SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT ON MANAGEMENT'S ASSERTION RELATED TO ITS

AEM Sferic, Lightning Network and Elements 360 Platforms

Relevant to Security, Availability, and Confidentiality

For the period August 27, 2025 to November 27, 2025

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Prepared by:

Sensiba

Table of Contents

1. Independent Service Auditors' Report

To the Management of Advanced Environmental Monitoring (AEM) (AEM)

Scope

We have examined AEM's accompanying assertion titled "Assertion of AEM Management" (assertion) that the controls within AEM's Sferic, Lightning Network and Elements 360 Platforms (system) were effective throughout the period August 27, 2025 to November 27, 2025, to provide reasonable assurance that AEM's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA*, Trust Services Criteria.*

Service Organization's Responsibilities

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

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

Our examination included:

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

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

Inherent Limitations

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements 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 AEM's Sferic, Lightning Network and Elements 360 Platforms were effective throughout the period August 27, 2025 to November 27, 2025, to provide reasonable assurance that AEM's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

San Jose, California
January 26, 2026

2. Assertion of AEM Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Advanced Environmental Monitoring (AEM) (AEM) Sferic, Lightning Network and Elements 360 Platforms (system) throughout the period August 27, 2025 to November 27, 2025, to provide reasonable assurance that AEM's service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of AEM's Sferic, Lightning Network and Elements 360 Platforms," (description) 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 August 27, 2025 to November 27, 2025, to provide reasonable assurance that AEM's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022)* in AICPA*, Trust Services Criteria.*

AEM's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description.

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 August 27, 2025 to November 27, 2025, to provide reasonable assurance that AEM's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by Advanced Environmental Monitoring (AEM) Management

January 26, 2026

3. Description of AEM's Sferic, Lightning Network and Elements 360 Platforms

Company Background

Advanced Environmental Monitoring (AEM) is a leading provider of innovative environmental monitoring solutions designed to deliver critical insights that help protect people, communities, and infrastructure from environmental risks. Headquartered in the United States and operating globally, AEM integrates cutting-edge technology with robust data analytics to provide reliable, real-time environmental intelligence.

The company offers a comprehensive portfolio of monitoring systems, software platforms, and decision-support tools for a wide range of applications, including weather forecasting, air and water quality, lightning detection, hazardous thunderstorms, flood prediction & warning, wildfire detection & monitoring, and other environmental or weather-related hazards. AEM's solutions are deployed across various sectors, including government agencies (national/federal, state/provincial and local municipalities), energy & utilities, transportation, mining, agriculture, and emergency management organizations.

Through a family of specialized brands and subsidiaries, AEM combines decades of domain expertise with state-of-the-art Internet of Things (IoT) technologies and cloud-based platforms to enable high-fidelity environmental data collection, analysis, and visualization. Its mission is to empower customers with actionable environmental intelligence to make informed decisions that protect lives, optimize operations, and increase resilience in the face of growing environmental challenges.

AEM is committed to maintaining the highest standards of security, privacy, and operational integrity, aligning with SOC 2 principles to ensure the security, confidentiality, availability, and integrity of its systems and customer data.

Services Provided

AEM offers a comprehensive suite of environmental monitoring services and solutions designed to provide real-time data and actionable insights for managing environmental risks. These services support organizations in sectors such as agriculture, energy, transportation, emergency management, and government.

AEM's platforms integrate hardware, software, and professional services to deliver end-to-end multi-hazard monitoring and decision support capabilities, including:

- Design services: AEM provides design services related to communications networks, early warning systems, and other solution design or consultation services associated with ensuring the integration of hardware, software and services will satisfy the needs of our customers.
- Deployment and management of environmental sensor networks: AEM installs and operates intelligent sensing networks that collect data on various environmental parameters.
- Data integration and analysis: The Sferic and AEM Elements® 360 applications consolidate data from diverse sources, including in-house and proprietary networks, to provide a unified view of environmental hazards.
- Automated alerting and notifications: The Sferic and AEM Elements® 360 applications deliver real-time alerts based on customizable thresholds, enabling prompt responses to environmental events.
- Visualization and reporting tools: AEM provides dashboards, maps, and reports that offer insights into environmental conditions and trends.
- Professional services: AEM offers meteorological consulting, field services, and training to support the implementation and maintenance of monitoring systems.

Information is disseminated to users through secure channels, including web portals, APIs, and mobile applications, ensuring timely access to critical environmental data.

Principal Service Commitments and System Requirements

AEM has developed its operational processes and procedures to align with its objectives for delivering high-quality environmental monitoring services. These objectives are informed by the service commitments AEM makes to its clients, the legal and regulatory frameworks governing its services, and the internal financial, operational, and compliance standards established by the organization.

AEM's services are subject to the security and privacy requirements of applicable laws and regulations in the jurisdictions where it operates.

Security commitments to clients are clearly documented and communicated through Service Level Agreements (SLAs), customer contracts, and detailed service descriptions available online. These commitments are standardized and encompass, but are not limited to, the following:

- Incorporation of security principles into the core design of AEM's platforms, ensuring that system users have access to necessary information based on their roles while restricting access to non-essential data.
- Implementation of encryption technologies to safeguard customer data both at rest and during transmission.

To support the fulfillment of these security commitments, as well as to comply with relevant laws and regulations, AEM has established comprehensive operational requirements. These requirements are communicated through AEM's policies and procedures, system design documentation, and customer contracts. The organization's information security policies outline a holistic approach to protecting systems and data, covering aspects such as service design and development, system operation, management of internal business systems and networks, and employee recruitment and training. Additionally, standard operating procedures have been documented to guide the execution of specific manual and automated processes essential to the operation and development of AEM's platforms.

AEM's SOC 2 audit scope includes the following products:

- Elements 360 - Elements 360 is AEM's decision support application designed to help agencies, businesses, and communities prepare for, monitor, detect, and respond to a wide array of natural hazards. It delivers a combination of historical, real-time, and forecast weather data, providing a comprehensive view of environmental risks. The application supports optimized decision-making through customizable dashboards, automated alerting, and seamless data integration.
- Sferic Products - The Sferic products encompass tools such as Sferic Maps® and Sferic Siren, which provide real-time weather visualization, alerting, and decision support. These tools integrate data from various sources to deliver timely and accurate weather information and alerts, aiding customers in operational decision-making and safety protocols.
- Lightning Network Products: AEM's Lightning products include Lightning API and Network Manager. The Lightning API delivers near real time lightning data via REST APIs, Web Sockets, and/or TCP/IP Sockets from the Earth Networks Total Lightning Network (ENTLN) or a Private Lightning Network using AEM's software. The Network Manager provides performance details about the lightning sensors that power the network.

Through these product lines, AEM commits to delivering reliable, secure, and compliant environmental monitoring services that meet the needs of its user entities.

Components of the System

Infrastructure

Primary Infrastructure		
Hardware	Type	Purpose
AWS	EC2	AEM utilizes EC2 to host and manage its environmental monitoring platforms, including the Sferic product line, Lightning Network product line, and Elements 360. By leveraging EC2's secure and scalable infrastructure, AEM ensures high availability and performance of its services, accommodating varying workloads and user demands.
AWS	S3	AEM utilizes Amazon S3 to store and manage data associated with its environmental monitoring platforms.
AWS	Various Database Services	AEM also utilizes various AWS database services, such as Amazon RDS and DynamoDB, to securely store, manage, and retrieve structured and unstructured data at scale, ensuring high availability, performance, and data integrity across its platforms.
AWS	Other Cloud Services: Identity Management, VPC, Load Balancers, Elastic IP, DNS management, etc.	AEM uses a suite of AWS infrastructure services to support secure, scalable, and resilient operations. IAM ensures only authorized personnel access cloud resources, while VPC provides a private, controlled networking environment. ELB enhances availability by distributing traffic across systems, Elastic IPs support rapid failover, and Route 53 ensures fast, reliable DNS routing to AEM's applications.
Computers	Laptops	AEM employee computers are configured with standardized security controls, including full-disk encryption, endpoint protection, and automatic software updates, ensuring secure access to company systems and safeguarding sensitive data across all workstations.

Software

Primary Infrastructure	
Software	Purpose
Microsoft 365	Office suite and collaboration tools.
Microsoft Entra ID	Identity management
Microsoft Defender	Endpoint protection & vulnerability management

Primary Infrastructure	
Software	Purpose
Microsoft Intune	Endpoint management
NetSuite	ERP system supporting Operations and Finance functions.
Salesforce	CRM system supporting Sales and Go-To-Market functions.
Celigo	Applications integration platform as a service.
Paylocity	Payroll and human resources information management system.
Jira	Project Management
Confluence	Engineering documents management
GitHub	Source code management system
AWS Inspector	Vulnerability management
GuardDuty	Security application used for automated intrusion detection (IDS)
Arctic Wolf	Managed Detection and Response

People

AEM has established a robust organizational structure that aligns each business function with its strategic objectives and operational responsibilities. The workforce is organized across several key departments, each of which contributes to the secure, reliable, and compliant operation of AEM's services and platforms. These departments are described below:

Operations

The Operations team at AEM is responsible for the core activities that support product delivery, service continuity, and quality outcomes. This team includes the following functional areas:

- Manufacturing: Responsible for the assembly and production of AEM's hardware products in accordance with defined quality and safety standards.
- Supply Chain: Oversees the procurement, inventory, logistics, and vendor coordination required to ensure timely delivery of parts and products.
- Meteorological Operations: Manages AEM's weather-focused services and data, including environmental monitoring and forecasting operations.
- Quality Management: Develops and enforces the quality management system framework to ensure organizational processes consistently meet quality standards.

These functions collectively ensure that AEM delivers reliable solutions to customers while maintaining operational excellence and compliance with relevant standards.

Commercial Group

The Sales and Marketing organization drives customer acquisition, market presence, and product positioning. The department includes:

- Sales & Business Development: Manages relationships with existing customer base, identifies and engages with prospective clients, expanding AEM's customer base and revenue opportunities.
- Sales Engineering: Provides technical expertise and solution configuration support throughout the sales process.
- Product Management: Owns the lifecycle of AEM's products, aligning features and enhancements with customer and market needs.
- Channel Management: Manages relationships with resellers, distributors, and strategic partners.
- Marketing: Oversees branding, demand generation, communications, and go-to-market strategy.

This group plays a central role in promoting AEM's mission and delivering solutions to global markets.

Technical Services

Technical Services at AEM encompasses all customer-facing support and post-deployment functions, ensuring seamless customer experiences and effective field service operations. Core teams include:

- Customer Support: Provides frontline assistance to customers, addressing product inquiries, troubleshooting issues, and resolving technical concerns.
- Field Services: Manages on-site installation, maintenance, and repair of AEM equipment, ensuring operational uptime and customer satisfaction.
- Project Management: Oversees the planning, execution, and delivery of customer and internal projects, ensuring alignment with scope, time, and quality expectations.
- Customer Success Management: Partners with customers to ensure they realize full value from AEM's solutions, fostering long-term relationships and retention.

Engineering

AEM's Engineering organization is responsible for the design, development, and innovation behind its products and services. The department includes:

- Hardware Engineering: Designs and validates electronic and mechanical components of AEM products.

- Software Development: Builds and maintains the software systems that power AEM's platforms and customer interfaces.
- Firmware Engineering: Develops embedded software to control and enhance hardware performance.
- Research & Development: Explores new technologies and methodologies to advance AEM's offerings and maintain a competitive edge.

This group plays a pivotal role in ensuring the continued evolution and reliability of AEM's technology ecosystem.

Information Technology & Security

The IT and Security department maintains the infrastructure, applications, and controls required to safeguard AEM's information systems and ensure operational resilience. This includes:

- IT Operations: Manages internal systems, user support, and network administration.
- Cloud Infrastructure & Operations: Oversees the provisioning, deployment, and monitoring of cloud-based services supporting AEM platforms.
- Enterprise Applications: Maintains and supports the suite of internal business applications, including ERP, CRM, and HR systems.
- Information Security: Develops and enforces policies and technical controls to protect data integrity, confidentiality, and availability across AEM's systems.

These teams ensure that AEM's technology landscape adheres to high standards of security, scalability, and compliance.

Human Resources

Human Resources (HR) at AEM provides comprehensive personnel and organizational support, helping to attract, retain, and develop talent. The HR team oversees:

- HR Management: Recruitment, performance management, and employee relations.
- Payroll: Administration of compensation processes and compliance with labor regulations.
- Benefits Management: Design and delivery of employee benefits programs, including healthcare, retirement, and wellness offerings.

HR ensures that AEM maintains a motivated and compliant workforce aligned with its corporate values.

Finance

The Finance department is responsible for financial stewardship, compliance, and internal controls. It includes:

- Accounting: Oversees financial reporting, audits, and general ledger maintenance.
- Treasury Management: Manages cash flow, banking relationships, and liquidity planning.
- Accounts Payable: Ensures timely and accurate payment of obligations and vendor invoices.

This function provides critical oversight of AEM's fiscal health and supports data-driven decision-making across the business.

This functional structure ensures that AEM's operational and control environment supports the Trust Services Criteria for security, availability, processing integrity, confidentiality, and privacy - critical pillars of the SOC 2 framework.

Data

At AEM, data is a critical asset underpinning the delivery of environmental intelligence, operational services, and customer value. AEM collects, processes, stores, and transmits various categories of data to support its solutions across environmental monitoring, forecasting, analytics, and transportation services. Data includes all digital records managed within the scope of the system boundary, encompassing customer-submitted content, system-generated logs, and third party-integrated content. The company defines its core data components as follows:

AEM Data Categories

- Environmental Data: Aggregated data collected over time from both internal systems and trusted external sources (e.g., government agencies, research institutions, third-party environmental data providers). This includes long-term trends in weather, air quality, water levels, and more, used for analytics, modeling, and retrospective reporting.
- Sensor Data: Real-time telemetry captured from AEM-deployed field sensors, including but not limited to weather stations, air quality monitors, hydrological sensors, fire detection systems, and infrastructure monitoring devices.
- Forecast Data: Predictive environmental models produced internally or acquired through strategic partnerships. Forecasts may include weather predictions, fire risk assessments, flood forecasting, and other time-sensitive environmental indicators.

- User Information: Includes user login credentials (hashed and secured), user roles, authentication metadata, and access history. Additional user data includes:
    - Location Data: Where applicable, user location information is captured (e.g., for mobile app interactions or geo-contextual notifications).
    - Notification Preferences and Logs: Settings and history of system alerts and notifications sent to users via email, SMS, or in-app messaging.
- Access Logs: System-generated records that capture login attempts, session durations, role-based access events, permission changes, and other security-relevant activity. These logs support auditability and anomaly detection.
- Error Logs: Detailed diagnostic logs from AEM applications and systems, capturing exceptions, failed processes, data validation errors, and integration issues used for support, root cause analysis, and continuous improvement.

Data Lifecycle and Processing

Data acquisition begins with telemetry sent from AEM field devices and systems integrations. These inputs are processed through secure ingestion pipelines, validated for quality, and stored within cloud-based or edge-computing infrastructure depending on service requirements.

User interactions—such as portal logins, data queries, configuration changes, and notification triggers—are logged and monitored. For transportation workflows, data entry may begin with a service request and culminate in a validated record of trip execution, routing performance, and compliance verification.

All data collected by AEM undergoes classification, validation, and processing in accordance with defined business rules and security protocols. Key data is retained for analytics, compliance reporting, and long-term trend analysis as outlined in AEM's data retention policies.

Reporting and Data Security

AEM's reporting infrastructure enables data dissemination based on role and business function. Available formats and channels include:

- Secure Dashboards and Web Pages for internal teams and external customers.
- PDF and CSV Reports distributed via secure methods.
- Event Alerts and Notifications delivered through encrypted email, SMS, or mobile push.

All data transmission outside of AEM-controlled environments is encrypted using Transport Layer Security (TLS). Role-based access control (RBAC) governs internal access, and all systems utilize multi-factor authentication (MFA) and detailed audit logging to enforce accountability.

Data processing, storage, and sharing adhere to AEM's internal security framework, which aligns with the Trust Services Criteria for security, availability and confidentiality, as defined in the SOC 2 standard.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the AEM policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any AEM team member.

Physical Security

AEM utilizes Amazon Web Services (AWS) for hosting its cloud infrastructure. Consequently, the physical security of data centers and associated infrastructure is governed by AWS's robust physical security controls, which include perimeter fencing, 24/7 surveillance, biometric access controls, and stringent visitor management protocols. These measures ensure the protection of AEM's cloud-hosted assets.

Logical Access

AEM has established comprehensive logical access controls to safeguard its information systems and data. These controls ensure that only authorized individuals can access systems and data, aligning with the Trust Services Criteria for security and confidentiality.

Access Control Principles

AEM's access control framework is built upon the following principles:

- Least Privilege: Users are granted the minimum level of access necessary to perform their job functions.
- Separation of Duties: Critical functions are divided among different individuals to reduce the risk of fraud or error.
- Need to Know: Access to sensitive information is restricted to individuals who require access for legitimate business purposes.
- Role-Based Access Control (RBAC): Access rights are assigned based on the user's role within the organization, aligning with job functions and responsibilities.

User Identification and Authentication

All users are assigned unique user IDs to ensure accountability. Authentication mechanisms include strong password policies and, where applicable, multi-factor authentication (MFA) to enhance security. Passwords must meet complexity requirements and must be changed periodically.

Access Provisioning and Deprovisioning

Access to AEM's systems and data is granted based on the principle of least privilege, ensuring users have only the access necessary for their roles. Access requests are documented and require approval from authorized personnel. Upon termination or role change, access rights are promptly revoked to prevent unauthorized access.

Privileged Access Management

Administrative and privileged accounts are strictly controlled. MFA is enforced for these accounts on all mission-critical systems. All actions by privileged accounts are logged and monitored for suspicious activity. Privileged access is granted for a limited time and only when necessary, with automatic revocation after the specified time period.

Access Reviews

Periodic access reviews are conducted to ensure that users' access rights remain appropriate. These reviews involve verifying current access against job responsibilities and adjusting permissions as necessary.

Logging and Monitoring

All access to critical systems and data is logged, and logs are reviewed regularly to detect unauthorized access attempts or anomalies. Logging includes successful and failed login attempts, changes to user privileges, and access to sensitive data.

Remote Access Control

All remote access to the company network is conducted through a Virtual Private Network (VPN) using MFA.

Automated Logoffs

Company-issued devices and bring-your-own or third-party devices that may connect to company systems are configured to enforce a screensaver lock with a timeout.

Application and System Accounts

Application and system accounts and related access privileges are provisioned based on documented authorization from management and limited to only the access needed for the operability of an application or system. Interactive use of these accounts is prevented unless needed for exceptional circumstances, with explicit management approval and documentation.

Data Access Control

All data is classified based on its sensitivity according to the company's Information Security Policy. Access to confidential data is restricted based on the need-to-know principle. Sensitive data requires encryption both in transit and at rest, with decryption permitted only for authorized users with proper credentials.

Policy Enforcement and Review

Compliance with the System Access Control Policy is verified through various methods, including IT tool reports and both internal and external audits. Any known violations of this policy are reported to the Senior Director of Information Technology and may result in disciplinary action. The policy is reviewed annually or whenever there are significant changes to ensure its continued relevance and effectiveness.

These logical access controls are integral to AEM's overall security posture, ensuring that systems and data are protected against unauthorized access and aligning with SOC 2 requirements.

Computer Operations – Backups

AEM employs a comprehensive backup strategy to ensure the confidentiality, integrity, and availability of its data across both corporate and production environments. Backup operations are managed by AEM's Cloud Operations team and are designed to support rapid recovery in the event of data loss, corruption, or system failure.

All backup data is stored within Amazon Web Services (AWS) infrastructure. Physical access to AWS data centers is governed by AWS's stringent security policies and controls. Backup data is encrypted, with access to encryption keys restricted to authorized personnel.

In the event of a backup failure or exception, AEM's operations personnel promptly investigate to identify the root cause. Subsequent actions may include re-running the backup job immediately or allowing it to execute during the next scheduled backup window.

AEM has implemented monitoring and alerting mechanisms to track the status of backup jobs. Notifications for backup job failures are configured to ensure timely awareness and response. These backup procedures are integral to AEM's commitment to data protection and operational resilience, ensuring alignment with SOC 2 requirements.

Computer Operations – Availability

AEM has established comprehensive processes and procedures to ensure the availability of its computer operations, aligning with SOC 2 Trust Services Criteria. These measures encompass incident response, capacity management, and patch management to maintain continuous service delivery and system reliability.

Incident Response

AEM maintains documented incident response policies and procedures to guide personnel in identifying, reporting, and responding to information technology incidents. These procedures facilitate prompt action upon detection of system security breaches or other incidents, ensuring timely mitigation and restoration of services.

Capacity Management

AEM leverages Amazon Web Services (AWS) to provide scalable and resilient infrastructure for its applications and services. Capacity management is integral to ensuring that computing resources meet current and anticipated demands while maintaining performance and availability.

AEM utilizes AWS Auto Scaling to dynamically adjust compute resources based on real-time demand, ensuring optimal performance during varying workloads. This approach eliminates the need for manual intervention and reduces the risk of over-provisioning or under-provisioning resources.

AWS CloudWatch is employed to monitor key performance indicators such as CPU utilization, memory usage, and network throughput. These metrics inform scaling decisions and help identify potential bottlenecks or resource constraints.

AEM's infrastructure is designed with high availability in mind, deploying resources across multiple Availability Zones within AWS regions. This configuration provides redundancy and fault tolerance, minimizing the impact of potential failures in a single zone.

Regular assessments are conducted to forecast future capacity requirements based on usage trends and business growth projections. This proactive planning ensures that infrastructure can accommodate increased demand without compromising service quality.

Patch Management

AEM has implemented a structured patch management process to ensure that systems are updated in accordance with vendor-recommended operating system patches. System owners review proposed patches to determine applicability, considering the security and availability impact on critical applications. Patches are tested and validated prior to deployment, and installations are verified to confirm successful implementation.

These processes and procedures collectively support AEM's commitment to maintaining the availability of its computer operations, ensuring continuous and reliable service delivery in alignment with SOC 2 requirements.

Change Control

AEM has established comprehensive Software Development Life Cycle (SDLC) and Change Management policies to ensure that all modifications to its systems, applications, and infrastructure are conducted in a controlled and secure manner. These policies are designed to maintain system integrity and minimize risks associated with changes.

Change Request and Initiation

All proposed changes are initiated through a formal change request process. Requests are documented in AEM's ticketing system, detailing the nature of the change, rationale, potential impact, and affected systems or components. Each request undergoes an initial assessment to determine its priority, risk level, and required resources.

Documentation and Approval

Comprehensive documentation is maintained for each change, including technical specifications, implementation plans, testing procedures, and rollback strategies. Changes are reviewed and approved by designated personnel, ensuring that they align with business objectives and security standards. Emergency changes follow an expedited approval process but are subject to post-implementation review and documentation.

Development and Testing

Development activities occur in environments segregated from production to prevent unintended impacts on live systems. Changes undergo rigorous testing, to validate functionality and identify potential issues. Test results are documented and reviewed as part of the approval process.

Deployment and Implementation

Approved changes are scheduled for deployment during designated maintenance windows to minimize disruption. Deployment plans include detailed steps, responsible parties, and communication strategies. Post-deployment monitoring ensures that changes function as intended and do not adversely affect system performance or security.

Version Control and Audit Trail

AEM utilizes version control systems to manage source code and configuration changes. These systems maintain a history of modifications, including timestamps, authorship, and change descriptions, facilitating traceability and rollback if necessary.

Patch Management

Regular patch management processes are in place to apply vendor-recommended updates to systems and applications. Patches are evaluated for relevance and potential impact before deployment. Critical patches are prioritized and implemented promptly to address security vulnerabilities.

Segregation of Duties

Roles and responsibilities within the change management process are clearly defined to enforce segregation of duties. Individuals responsible for developing changes are distinct from those approving and deploying them, reducing the risk of unauthorized or unreviewed modifications.

Monitoring and Continuous Improvement

The change management process is subject to ongoing monitoring and periodic reviews. Metrics such as change success rates, incident occurrences post-change, and adherence to timelines are analyzed to identify areas for improvement. Feedback mechanisms are in place to refine processes and enhance efficiency.

Data Communications

AEM employs a multi-layered approach to secure data communications, ensuring the confidentiality, integrity, and availability of information transmitted across its networks.

Network Security

AEM's infrastructure is hosted within Amazon Web Services (AWS), utilizing Amazon Virtual Private Cloud (VPC) to establish logically isolated network environments. Security Groups and Network Access Control Lists (ACLs) are configured to control inbound and outbound traffic at the instance and subnet levels, respectively.

AEM employs AWS Web Application Firewall (AWS WAF) to enhance the security of its web applications. AWS WAF enables AEM to monitor and filter HTTP and HTTPS requests based on customizable rules, effectively mitigating common web exploits such as SQL injection and cross-site scripting (XSS). By integrating AWS WAF with services like Amazon CloudFront and Application Load Balancer, AEM ensures that malicious traffic is identified and blocked at the edge, reducing latency and safeguarding application availability. Additionally, AWS WAF's managed rule groups and real-time metrics provide AEM with streamlined security management and visibility into web traffic patterns.

For its On-Premise Corporate IT environment, AEM utilizes firewall systems to monitor and control incoming and outgoing network traffic based on predetermined security rules. These firewalls are configured to deny unauthorized access and permit only explicitly authorized communications. Network Address Translation (NAT) is implemented to manage internal IP addresses, adding an additional layer of security by obscuring internal network structures from external entities.

Redundancy and High Availability

To mitigate the risk of single points of failure, AEM's network infrastructure incorporates redundancy across critical components, including firewalls, routers, and servers. In the event of a primary system failure, redundant systems are configured to take over seamlessly, ensuring uninterrupted service delivery.

Penetration Testing and Vulnerability Management

AEM conducts regular penetration testing to assess the security posture of its systems. These tests simulate potential attack scenarios to identify and remediate vulnerabilities. Additionally, vulnerability scanning is performed on a quarterly basis using industry-standard tools and methodologies. Findings from these assessments are documented, and remediation efforts are tracked to resolution.

Secure Remote Access

Authorized personnel can access AEM systems remotely through secure Virtual Private Network (VPN) connections. These VPNs employ strong encryption protocols and require multi-factor authentication (MFA) to verify user identities, thereby safeguarding against unauthorized access.

Data Encryption

All data transmitted over AEM networks is encrypted using industry-standard protocols to protect against interception and tampering. This includes the use of Transport Layer Security (TLS) for web-based communications and secure shell (SSH) protocols for administrative access.

Monitoring and Incident Response

AEM maintains continuous monitoring of its network infrastructure to detect and respond to security incidents promptly. An incident response plan is in place, outlining procedures for identifying, reporting, and mitigating security events. Logs are maintained and reviewed regularly to ensure compliance with security policies and to support forensic investigations when necessary.

Boundaries of the System

The scope of this report includes the Services performed by AEM. This report does not include the data center hosting services provided by AWS.

The applicable trust services criteria and the related controls:

The Trust Services Categories that are in scope for the purposes of this report are as follows:

- **Security**: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability or confidentiality of information or systems and affect the entity's ability to meet its objectives.
- **Availability**: Information and systems are available for operation and use to meet the entity's objectives.
- **Confidentiality**: Information designated as confidential is protected to meet the entity's objectives.

Control Environment

Integrity and Ethical Values

AEM has established a control environment grounded in integrity, transparency, and ethical responsibility. The organization recognizes that the effectiveness of internal controls is inherently linked to the integrity and ethical standards of its people—the individuals who design, implement, and monitor those controls.

AEM's leadership actively promotes a culture of ethical conduct, setting a strong "tone at the top." This culture is communicated and reinforced through formal policies, consistent behaviors, and leadership accountability. AEM's Code of Business Conduct clearly articulates the company's expectations regarding lawful, ethical, and responsible behavior. It applies to all employees, contractors, and relevant third parties, and covers a wide range of topics including anti-bribery, conflicts of interest, data confidentiality, and respect in the workplace.

All new employees are required to review and acknowledge AEM's Code of Business Conduct upon hire. Ongoing ethics training and awareness programs are conducted to ensure continued alignment with the company's values. In addition, AEM's Anti-Bribery and Anti-Corruption Policy reinforces its zero-tolerance stance on unethical or illegal practices, and outlines specific guidelines for preventing and responding to potential violations.

To promote accountability and transparency, AEM has implemented a confidential Whistleblower Policy that encourages personnel to report unethical or unlawful behavior without fear of retaliation. Reports are investigated promptly and thoroughly, and any substantiated violations are addressed with appropriate disciplinary action.

AEM's hiring process includes pre-employment background checks to verify candidate integrity and suitability for employment. Once onboarded, employees are expected to adhere to all applicable policies, which are published and readily accessible via the company intranet. A confidentiality agreement—signed by all employees—further reinforces the obligation to protect sensitive company and client information.

AEM's Leadership team takes proactive steps to mitigate incentives or pressures that could encourage unethical conduct. This includes aligning performance objectives with organizational values and ensuring that no individual has unchecked authority over critical functions, consistent with the principles of segregation of duties and least privilege.

Commitment to Competence

AEM is committed to maintaining a workforce with the skills, knowledge, and ethical standards necessary to support its operations and deliver high-quality service. Competence at AEM is defined as the combination of technical knowledge, role-specific expertise, and professional judgment required to effectively carry out assigned responsibilities.

Management carefully defines the competencies required for each role within the organization and translates these requirements into formal job descriptions. These position descriptions outline necessary qualifications, technical skills, and expected behaviors aligned with AEM's core values and operational standards.

To ensure these competencies are maintained and enhanced over time, AEM invests in ongoing learning and professional development. This includes structured onboarding programs, technical training, compliance and security awareness education, and role-specific upskilling opportunities. Training requirements are reviewed periodically to remain aligned with evolving technologies, customer expectations, and regulatory changes.

Performance reviews are conducted on a regular basis to assess individual development, reinforce accountability, and identify growth opportunities. Managers are responsible for ensuring that employees under their supervision possess the competencies required for their roles and are supported in meeting those expectations.

By aligning human capital practices with business objectives, AEM ensures its workforce remains competent, capable, and equipped to support the organization's internal control system and broader Trust Services Criteria.

Management's Philosophy and Operating Style

AEM's management philosophy and operating style reflect a strong commitment to risk-aware decision-making, transparency, and operational discipline. These values influence every level of the organization, guiding how strategic objectives are defined, risks are assessed, and controls are designed and enforced.

Management adopts a proactive and structured approach to identifying, evaluating, and responding to business risks. This includes periodic enterprise risk assessments and operational reviews that inform strategic planning, resource allocation, and the design of key internal controls. Management places particular emphasis on balancing innovation and operational agility with the need for reliability, compliance, and long-term sustainability.

AEM's leadership regularly monitors developments in the regulatory landscape, industry trends, and emerging technologies. This insight is used to anticipate and adapt to risks that may impact service delivery, data protection, or customer trust. Formal briefings, legal and compliance updates, and security reviews are conducted regularly to ensure management is informed and engaged in critical risk and compliance matters.

Executive leadership convenes on a recurring basis to evaluate the effectiveness of corporate initiatives, assess performance metrics, and align business operations with company values and strategic goals. These meetings serve as a forum to review major decisions, address cross-functional challenges, and ensure company-wide alignment on ethical practices and risk tolerance.

In addition, management actively supports a culture of accountability and data-driven decision-making. Information systems and reporting tools are leveraged to monitor operational performance and compliance indicators. Leadership encourages openness and responsiveness in internal communications, ensuring that issues are surfaced and addressed promptly.

Organizational Structure and Assignment of Authority and Responsibility

AEM has established a clearly defined organizational structure that supports the effective planning, execution, and oversight of its business operations. This structure provides the foundation for assigning authority, aligning responsibilities, and ensuring accountability across all levels of the organization.

The organizational design reflects AEM's size, operational complexity, and service offerings. It is structured to promote clear reporting relationships, enable functional specialization, and support the achievement of organizational objectives while maintaining compliance with internal policies and regulatory requirements.

Authority and responsibility are assigned based on job roles, with well-defined scopes documented in position descriptions and role-based access frameworks. Key operational and technical decisions are governed through formal approval hierarchies, delegation matrices, and documented procedures that align decision rights with levels of responsibility and expertise.

AEM maintains up-to-date organizational charts that communicate reporting lines, departmental functions, and key leadership roles. These charts are reviewed periodically and updated in response to structural or personnel changes. New hires receive orientation that includes an overview of AEM's structure, their role within it, and how their responsibilities contribute to broader business goals.

Additionally, AEM reinforces accountability by setting clear performance expectations, implementing regular management reviews, and aligning individual and team objectives with the company's mission and strategic direction. Communication practices, including internal newsletters, team meetings, and enterprise collaboration tools, are used to ensure transparency, cross-functional alignment, and a shared understanding of corporate priorities. Through this structured assignment of authority and responsibility, AEM ensures that personnel are empowered to act within their roles while remaining aligned with the organization's objectives and control expectations

Human Resource Policies and Practices

AEM recognizes that its ability to deliver secure, reliable, and high-quality services depends on attracting, developing, and retaining skilled and ethical personnel. The company's human resource (HR) policies and procedures are designed to foster a high-performing workforce that operates with professionalism, integrity, and accountability.

AEM maintains documented HR practices covering the full employee lifecycle—including recruitment, onboarding, performance management, training and development, promotion, compensation, and termination. These policies are aligned with AEM's values and control objectives, and support the organization's compliance, security, and quality standards.

All new employees participate in a formal onboarding process, which includes mandatory security awareness and compliance training. As part of this process, employees are required to acknowledge receipt of the employee handbook, which outlines key company policies, including the Code of Conduct, confidentiality expectations, and information security responsibilities. A separate confidentiality agreement must also be signed to reinforce the safeguarding of proprietary and customer information.

Ongoing training programs are provided to ensure employees maintain relevant skills and stay informed of evolving security, privacy, and regulatory requirements. Managers conduct annual performance evaluations to assess employee effectiveness, support professional growth, and align individual contributions with organizational goals.

AEM's termination procedures are clearly documented and include a standardized checklist to ensure that all company assets (e.g., access credentials, equipment, and data) are returned or revoked in a timely and secure manner. HR and IT work in coordination to deprovision system access promptly upon employee separation.

These HR practices help establish a control-conscious culture and ensure that personnel understand their roles and responsibilities within the internal control environment.

Risk Assessment Process

AEM employs a structured and comprehensive risk assessment process as a foundational component of its information security and control environment. This process is designed to identify, evaluate, and treat risks that may impact the confidentiality, integrity, and availability of AEM systems, data, or services. It supports the organization's ability to deliver secure and reliable services to clients and maintain compliance with regulatory and contractual obligations.

AEM's risk assessment process follows a defined methodology approved by senior leadership and led by the Head of Information Security. It includes the following key stages:

- Asset Identification – All assets within the scope of the information security program are cataloged. This includes hardware, software, infrastructure, documentation, third-party services, and any component that may affect security or operational resilience.
- Threat and Vulnerability Mapping – For each asset, applicable threats and vulnerabilities are identified and cataloged in a risk register. Each risk is assigned an owner responsible for its evaluation and mitigation.
- Risk Evaluation – Each risk is assessed by calculating the product of its impact and likelihood, using standardized criteria. The resulting risk scores are categorized as Low, Medium, High, or Critical, using a risk scoring matrix.
- Treatment and Mitigation – Risks classified as High or Critical must be remediated through controls, mitigations, or other treatment strategies. Medium and Low risks are tracked and addressed at management's discretion. Treatment options may include implementing technical safeguards, transferring the risk (e.g., via insurance), avoiding the risk (e.g., discontinuing an activity), or accepting the risk if the cost of treatment outweighs the potential impact.

<u>Governance and Oversight</u>

Roles and responsibilities are clearly defined across the organization:

- Senior Leadership approves the risk management framework, ensures alignment with strategic objectives, and reviews escalated risks.
- Risk Owners are accountable for managing specific risks, implementing mitigation plans, and reporting updates.
- The Head of Information Security oversees the overall risk management process and ensures cross-functional coordination.

- IT and Business Teams contribute to risk identification and implement mitigation measures.
- All employees are expected to report potential risks and comply with internal policies.

Monitoring and Continuous Improvement

Risk assessments are reviewed and updated at least annually, or sooner if new risks are identified. AEM maintains a formal Risk Assessment Report that documents all evaluations, treatment plans, and status updates. The process is tightly integrated with change management, compliance reviews, and incident response procedures to ensure alignment across security, operations, and governance.

AEM's approach to risk management ensures that operational and security risks are continuously identified, prioritized, and addressed in a manner that aligns with its business objectives and the SOC 2 Trust Services Criteria. This ongoing assessment supports a proactive security posture and enables informed, risk-based decision-making across the enterprise.

Information and Communications Systems

Effective information and communication are essential components of AEM's internal control framework. AEM has established robust systems and processes to ensure that relevant, accurate, and timely information is captured, processed, and disseminated to support operational effectiveness, compliance, and informed decision-making.

Information is exchanged across the organization through a combination of formal systems and structured communication channels. AEM leverages secure, enterprise-grade platforms—including cloud-based collaboration tools, business applications, monitoring dashboards, and security alerting systems—to process transactions, track system activity, and support operational workflows. These systems ensure that critical data related to security, performance, and service delivery is accurately recorded and made available to authorized personnel.

In addition to automated reporting, AEM maintains strong internal communication practices to facilitate the flow of key information across all functional areas. Regular cross-functional team meetings, weekly operational syncs, and security-specific briefings are conducted to share updates, identify risks, and coordinate process improvements. These meetings are complemented by quarterly company-wide town halls, where senior leadership provides strategic updates, reinforces company values, and discusses developments affecting AEM's business and its people.

To ensure policy awareness and compliance, updates to security, privacy, and operational procedures are distributed through formal communications such as email notifications, internal bulletins, and the company intranet. New or revised policies are also discussed in relevant team meetings and reinforced through training where applicable.
External communication with customers, vendors, and partners is handled with similar care. Designated personnel are responsible for ensuring that accurate information is shared in a timely and secure manner. Feedback mechanisms—such as customer support channels, incident response processes, and supplier reviews—provide ongoing insight into stakeholder needs and emerging issues.

By maintaining clear, reliable, and secure communication systems, AEM supports the effectiveness of its internal controls and ensures alignment with the Trust Services Criteria for security, availability, and confidentiality.

Monitoring Controls

AEM employs a comprehensive monitoring program to ensure that internal controls are functioning effectively and remain aligned with business objectives, operational conditions, and compliance requirements. This process includes both ongoing monitoring and periodic evaluations, enabling management to proactively detect control weaknesses, evaluate performance, and implement timely corrective actions.

Ongoing Monitoring

Monitoring activities are embedded in AEM's day-to-day operations and are the responsibility of both functional managers and centralized governance teams. These activities include routine performance reviews, quality assurance checks, system and access audits, compliance tracking, and control self-assessments.

Management is actively engaged in reviewing results from these activities through structured departmental meetings, internal reviews, and operational debriefs. When variances or deviations from expected control behaviors are identified, immediate action is taken to assess the root cause and determine whether retraining, procedural updates, or system changes are required.

AEM supplements these efforts with continuous control monitoring using system alerts, automated compliance tools, and dashboards that provide real-time visibility into control performance and anomalies. Results from these tools are used to drive continuous improvement and enhance internal awareness.

Reporting and Corrective Action

AEM utilizes a centralized internal tracking system to document and monitor findings from ongoing evaluations and assessments. This system allows teams to assign ownership, establish remediation timelines, and track the status of corrective actions.

Escalation procedures are in place to ensure that high-risk issues are communicated to senior leadership without delay.
Significant deficiencies or recurring issues are reviewed during quarterly compliance and risk committee meetings and discussed in annual executive risk assessments.

Corrective actions are monitored through resolution, with verification steps documented to confirm effectiveness. Lessons learned from control breakdowns are used to enhance policies, strengthen procedures, and reinforce employee training programs.

Through this integrated approach to monitoring, AEM ensures that its control environment remains dynamic, resilient, and responsive.

Changes to the System in the Last 3 Months

No significant changes have occurred to the services provided to user entities in the 3 months preceding the end of the review date.

Incidents in the Last 3 Months

No significant incidents have occurred to the services provided to user entities in the 3 months preceding the end of the review date.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to AEM's Sferic, Lightning Network and Elements 360 Platforms.

Subservice Organizations

AEM's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to AEM's services to be solely achieved by AEM's control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of AEM.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met.

Security Category	
Criteria	*Controls expected to be in place*
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	

Security Category	
Criteria	*Controls expected to be in place*
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides.
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	

Security Category	
Criteria	*Controls expected to be in place*
CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where the entity's system resides.

Availability Category	
Criteria	*Controls expected to be in place*
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	AWS is responsible for managing environmental protections within the data centers that house network, virtualization management, and storage devices for its cloud hosting services where the entity's system resides.

AEM management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, AEM performs monitoring of the subservice organization controls, including the following procedures

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

Complementary User Entity Controls

AEM's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the SOC 2 Criteria related to AEM's services to be solely achieved by AEM's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of AEM's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to AEM.
2. User entities are responsible for notifying AEM of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of AEM services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize AEM services.
6. User entities are responsible for providing AEM with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying AEM of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.