

Nimbleford Analytics, Inc.

System and Organization Controls (SOC) 2[®] Type 2 Report
on Management's Description of Its Nimbleford Insights Platform and on the
Suitability of the Design and Operating Effectiveness of Its Controls Relevant to
Security, Availability and Confidentiality

Service organization	Nimbleford Analytics, Inc. 1180 Larchmont Avenue, Suite 400, Columbus, Ohio 43215
System	Nimbleford Insights platform (software as a service)
Review period	October 1, 2025 to September 30, 2026
Trust services categories	Security, Availability and Confidentiality
Independent service auditor	Quillfeather & Rook LLP, Certified Public Accountants
Report date	October 21, 2026

CONFIDENTIAL. This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Nimbleford Analytics, Inc., user entities of the Nimbleford Insights platform during some or all of the period October 1, 2025 to September 30, 2026, business partners of Nimbleford Analytics, Inc. subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the matters described herein. It is not intended to be, and should not be, used by anyone other than these specified parties.

Table of Contents

Section 1 · Independent Service Auditor's Report	3
Section 2 · Management of Nimbleford Analytics, Inc.'s Assertion	7
Section 3 · Nimbleford Analytics, Inc.'s Description of Its Nimbleford Insights Platform	9
Services provided, infrastructure, software, people, data and procedures	9
Subservice organizations and complementary subservice organization controls	11
Complementary user entity controls	12
Section 4 · Trust Services Criteria, Related Controls, Tests of Controls and Results of Tests	13
Section 5 · Other Information Provided by Nimbleford Analytics, Inc.	18

Section 1 · Independent Service Auditor's Report

To the Board of Directors and Management of Nimbleford Analytics, Inc.:

Scope

We have examined Nimbleford Analytics, Inc.'s ("Nimbleford" or "the Company") accompanying description of its Nimbleford Insights platform titled "Nimbleford Analytics, Inc.'s Description of Its Nimbleford Insights Platform" throughout the period October 1, 2025 to September 30, 2026 (the "description") based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022)* (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2025 to September 30, 2026 to provide reasonable assurance that Nimbleford'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)*.

Nimbleford uses Amazon Web Services, Inc. ("AWS"), a subservice organization, to provide cloud infrastructure hosting, physical data center security and environmental protection, and the underlying network and storage services on which the Nimbleford Insights platform runs. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nimbleford, to achieve Nimbleford's service commitments and system requirements based on the applicable trust services criteria. The description presents Nimbleford's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Nimbleford's controls. **The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.**

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Nimbleford, to achieve Nimbleford's service commitments and system requirements based on the applicable trust services criteria. The description presents Nimbleford's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Nimbleford's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

The information included in Section 5, "Other Information Provided by Nimbleford Analytics, Inc.," is presented by management of Nimbleford to provide additional information and is not a part of the description. Information about Nimbleford's penetration testing, its bug bounty program and its planned

control enhancements has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls, and accordingly, we express no opinion on it.

Service organization's responsibilities

Nimbleford 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 Nimbleford's service commitments and system requirements were achieved. In Section 2, Nimbleford has provided the accompanying assertion titled "Management of Nimbleford Analytics, Inc.'s Assertion" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Nimbleford is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service auditor's responsibilities

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

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

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

based on the applicable trust services criteria; and

- Evaluating the overall presentation of the description.

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 examination engagement.

Inherent limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of tests of controls

The specific controls we tested and the nature, timing, and results of those tests are presented in Section 4, "Trust Services Criteria, Related Controls, Tests of Controls and Results of Tests" (Section 4).

Deviations noted in tests of controls

Our tests of the operating effectiveness of controls identified deviations in three controls, which are described in Section 4: the timeliness of the quarterly user access review (control CC6.2.3), the timely removal of logical access for terminated personnel (control CC6.3.2), and the documented peer approval of changes deployed to production (control CC8.1.2). Management's responses to these deviations are included in Section 4 and have not been subjected to the procedures applied in our examination. The deviations noted were not of a nature or magnitude that would cause the controls, taken as a whole, to fail to provide reasonable assurance that the service commitments and system requirements were achieved.

Opinion

In our opinion, in all material respects,

- a. the description presents Nimbleford's Nimbleford Insights platform that was designed and implemented throughout the period October 1, 2025 to September 30, 2026, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period October 1, 2025 to September 30, 2026, to provide reasonable assurance that Nimbleford's service commitments

and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Nimbleford's controls throughout that period; and

- c. the controls stated in the description operated effectively throughout the period October 1, 2025 to September 30, 2026, to provide reasonable assurance that Nimbleford's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Nimbleford's controls operated effectively throughout that period.

Restricted use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Nimbleford; user entities of Nimbleford's Nimbleford Insights platform during some or all of the period October 1, 2025 to September 30, 2026; business partners of Nimbleford subject to risks arising from interactions with the system; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the matters described herein. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Quillfeather & Rook LLP

Quillfeather & Rook LLP
Columbus, Ohio
October 21, 2026

Section 2 · Management of Nimbleford Analytics, Inc.'s Assertion

We have prepared the accompanying description of Nimbleford Analytics, Inc.'s ("Nimbleford") Nimbleford Insights platform titled "Nimbleford Analytics, Inc.'s Description of Its Nimbleford Insights Platform" throughout the period October 1, 2025 to September 30, 2026 (the "description") based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2[®] Report (With Revised Implementation Guidance — 2022)* (description criteria). The description is intended to provide report users with information about the Nimbleford Insights platform that may be useful when assessing the risks arising from interactions with Nimbleford's system, particularly information about system controls that Nimbleford has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP section 100.

Nimbleford uses Amazon Web Services, Inc. ("AWS"), a subservice organization, to provide cloud infrastructure hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nimbleford, to achieve Nimbleford's service commitments and system requirements based on the applicable trust services criteria. The description presents Nimbleford's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Nimbleford's controls. The description does not disclose the actual controls at the subservice organization.

The description also indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Nimbleford, to achieve Nimbleford's service commitments and system requirements based on the applicable trust services criteria. The description presents Nimbleford's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Nimbleford's controls.

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

- a. the description presents the Nimbleford Insights platform that was designed and implemented throughout the period October 1, 2025 to September 30, 2026, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period October 1, 2025 to September 30, 2026, to provide reasonable assurance that Nimbleford's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Nimbleford's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period October 1, 2025 to September 30, 2026, to provide reasonable assurance that Nimbleford's service commitments and

system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Nimbleford's controls operated effectively throughout that period.

Dana Whitcombe

Chief Executive Officer, Nimbleford Analytics, Inc.

October 21, 2026

Priya Ostrander

Chief Information Security Officer, Nimbleford Analytics, Inc.

October 21, 2026

Section 3 · Nimbleford Analytics, Inc.'s Description of Its Nimbleford Insights Platform

Company overview and services provided

Nimbleford Analytics, Inc. was founded in 2017 and is headquartered in Columbus, Ohio. The Company provides the Nimbleford Insights platform, a multi-tenant software-as-a-service analytics product that mid-market retailers, distributors and consumer brands use to consolidate point-of-sale, inventory and e-commerce data, build demand forecasts and share dashboards across their organizations. Customers load data into the platform through secure file transfer, published application programming interfaces (APIs) and pre-built connectors to commerce and enterprise resource planning systems. As of September 30, 2026, the Company had 212 employees, of whom 58 were in engineering and 9 in the security and infrastructure team.

Principal service commitments and system requirements

Nimbleford designs its processes and procedures to meet its objectives for the Nimbleford Insights platform. Those objectives are based on the service commitments that Nimbleford makes to user entities in its Master Subscription Agreement, Data Processing Addendum and Service Level Agreement, and on the operational and compliance requirements that Nimbleford has established for the services. Service commitments include the following:

- **Security:** customer data is encrypted at rest using AES-256 and in transit using TLS 1.2 or higher; access to customer data by Nimbleford personnel is restricted to authorized individuals with a business need.
- **Availability:** the Nimbleford Insights platform is designed to be available 99.9% of the time in each calendar month, excluding scheduled maintenance announced at least 72 hours in advance.
- **Confidentiality:** customer data is used only to provide the services; upon termination of a subscription, customer data is deleted from production systems within 30 days and from backups when those backups expire.

Components of the system

Infrastructure

The Nimbleford Insights platform is hosted entirely on Amazon Web Services in the US East (N. Virginia) region, with backups replicated to the US West (Oregon) region. Production workloads run in containers on Amazon Elastic Kubernetes Service; customer data is stored in Amazon Aurora PostgreSQL databases and Amazon S3 object storage. Physical and environmental security of the data centers, and the underlying compute, network and storage hardware, are the responsibility of AWS (see "Subservice organizations" below). Customer data is not stored outside the United States.

Software

The platform consists of the customer web application, the ingestion and transformation pipeline, the forecasting service and the public API. Supporting tools include an identity provider used for single sign-on (SSO) by Nimbleford personnel, a source code repository and continuous integration and deployment (CI/CD) pipeline, a ticketing system, a security information and event management (SIEM) service, an endpoint management service and a vulnerability scanning service.

People

The Chief Information Security Officer (CISO) reports to the Chief Executive Officer and is responsible for the information security program. The Security Steering Committee, consisting of the CEO, CISO, Chief Technology Officer and VP of People, meets quarterly to review risks, incidents and the status of the security program. Engineering teams own the services they build and operate them under an on-call rotation.

Data

Customer data consists of sales, inventory, product and pricing records and the dashboards and forecasts derived from them. The platform is not designed to receive payment card data, protected health information or government identifiers, and the Master Subscription Agreement prohibits customers from submitting such data. Customer data is classified as Confidential under the Company's data classification policy.

Processes and procedures

Logical access

Access by Nimbleford personnel to production systems is granted through the Company's identity provider with single sign-on and multi-factor authentication (MFA), which is enforced for all workforce accounts. Access requests are submitted through the ticketing system and approved by the system owner before access is provisioned. Production database access is limited to members of the infrastructure team and on-call engineers and is granted on a just-in-time basis for a maximum of eight hours. System owners review user access to production systems each quarter; reviews are to be completed within 15 days after the end of each quarter. When an employee or contractor leaves the Company, the People team submits a termination ticket and access to the identity provider and production systems is to be revoked within one business day of the termination date.

Change management

Changes to application code and infrastructure configuration are made through pull requests in the source code repository. Each pull request requires review and approval by an engineer other than its author before it can be merged; branch protection rules enforce this requirement on the main branch. Automated tests and static analysis run in the CI/CD pipeline before deployment. Emergency changes may be deployed with approval from the on-call lead and are reviewed after deployment within two business days.

Vulnerability management and monitoring

Authenticated vulnerability scans of production infrastructure and container images are performed weekly. Vulnerabilities rated critical are to be remediated within 15 days and those rated high within 30 days. Logs from production systems, the identity provider and the CI/CD pipeline are sent to the SIEM, where alerts for defined security events are routed to the security team. Logs are retained for 12 months.

Incident response

The incident response plan defines severity levels, roles, communication paths and post-incident review. Customers are notified of a security incident affecting their data without undue delay and in any event within 72 hours of Nimbleford confirming the incident, as committed in the Data Processing Addendum. The plan is tested annually through a tabletop exercise; the exercise during the review period took place on April 14, 2026.

Backup, recovery and availability

Production databases are backed up automatically every 24 hours, and backups are retained for 35 days. Backups are encrypted and replicated to a second AWS region. The disaster recovery plan defines a recovery point objective (RPO) of 24 hours and a recovery time objective (RTO) of 12 hours for the Nimbleford Insights platform. A restoration test is performed quarterly, and a full disaster recovery test is performed annually; the test during the review period took place on March 9, 2026. Platform availability is monitored continuously by an external monitoring service.

Human resources security

New employees undergo a background check before their start date, sign the Company's confidentiality agreement and acceptable use policy, and complete security awareness training within 30 days of hire. All personnel complete security awareness training annually.

Vendor management

The Company maintains an inventory of vendors that process customer data or support the production environment. Such vendors are assessed before engagement and reviewed annually, including a review of their SOC 2 reports or equivalent assurance where available.

Subservice organizations

Nimbleford uses Amazon Web Services, Inc. as a subservice organization for cloud infrastructure hosting. **The carve-out method has been used for AWS: the controls of AWS are excluded from the scope of this report, and the description includes only the controls of Nimbleford.** Nimbleford's controls are designed with the assumption that the following types of complementary subservice organization controls (CSOCs) are implemented by AWS:

Criteria	Complementary subservice organization controls expected at AWS
CC6.4	Physical access to data centers housing the production environment is restricted to authorized personnel and monitored.

CC6.1, CC6.6	The hypervisor and underlying infrastructure isolate customer environments, and the network infrastructure is protected from unauthorized access.
CC7.2	Infrastructure is monitored for security events, and incidents affecting customers are communicated to them.
A1.2	Environmental protections, including power, cooling and fire suppression, are maintained and tested; storage hardware is replaced when it fails.
C1.2	Storage media are securely destroyed when decommissioned.

Nimbleford reviews the AWS SOC 2 report annually and evaluates the impact of any exceptions noted.

Complementary user entity controls

Nimbleford's controls were designed with the assumption that certain controls would be implemented by user entities (customers). The complementary user entity controls (CUECs) below are necessary, along with Nimbleford's controls, to achieve the service commitments and system requirements. **User entities are responsible for:**

Criteria	Complementary user entity controls
CC6.1, CC6.2	Provisioning, reviewing and removing the access of their own users to the Nimbleford Insights platform, including assigning user roles in accordance with least privilege.
CC6.1	Configuring single sign-on and enforcing multi-factor authentication for their users through their own identity provider, where they elect to use SSO.
CC6.1	Protecting the API keys issued to their organization and rotating them when personnel with access leave.
CC6.7	Ensuring that data transmitted to the platform through connectors and file transfer is sent from secure, authorized sources.
CC7.3	Notifying Nimbleford promptly of suspected security incidents or unauthorized use of their accounts.
C1.1	Not submitting payment card data, protected health information or other restricted data to the platform.

Section 4 · Trust Services Criteria, Related Controls, Tests of Controls and Results of Tests

This section presents the controls that Nimbleford has designed to meet the applicable trust services criteria, the tests performed by Quillfeather & Rook LLP to determine whether those controls operated effectively throughout the period October 1, 2025 to September 30, 2026, and the results of those tests. Tests of operating effectiveness included inquiry of appropriate personnel, observation of the application of controls, inspection of documents and records, and reperformance. Where sampling was used, sample sizes were determined based on the frequency of the control and the population of occurrences in the review period.

Control	Control activity specified by Nimbleford · test performed by the service auditor · results of tests
CC1.0 · Control environment	
CC1.1.1	Personnel acknowledge the Code of Conduct and the acceptable use policy at hire and annually. Test performed. Inspected acknowledgements for a sample of 25 new hires and 25 current personnel. Result. No exceptions noted.
CC1.3.1	An organization chart defines reporting lines; the CISO reports to the CEO. Test performed. Inspected the organization chart and the CISO's job description. Result. No exceptions noted.
CC1.4.1	Background checks are completed before the start date of new employees. Test performed. Inspected background check results for a sample of 25 new hires. Result. No exceptions noted.
CC1.4.2	Personnel complete security awareness training within 30 days of hire and annually. Test performed. Inspected training records for a sample of 25 new hires and 25 current personnel. Result. No exceptions noted.
CC2.0 · Communication and information	
CC2.2.1	Information security policies are reviewed and approved annually and published on the Company intranet. Test performed. Inspected the policies, their approval records and the intranet page. Result. No exceptions noted.
CC2.3.1	Service commitments are communicated to customers in the Master Subscription Agreement, Data Processing Addendum and Service Level Agreement. Test performed. Inspected the current agreements and the public status page. Result. No exceptions noted.
CC3.0 · Risk assessment	
CC3.1.1	A formal risk assessment is performed annually and reviewed by the Security Steering Committee. Test performed. Inspected the risk assessment dated February 2026 and the committee minutes. Result. No exceptions noted.

Control	Control activity specified by Nimbleford · test performed by the service auditor · results of tests
CC3.4.1	Changes with a significant effect on the system of internal control are assessed by the Security Steering Committee. Test performed. Inspected the minutes of the four quarterly committee meetings. Result. No exceptions noted.
CC4.0 · Monitoring activities	
CC4.1.1	The security team monitors the operation of key controls through a compliance automation tool, and exceptions are tracked to resolution. Test performed. Inspected the tool's configuration and the tracked exceptions. Result. No exceptions noted.
CC5.0 · Control activities	
CC5.2.1	Technology general controls are defined in policy and assigned to control owners. Test performed. Inspected the control register and assignments. Result. No exceptions noted.
CC6.0 · Logical and physical access controls	
CC6.1.1	Workforce access to production systems requires single sign-on through the identity provider with multi-factor authentication. Test performed. Inspected the identity provider's authentication policy and attempted to authenticate without a second factor. Result. No exceptions noted.
CC6.1.2	Customer data is encrypted at rest with AES-256 and in transit with TLS 1.2 or higher. Test performed. Inspected encryption settings of production databases and storage buckets and the load balancer TLS policy. Result. No exceptions noted.
CC6.1.3	Production database access is granted just in time, for a maximum of eight hours, to members of the infrastructure team and on-call engineers. Test performed. Inspected the access broker configuration and a sample of 25 access grants. Result. No exceptions noted.
CC6.2.1	New access to production systems is approved by the system owner before it is provisioned. Test performed. Inspected approval tickets for a sample of 25 access grants. Result. No exceptions noted.
CC6.2.3	System owners review user access to production systems quarterly; reviews are completed within 15 days after quarter end, and inappropriate access is removed. Test performed. Inspected the access reviews for the four quarters in the review period. Result. Exception noted. The review for the quarter ended June 30, 2026 was completed on August 10, 2026, 41 days after quarter end. The other three reviews were completed within 15 days. No inappropriate access was identified in the late review.

Control	Control activity specified by Nimbleford · test performed by the service auditor · results of tests
CC6.3.1	Access changes for personnel who change roles are requested and approved through the ticketing system. Test performed. Inspected tickets for a sample of 10 role changes. Result. No exceptions noted.
CC6.3.2	Access to the identity provider and production systems is revoked within one business day of an employee's or contractor's termination date. Test performed. Inspected termination tickets and identity provider logs for a sample of 25 terminated personnel. Result. Exception noted. For 2 of 25 terminated personnel sampled, access was revoked 4 and 6 business days after the termination date. Inspection of logs showed no activity by these accounts after the termination date.
CC6.6.1	Network traffic to production is restricted by security groups and a web application firewall; administrative interfaces are not exposed to the internet. Test performed. Inspected security group rules, the web application firewall configuration and an external port scan. Result. No exceptions noted.
CC6.7.1	Removable media are blocked and full-disk encryption is enforced on company laptops by the endpoint management service. Test performed. Inspected the endpoint management policies and the compliance report for all managed laptops. Result. No exceptions noted.
CC6.8.1	Endpoint protection software is installed on all company laptops and production hosts, and alerts are sent to the security team. Test performed. Inspected the endpoint protection console for all managed devices. Result. No exceptions noted.
CC7.0 · System operations	
CC7.1.1	Authenticated vulnerability scans of production infrastructure and container images are performed weekly; critical vulnerabilities are remediated within 15 days and high vulnerabilities within 30 days. Test performed. Inspected scan schedules and results for a sample of 10 weeks and remediation tickets for all critical and high vulnerabilities in those scans. Result. No exceptions noted.
CC7.2.1	Production, identity provider and CI/CD logs are sent to the SIEM, and alerts for defined security events are routed to the security team. Logs are retained for 12 months. Test performed. Inspected the SIEM log sources, alert rules, a sample of 15 alerts and the retention setting. Result. No exceptions noted.
CC7.3.1	Security incidents are recorded, classified by severity and handled in accordance with the incident response plan. Test performed. Inspected the incident log and all 3 incidents recorded during the review period. Result. No exceptions noted.

Control	Control activity specified by Nimbleford · test performed by the service auditor · results of tests
CC7.4.1	The incident response plan is tested annually through a tabletop exercise. Test performed. Inspected the tabletop exercise report dated April 14, 2026. Result. No exceptions noted.
CC7.5.1	Affected customers are notified within 72 hours of Nimbleford confirming a security incident affecting their data. Test performed. Inquired of management and inspected the incident log. No incident affecting customer data occurred during the review period, so the operating effectiveness of this control could not be tested. Result. No testing performed: the circumstances that warrant the operation of the control did not occur.
CC8.0 · Change management	
CC8.1.1	Branch protection on the main branch requires a pull request approved by a reviewer other than the author before merging. Test performed. Inspected branch protection settings of the production repositories. Result. No exceptions noted.
CC8.1.2	Changes deployed to production have a documented peer approval; emergency changes are reviewed within two business days after deployment. Test performed. Inspected a sample of 40 production deployments, including 3 emergency changes. Result. Exception noted. For 1 of 40 deployments sampled, an infrastructure configuration change was applied directly through the cloud console by an administrator, outside the pull request process, and had no documented peer approval. The change was reviewed after the auditor inquired.
CC9.0 · Risk mitigation	
CC9.2.1	Vendors that process customer data are assessed before engagement and reviewed annually, including their SOC 2 reports where available. Test performed. Inspected the vendor inventory and the annual reviews of a sample of 10 vendors, including AWS. Result. No exceptions noted.
A1.0 · Additional criteria for availability	
A1.1.1	Capacity and performance of production systems are monitored and alerts are sent to on-call engineers. Test performed. Inspected monitoring dashboards and alert configuration. Result. No exceptions noted.
A1.2.1	Production databases are backed up every 24 hours; backups are encrypted, replicated to a second region and retained for 35 days. Test performed. Inspected backup configuration and the backup history for a sample of 25 days. Result. No exceptions noted.
A1.3.1	A backup restoration test is performed quarterly. Test performed. Inspected the restoration test records for the four quarters. Result. No exceptions noted.

Control	Control activity specified by Nimbleford · test performed by the service auditor · results of tests
A1.3.2	The disaster recovery plan, with an RPO of 24 hours and an RTO of 12 hours, is tested annually. Test performed. Inspected the disaster recovery plan and the test report dated March 9, 2026. Result. No exceptions noted.
C1.0 · Additional criteria for confidentiality	
C1.1.1	Customer data is classified as Confidential, and access to it is restricted as described in CC6.1. Test performed. Inspected the data classification policy. Result. No exceptions noted.
C1.2.1	Upon termination of a subscription, customer data is deleted from production systems within 30 days. Test performed. Inspected deletion records for a sample of 8 terminated customers. Result. No exceptions noted.

Management's responses to deviations

CC6.2.3 (quarterly access review). The review for the second quarter of 2026 was delayed when the system owner responsible for the review left the Company. Reviews are now assigned to a primary and a secondary owner, and the compliance automation tool escalates any review not completed within 10 days to the CISO.

CC6.3.2 (termination of access). Both late revocations concerned contractors whose end dates were not entered in the HR system by the hiring managers. Since July 2026, contractor accounts are created with an expiry date in the identity provider and are disabled automatically on that date.

CC8.1.2 (change approval). The change was a security group update made during an incident. Write access to the cloud console for production has since been limited to a break-glass role whose use generates an alert to the security team.

Section 5 · Other Information Provided by Nimbleford Analytics, Inc.

The information in this section is presented by management of Nimbleford Analytics, Inc. to provide additional information to user entities. It is not part of the description of the Nimbleford Insights platform, and it has not been subjected to the procedures applied in the examination by Quillfeather & Rook LLP. Accordingly, the service auditor expresses no opinion on it.

Penetration testing

In May 2026, Nimbleford engaged an independent security firm to perform a penetration test of the Nimbleford Insights web application and public API. The test identified 2 high-risk findings and 5 medium-risk findings. Management reports that both high-risk findings were remediated by July 2026 and that the medium-risk findings are tracked in the remediation plan, with four remediated as of the date of this report.

Responsible disclosure

Nimbleford accepts vulnerability reports from security researchers at security@nimbleford.example and through a published responsible disclosure policy. The Company does not currently operate a paid bug bounty program.

Planned enhancements

During 2027, Nimbleford plans to add Privacy and Processing Integrity criteria to the scope of its SOC 2 examination and to begin preparing for ISO/IEC 27001 certification.