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

AddEvent Platform

Relevant to Security

For the period August 11, 2025 to November 11, 2025

TOGETHER WITH INDEPENDENT AUDITORS’ REPORT

Prepared by:

Sensiba

Table of Contents

1. Independent Service Auditors' Report

To the Management of AddEvent (AddEvent)

Scope

We have examined AddEvent's accompanying assertion titled "Assertion of AddEvent Management" (assertion) that the controls within the AddEvent Platform (system) were effective throughout the period August 11, 2025 to November 11, 2025, to provide reasonable assurance that AddEvent's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *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

AddEvent 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 AddEvent's service commitments and system requirements were achieved. AddEvent has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, AddEvent 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 in achieving AddEvent'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 in achieving AddEvent'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 the AddEvent Platform were effective throughout the period August 11, 2025 to November 11, 2025, to provide reasonable assurance that AddEvent's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Sensiba LLP

San Jose, California
December 31, 2025

2. Assertion of AddEvent Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the AddEvent (AddEvent) Platform (system) throughout the period August 11, 2025 to November 11, 2025, to provide reasonable assurance that AddEvent's service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of the AddEvent Platform," (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 11, 2025 to November 11, 2025, to provide reasonable assurance that AddEvent's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022)* in AICPA*, Trust Services Criteria.*

AddEvent'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 11, 2025 to November 11, 2025, to provide reasonable assurance that AddEvent's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by AddEvent Management

December 31, 2025

3. Description of the AddEvent Platform

Company Background

AddEvent was founded in 2015, providing add-to-calendar functionality for customers of all sizes to use on their websites and in their emails. Solutions include hosted calendar and event pages, event sharing, RSVP functionality, subscription calendars, embeddable calendars, automated events, and more.

AddEvent's services help their customers reach their end users, so that events and appointments get on their calendars, increasing attendance and reducing no-show rates.

AddEvent's customers range from coaches and individual proprietors to small businesses and organizations, health clubs, doctor's offices, all the way up to Fortune 500 companies.

Services Provided

AddEvent is a SaaS platform that contains the following functionality:

- Calendar creation
- Event creation, with or without RSVP functionality
- Calendar subscriber management
- RSVP attendee management
- Cross-platform Add to Calendar buttons and links
- Template builder for event and calendar pages
- Template builder for RSVP management
- Analytics around end-user engagement

Customers use the platform to generate public event pages, public calendar pages, embeddable calendars, dynamically generated links and buttons for emails. Customers' end users then use these to add events and/or calendar subscriptions to their own calendars.

Principal Service Commitments and System Requirements

AddEvent's principal service commitments are based on its contracts and publicly stated objectives related to the operation of its SaaS platform. AddEvent commits to adhering to local privacy regulations and to a level of security that engenders the trust of our customers. As security is the primary trust service criteria, AddEvent commits to safeguarding its systems against unauthorized access, use, or modification through the implementation of layered security controls.

AddEvent does not have specific Service Level Agreements with its customers, but rather a general commitment to information security, including, but not limited to, the following:

- Access Management: User access is provisioned based on role-based access controls
- Data Encryption: All customer data is encrypted in transit and at rest

- Change Management: System changes follow a formal management process requiring peer review, testing, and approval before deployment to production
- Incident Management: Security incidents are identified, investigated, and resolved following the company's incident response plan, with notification to customers as required
- Monitoring and Logging: System activity and security events are continuously monitored using automated tools

AddEvent establishes operational requirements that support the achievement of security and system requirements. Such requirements are communicated in AddEvent's system policies and procedures. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, and how employees are hired and trained.

Components of the System

Infrastructure

Primary Infrastructure	
Hardware	Purpose
AWS	All services are cloud-hosted in the eu-west-1 region (Ireland). All software components and data are maintained in various services within AWS.

Software

Primary Infrastructure	
Software	Purpose
AddEvent Web Application	Core SaaS platform used by customers
AddEvent API	REST API for direct integration with AddEvent platform
AddEvent Public Content	Calendar and event landing pages, embeddable calendars, add to calendar processing accessible to end users
AddEvent website	Marketing content for company
AddEvent calendar feeds	System by which end users' calendar providers and individual calendar instances update subscriptions to customers' calendars

Primary Infrastructure	
Software	Purpose
	Third-party email service provider
	Third-party payment processor

People

AddEvent has staff organized in the following functional areas:

- Executive: The CEO oversees the management of the company.
- Operations: The Director of Operations over sees personnel, HR, and budgeting.
- Growth: The Head of Growth manages a team responsible for marketing, sales, and revenue operations.
- Product: The Senior Product Director is responsible for planning the functional improvement of the core product suite.
- Customer Success: Staff that interface with customers, responding to questions, issues, and requests related to the functionality of the core product suite.
- Engineering: The Head of Engineering manages a team of developers, DevOps, and QA engineers responsible for building and maintaining the software and supporting technology that comprises AddEvent's products.

Data

Data, as defined by AddEvent, constitutes the following:

- Customer identification data used to create accounts and users to access the SaaS platform (stored in the primary database)
- Core product data managed by customers, such as events and calendars (stored in the primary database)
- End user data associated with customer-managed data, such as RSVP attendees and calendar subscribers (stored in the primary database)
- Payment data (stored in, a third-party processor)
- Customer-uploaded files (stored in Bytescale, a third-party file storage service)
- Log data (stored in AWS Cloudwatch)

Customer identification data is processed when a customer initially creates a new account. Once a customer has created an account, they use the SaaS platform or API to add and manage core product data. End users may submit data that is accessible to customers when RSVPing to an event or subscribing to a calendar. Customer subscription, payment, and billing data is stored entirely in a third-party payment processor. Images that customers upload to appear on their event and calendar pages are stored in Bytescale. Log data for all aspects of the core system is stored in AWS Cloudwatch.

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 AddEvent's policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any AddEvent team member.

Physical Security

All services are hosted on AWS. AddEvent is a fully remote company and does not have a physical office. AWS does not allow AddEvent employees physical access to datacenters.

Logical Access

AddEvent follows the principle of least privilege when determining who needs access to a particular system and what level of access needs to be granted. Access shall be provisioned to the minimally required role needed in order to conduct business, perform a specific task, etc. Access is typically granted to new hires accordingly, and any changes to access may be requested via a System Access Request form.

Access to systems managing infrastructure, product development, and code source control is role-based. MFA is required for accessing all such systems. Access reviews are conducted quarterly.

When an employee leaves the company, offboarding is performed within 24 hours, with access revocation to all systems documented on a standard form. The only physical assets owned by the company are employee laptops, which are tracked by serial numbers in an asset tracking document.

Employees may use their Google Workspace sign-on with third-party systems that support it. Employees are otherwise required to keep work-related passwords in the company-managed password manager (1Password) and use MFA when available.

Prior to a new employee starting, an onboarding checklist is created with general company accounts plus any systems specific to the employee's department. All company services have a documented owner, and each owner addresses new account creation accordingly.

Computer Operations – Backups

All data stored in AddEvent's primary database is backed up daily, via automated AWS RDS backups. Backups are retained for seven days, allowing AddEvent to restore data up to a week old, as necessary. Backups are full snapshots of the database image, comprising all data.

Computer Operations – Availability

AddEvent has comprehensive monitoring and alerting in place for its core software applications.

AddEvent has incident response policies documented with roles and plans in the event of a security incident. The policies include a security tracking system, notification processes (internal and external), and a root cause analysis procedure.

AddEvent has defined RTO and RPO for system outages, based on its backup policies.

Change Control

In AddEvent's Software Development Life Cycle, all changes to production systems are documented in tickets, either as a task (for new functionality) or a bug (fixing existing functionality). New features are documented in product specifications that are then broken down into engineering tasks. All completed software changes must be vetted and approved through mandatory source control pull requests. All changes must be deployed to AddEvent's staging environment for verification and testing.

Testing is done via automated and manual QA, with all releases going through automated regression testing. All testing is done in AddEvent's staging environment, which is logically separated from the production environment.

All releases are versioned, to ensure that all changes are tracked and that rollbacks can be facilitated, as necessary.

Data Communications

AddEvent does not have an internal network. Internal collaboration tools are used to store documentation.

AddEvent's cloud infrastructure manages access to its software platforms. AddEvent's infrastructure is managed via Infrastructure-as-Code, stored in source control.

AddEvent engages with a third-party company to perform annual penetration testing of the web application. The company assesses the security of the identified environments to identify vulnerabilities, provide actionable recommendations, and ensure alignment with industry best practices. The company provides a comprehensive technical report outlining all identified vulnerabilities, including their severity, potential impact, and detailed remediation recommendations. AddEvent commits to addressing vulnerabilities that are found and enabling retesting.

AddEvent uses cloud tools to perform continuous vulnerability scanning. All identified vulnerabilities are prioritized and addressed based on severity level.

Boundaries of the System

The scope of this report includes the Services performed by AddEvent. 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.

Control Environment

Integrity and Ethical Values

AddEvent has formally documented organizational processes, including a code of conduct and employee handbook detailing behavioral expectations, standards, and ethical guidelines. All employees must acknowledge these policies upon hiring and annually thereafter. These policies include, but are not limited to:

- Equal opportunity employment
- Quality work environment
- Harassment
- Intellectual property
- Financial integrity
- Information security

All prospective hires must pass a background check as a condition of employment.

Commitment to Competence

AddEvent is committed to employing and retaining personnel with the competence necessary to support the achievement of its service commitments and system requirements.

- Recruitment and Hiring: AddEvent follows standardized hiring procedures that include background checks, reference verification, and assessment of technical and professional qualifications relevant to each position. Job descriptions clearly define required skills, experience, and responsibilities.
- Onboarding and Training: New employees receive onboarding and role-specific training, including instruction on security policies, acceptable use, data protection, and incident reporting procedures. Annual security awareness training is mandatory for all employees.
- Performance Management: Managers and employees work together annually to review performance and target areas for improvement moving forward.
- Leadership and Oversight: Executive management communicates expectations regarding performance, integrity, and compliance through the Code of Conduct, regular company meetings, and documented policies.

Management’s Philosophy and Operating Style

The AddEvent management team meets weekly to discuss ongoing initiatives, upcoming planning, financial reporting, growth and revenue plans, and company culture. AddEvent has a commitment to using data to aid in decision-making and has taken steps to implement comprehensive tracking of user behavior within its core platform to identify and prioritize the product features that existing and prospective customers seek. While AddEvent management sets the course of the company’s strategy, it relies on the autonomy of its employees to implement tactics that support that strategy. Judgement, decision-making skills, and effective communication are pillars of all employees at AddEvent, and these characteristics are emphasized as requirements of new hires.

Organizational Structure and Assignment of Authority and Responsibility

AddEvent has established a formal organizational structure designed to support the achievement of its objectives related to operations, reporting, and compliance. The structure defines clear lines of authority, responsibility, and accountability. The Company is led by the Chief Executive Officer (CEO) and manages through functional departments including Growth, Engineering, Product, and Customer Success. A formal organization chart exists detailing the hierarchy within the company.

Human Resource Policies and Practices

AddEvent’s employee policies around behavior and expectations are contained in its Employee Handbook, which all employees are required to acknowledge. AddEvent requires all employees to sign a confidentiality agreement upon hiring. Employee orientation varies from department to department but generally consists of a walk-through of all relevant systems, codebases, and documentation repositories, as well as individual one-on-one sessions with everyone in the company.

Employee evaluations are performed at least annually.

In the event an employee is terminated, an offboarding checklist is followed within 24 hours.

Risk Assessment Process

AddEvent uses a third-party Risk Assessment Register to identify, assess, and manage risks to the business. This risk assessment supports an event-based risk assessment process: risks are identified and assessed through an evaluation of threats and vulnerabilities and then organized into risk scenarios. These risk scenarios outline a potential event or situation that could adversely affect an organization's objectives. Risk scenarios typically include information about the context, the factors contributing to the risk, the potential consequences, and the conditions under which the risk might occur.

This process uses a scoring system for Impact and Likelihood to assess risk level. Management and relevant team members determine scoring for risks and make decisions about how to treat those risks, choosing among accepting, avoiding, transferring, or mitigating. Mitigating a risk involves determining a timeline for implementation and determination of residual risk post-mitigation.

Risk assessment is performed annually.

Information and Communications Systems

AddEvent collects multiple pieces of data on the usage of its core products. This data is tracked using both third-party systems and homegrown data monitoring. Data is presented in both summary and detail forms within these third-party systems, as well as in AddEvent's internal business intelligence dashboard tool.

AddEvent management and employees use this data to track company metrics. This information is reviewed weekly by management and is incorporated into presentations at AddEvent's weekly All-Hands meetings, in which departments share updates.

Day-to-day communication among AddEvent employees occurs in a messaging platform, including multiple department and functional channels. Documentation is maintained and shared in online collaboration tools.

Monitoring Controls

AddEvent has established processes to monitor the effectiveness of controls and to identify and remediate deficiencies that could affect the achievement of its service commitments and system requirements.

Management performs ongoing monitoring of system operations through automated tools, performance dashboards, and alerts generated by monitoring systems.

In addition to continuous monitoring, AddEvent conducts periodic reviews and assessments of its control environment. These include internal compliance audits, annual penetration tests, and vulnerability scanning.

System deficiencies are documented and prioritized for remediation. Security findings via vulnerability scanning, penetration testing, or other reporting mechanisms are prioritized based on severity and risk level.

Management's direct oversight of day-to-day operations ensures that issues surfaced by control processes are properly prioritized and addressed alongside regularly scheduled work items.

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 the AddEvent Platform.

Subservice Organizations

AddEvent'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 AddEvent's services to be solely achieved by AddEvent's control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of AddEvent.

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.	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.
CC6.2 - 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.	
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, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.	

Security Category	
Criteria	*Controls expected to be in place*
CC6.5 - The entity discontinues logical and physical protection 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.	
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.

AddEvent 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, AddEvent performs monitoring of the subservice organization controls, including the following procedures

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports on 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

AddEvent’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 AddEvent’s services to be solely achieved by AddEvent’s control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of AddEvent’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 AddEvent.
2. User entities are responsible for notifying AddEvent 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 supervision, management, and control of the use of AddEvent 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 AddEvent services.
6. User entities are responsible for providing AddEvent with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying AddEvent of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.