defined its cryptographic requirements, Axonius can help ensure compliance by leveraging its supported adapters. These adapters can verify that encryption is properly implemented across areas such as data loss prevention (DLP), backup encryption settings, and endpoint encryption solutions, in line with organizational policy and key management solutions. BitLocker Administration and Monitoring: provides a simplified administrative interface for organizations to manage BitLocker Drive Encryption, Symantec Endpoint Encryption: combines full-disk and removable media encryption with a centralized management interface to protect sensitive information and ensure compliance.	Partial
SC-17: Public Key Infrastructure Certificates	Organizations can consolidate and manage their public key certificates using the following adapter connections: Digicert CertCentral: management platform for issuing, installing, inspecting, remediating, and renewing an organization's certificates. Venafi: SaaS-based encryption key and certificate management solution for mixed IT environments.	Yes

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
SC – System and Communications Protection		
SC-20: Secure Name/ Address Resolution Service (Authoritative Source)	Axonius supports adapter connections to several DNS security management services and shows gaps in coverage in the tools below: Cisco Umbrella: secure internet gateway that provides DNS and IP layer enforcement and control callback blocking. Men&Mice DNS Management: network management software allowing DNS security configurations across an enterprise. Cloudflare DNS: centralized management platform where DNS filtering can be configured if using Cloudflare products or infrastructure. BlueCat Enterprise DNS: centralized management platform to connect assets and manage DNS filtering services on those assets. DNS Made Easy: DNS management services and tools to provide traffic management solutions to organizations.	Partial
SC-23: Session Authenticity	Axonius cannot directly ensure session authenticity across an enterprise/agency, but organizations can use supported adapters for firewall management, Active Directory Group Policy configurations, applicable remote conferencing settings, and applicable email security services to prove compliance.	Partial
SC-28: Protection of Information at Rest	Axonius supports adapter connections to various encryption management solutions organizations can use to validate that their systems are encrypted according to configured policies. BitLocker Administration and Monitoring: provides a simplified administrative interface for organizations to manage BitLocker Drive Encryption Symantec Endpoint Encryption: combines full-disk and removable media encryption with a centralized management interface to protect sensitive information and ensure compliance.	Yes
SC-28 (1): Protection of Information at Rest | Cryptographic Protection	Axonius supports adapter connections to various encryption management solutions organizations can use to validate that their systems are encrypted according to their configured policies. BitLocker Administration and Monitoring: provides a simplified administrative interface for organizations to manage BitLocker Drive Encryption Symantec Endpoint Encryption: combines full-disk and removable media encryption with a centralized management interface to protect sensitive information and ensure compliance.	Yes

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
SI – System and Information Security		
SI-2: Flaw Remediation	Axonius offers the Query Wizard to identify outdated systems. Fortify Software Security Center offers security assurance solutions that address the threats posed by security flaws in business-critical software applications.	Partial
SI-2 (2): Flaw Remediation | Automated Flaw Remediation Status	Enforcements can be created to automate this process based on a number of factors, such as data from the vulnerability scans, SCCM, or CVE checks. Axonius provides an additional layer of verification that an organization's flaw remediation process is working.	Partial
SI-3: Malicious Code Protection	Axonius helps identify gaps in the coverage of an organization's malicious code protection tools, whether they are host-based or network-based. This visibility ensures that no devices are left unprotected, regardless of the tools in use.	Partial

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
SI – System and Information Security		
SI-4: System Monitoring	For system monitoring, Axonius shows gaps in coverage and can take enforcement actions to resolve those gaps. Axonius offers the following solutions for system monitoring: Contrast Security: protects software applications against cyberattacks. CrowdStrike Falcon: delivers nextgeneration antivirus, endpoint detection and response (EDR), managed threat hunting, and threat intelligence. Cybereason Deep Detect & Respond (EDR): defends against advanced attacks by collecting and analyzing behavioral data to identify suspicious activities. CyCognito: delivers proactive attack surface and digital risk protection across the entire extended IT ecosystem to help organizations identify, categorize, prioritize, and eliminate attacker-exposed risk. Darktrace Immune System: protects the workforce and data from sophisticated attackers by detecting, investigating, and responding to cyber-threats. Endgame: an endpoint protection platform that combines online and offline protection against exploits, phishing, malware, ransomware, and fileless attacks. Heimdal Security: protects organizations and home users against malware attacks. Palo Alto Networks Cortex XDR: a detection and response app that natively integrates network, endpoint, and cloud data to detect threats and stop sophisticated attacks. Palo Alto Traps Endpoint Security Manager (ESM): delivers endpoint protection to prevent advanced persistent threats (APTs) and zeroday attacks.	Partial
SI-4 (2): System Monitoring | Automated Tools and Mechanisms for Real-Time	Axonius supports adapter connections to many SIEM and network monitoring tools and is displayed through the dashboard function to assure all devices are being monitored.	Partial

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
SI – System and Information Security		
SI-4 (4): System Monitoring | Inbound and Outbound Communications Traffic	Axonius allows the integration of solutions that monitor network activities which includes setting predefined criteria for abnormal activities or conditions. Sample adapters include: ConnectWise Automate: monitors, manages, and supports client networks via out-of-the-box scripts, continuous monitoring, and automation capabilities. Awake Security: a network traffic analysis solution that's capable of detecting and visualizing behavioral, malintent, and compliance incidents. Cisco Stealthwatch: an agentless malware detection solution that provides visibility and network traffic security analytics across the extended network, including endpoints, branches, data centers, and cloud environments.	Yes
SI-4 (14): System Monitoring | Wireless Intrusion Detection	Axonius supports adapters for network access control (NAC) solutions to allow enterprises/agencies to identify devices within their environment, enforce security policies, and remediate threats. Additionally, dashboards can be configured on the Axonius platform to display any rogue device that was not deployed with an organization's typical software or agents.	Yes
SI-4 (20): System Monitoring | Privileged Users	Axonius supports adapter connections to AD, Azure AD, and many IAM solutions to gather data on an organization's users. This data can be viewed or queried within the 'Users' tab in the Axonius platform. By employing filters, specific queries, or applicable adapter connections to monitoring solutions, organizations can create dashboards that display privileged users, devices accessed by these privileged users, and other details that would support additional monitoring capabilities.	Yes
SI-4 (22): System Monitoring | Unauthorized Network Services	Some application-level controls can be employed to restrict network traffic. For example, Axonius allows direct access to firewall management interfaces, such as Palo Alto Networks. Palo Alto management software allows organizations to restrict unauthorized network services, such as Tor, by configuring security policies to block certain applications, denying self-signed certificates, blocking risky URL categories, blocking unknown applications, or managing a source and destination IP list that restricts where traffic is allowed to ingress from or egress to.	Partial

VERSION	AXONIUS CAPABILITY	SUPPORTS COMPIANCE
SI – System and Information Security		
SI-5: Security Alerts, Advisories, and Directives	Axonius supports adapter connections to external security monitoring and alerting services such as BitSight, BinaryEdge, and UpGuard, which can be used to generate internal alerts for organizations. For example, Axonius can automate the intake of results from known exploited vulnerabilities and displaying the results for the environment. Axonius can also streamline identifying gaps in executive OMB orders such as but not limited to: EO-M-21-31, EO - 14028, and NDAA 889.	Partial
SI-7: Software, Firmware, and Information Integrity	Organizations can track their employed integrity verification tools and use Axonius to ensure all assets within the organization have the expected coverage. Some integrity checking tools supported by Axonius include: VMware Carbon Black App Control (formerly Carbon Black CB Protection): protects critical systems and servers to prevent unwanted changes and ensure continuous compliance with regulatory mandates. Eclypsium: protects the foundation of computing infrastructure, controlling risks and stopping threats to enterprise firmware and hardware devices.	Partial
SI-8: Spam Protection	Axonius allows integration of Proofpoint, which offers threat protection from targeting email, mobile, social, cloud, and other digital channels. Proofpoint Targeted Attack Protection (TAP). Axonius can also show gaps in coverage of these tools.	Partial
SI-12: Information Management and Retention	Axonius saves historically collected data which can be used in the dashboard and in the Devices and Users pages to show insights. Information within the system can be retained through lifecycle settings where historical snapshot data can be taken and saved for a defined number of days.	Partial