System and Organization Controls (SOC) 3 Report

Report on Actionable Insights Forum's Actionable Insights Resources Relevant to Security

For the period February 1, 2026 to April 30, 2026

MODERN Assurance

The report accompanying this description was issued by Modern Assurance, LLC.

PRIVATE AND CONFIDENTIAL

Table of Contents

Section I: Independent Service Auditor’s Report

MODERN Assurance

Independent Service Auditor’s Report

To Management of Actionable Insights Forum,

Scope

We have examined Actionable Insights Forum's (Actionable's) accompanying assertion, titled “Actionable Insights Forum's Management Assertion” (assertion) that the controls within Actionable's Actionable Insights Resources (system) were effective throughout the period February 1, 2026 to April 30, 2026 to provide reasonable assurance that Actionable'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 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity,* Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Actionable uses the subservice organizations described in the “Subservice Organizations” subsection of Attachment A of the report. The information included within the Boundaries of Actionable Insights Forum's System (Attachment A) indicates that Actionable's controls can provide reasonable assurance that certain service commitments and system requirements, based on the applicable trust services criteria, can be achieved only if the controls at the subservice organizations, assumed in the design of Actionable's controls, are suitably designed and operating effectively along with related controls at the service organization. The information included within the boundaries of the system presents Actionable's system and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at the subservice organizations. Our examination did not extend to the services provided by the subservice organizations and we have not evaluated whether the controls management assumes have been implemented at the subservice organizations or whether such controls were suitably designed and operating effectively throughout the period February 1, 2026 to April 30, 2026.

Service Organization’s Responsibilities

Actionable 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 Actionable's service commitments and system requirements were achieved. Actionable has provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Actionable is

responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on 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 the controls were not effective to achieve Actionable'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 Actionable'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 examination engagement.

Inherent Limitations

There are inherent limitations in 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 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.

Opinion

In our opinion, management's assertion that the controls within Actionable's Actionable Insights resources were effective throughout the period February 1, 2026 to April 30, 2026 to provide reasonable assurance that Actionable's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Modern Assurance, LLC

May 6, 2026
Denver, Colorado

Section II: Actionable Insights Forum's Management Assertion

Actionable Insights Forum's Management Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Actionable Insights Forum's (Actionable's) Actionable Insights resources (system) throughout the period February 1, 2026 to April 30, 2026 to provide reasonable assurance that Actionable'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 (AICPA, Trust Services Criteria)*. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

The information included within the Boundaries of Actionable Insights Forum's System (Attachment A) indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Actionable, to achieve Actionable's service commitments and system requirements based on the applicable trust services criteria. The Boundaries of Actionable Insights Forum's System (Attachment A) presents the types of complementary subservice organization controls assumed in the design of Actionable's controls, and does not disclose the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period February 1, 2026 to April 30, 2026 to provide reasonable assurance that Actionable's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the subservice organizations applied the complementary controls assumed in the design of Actionable's controls throughout that period. Actionable'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 Attachment B.

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 February 1, 2026 to April 30, 2026 to provide reasonable assurance that Actionable's service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A

Boundaries of Actionable Insights Forum's system

Attachment B

Actionable Insights Forum's Service Commitments and System Requirements

Attachment A: Boundaries of Actionable Insights Forum's System

Actionable Insights Forum's Actionable Insights Resources

Overview of the Company and Types of Services Provided

Actionable Insights Forum (“Actionable” or “the Company”) is an educational non-profit organization dedicated to advancing the professional standards and operational efficiency of the property restoration and insurance claims industry. As a member-based organization, Actionable serves as a collaborative hub for industry professionals, providing data-driven resources and educational tools designed to streamline the claims process. Its mission is centered on fostering a more transparent and consistent ecosystem for all stakeholders involved in property recovery.

Actionable’s primary service offering is the Actionable Profile, a comprehensive platform available through the Pro Plan Membership. The Actionable Profile provides live, real-time estimating guidance directly integrated into industry-standard software. By leveraging a proprietary database of thousands of validated rules and best practices, the service acts as an automated consultant, helping users identify missing components, correct inaccuracies, and ensure compliance with industry standards before a claim is submitted.

Actionable is a foundation that exists to preserve the health of the restoration ecosystem by clarifying globally recognized billing standards. As a natural expression of this mission, Actionable established estimating guidelines that help Xactimate users generate accurate estimates that are approved without hesitation.

The scope of this report includes the Actionable Insights resources.

Components of the System

Infrastructure

Actionable Insights Resources is comprised of the following components:

Component	Description	Hosted Location
Actionable Xactimate Profile	Actionable provides and maintains data for templated profiles within Verisk's Xactimate product, which provides guidance for estimators. Actionable is responsible for the data and for providing it to Verisk, and Verisk is responsible for reviewing the data before loading it into their platform.	Verisk
Enterprise Reporting	For Actionable customers who use the custom reporting service, Verisk provides Actionable a PowerBI instance with the data related to active estimates. Actionable creates custom reports on the data through PowerBI and distributes the reports to clients on a monthly basis. As of April 2026, PowerBI was replaced by Google Looker for this process.	PowerBI (Microsoft Azure) Google Looker

Software

Actionable utilizes the following software to support the platform:

Function	Software used
Authentication manager	Google
Human resources	Gusto
Password management	1Password
Monitoring and logging	Google Workspace Alerts
Mobile device management	JumpCloud

Data

Actionable sends data sets to Verisk in an encrypted format specified by Verisk. For enterprise reporting clients, Actionable accesses data provided by Verisk via PowerBI to create custom reporting for delivery to customers. Sensitive data is not transmitted outside of Actionable's environment. The Company uses TLS to encrypt data when transmitted over email (AC-11). Actionable receives data from Verisk and imports the data into PowerBI (through March 2026) and into GoogleLooker (April 2026 onward) to create custom reporting for customers.

People

Actionable's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored.

Actionable has established an organizational structure that includes consideration of key areas of authority and responsibility, as well as appropriate lines of reporting.

Policies

Actionable has implemented the following policies, which serve as the basis for Company procedures, are made accessible to all relevant employees and contractors, and are reviewed annually:

- Acceptable Usage Policy - defines standards for appropriate and secure use of company hardware and electronic systems, including storage media, communication tools, and internet access. This policy is acknowledged by employees and contractors upon hire (ORG-10).
- Access Control Policy - governs authentication and access to applications, resources, and tools (AC-04).
- Business Continuity and Disaster Recovery Policy - governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption (AVA-04).
- Change Management Policy - governs the documentation, tracking, testing, and approval of system, network, security, and infrastructure changes for applications, resources, and tools (CM-07).

- Code of Conduct - outlines ethical expectations, behavior standards, and ramifications of non-compliance. This policy is acknowledged by employees and contractors upon hire (ORG-01).
- Encryption and Key Management Policy - supports the requirements for secure encryption and decryption of app secrets and governs the use of cryptographic controls (AC-12).
- Information Security and HR Security Policy - establishes the security requirements for maintaining the security of applications, resources, and tools (ORG-12).
- Internal Audit, Continual Improvement, and Non-Conformity Corrective Action Policy - identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies (ORG-14).
- Network Management Policy - identifies the requirements for protecting information and systems within and across networks (NET-06).
- Risk Management Procedure - governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners (RA-01).
- Incident Management Policy - outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution (IR-01).
- Vendor Management Policy - defines a framework for the onboarding and management of the vendor relationship cycle (RA-04).

Control Environment

The objectives of internal control as it relates to the Actionable Insights resources are to provide reasonable, but not absolute, assurance that controls are suitably designed and operating effectively to meet the relevant control objectives, that assets are protected from unauthorized use or disposition, and that transactions are executed in accordance with management's authorization and client instructions. Management has established and maintains controls designed to monitor compliance with established policies and procedures. The remainder of this subsection discusses the tone at the top as set by management, the integrity, ethical values, and competence of Actionable employees, the policies and procedures, the risk management process and monitoring, and the roles of

significant control groups. The internal control structure is established and refreshed based on Actionable's assessment of the risks facing the organization.

Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of key processes. Integrity and ethical behavior are the products of Actionable's ethical and behavioral standards, how they are communicated, and how they are monitored and enforced in its business activities. They include management's actions to remove or reduce incentives/pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of the entity's values and behavioral standards to personnel through policy statements and Code of Conduct, and by the examples the executives set. Actionable's executive management recognizes their responsibility to foster a strong ethical environment within Actionable to ensure that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct. This responsibility is characterized and reflected in the Code of Conduct, which is distributed to all applicable personnel of the organization.

Risk Assessment Process

Actionable has defined a risk management framework for evaluating information security risk and other relevant forms of business risk. A formal risk assessment is performed at least annually to identify, update, and assess relevant internal and external threats related to security, which also considers the potential for fraud (RA-02). A risk register is maintained to record the risk mitigation strategies for identified risks, and to track the development or modification of controls consistent with the risk mitigation strategy (RA-03).

Due to the company's heavy reliance on outside vendors for critical infrastructure, processing capabilities, and business functions, the company has developed a Vendor Management Policy that establishes the compliance and performance expectations required of vendors, and the due diligence and monitoring expectations required of the Company's personnel. Agreements, which include security requirements, are executed with vendors in accordance with the Vendor Management Policy (RA-06). Actionable collects and reviews the compliance reports (i.e. SOC 2, SOC 3, or ISO 27001) for its high-risk vendors on at least an annual basis (RA-05).

Monitoring Activities

Actionable performs several types of monitoring to assess the security and health of the in-scope environment and the related controls. The company leverages a continuous

monitoring solution that monitors internal controls used in the achievement of service commitments and system requirements. The tool identifies instances of non-compliance for management to resolve (ORG-05).

Alerting software is used to notify impacted teams of potential security events, and identified events are tracked to resolution (NET-05). The Security Department meets quarterly to coordinate security initiatives, review network security and management of infrastructure, and discuss security risks (NET-07).

Incident Response

The Company employs multiple mechanisms to identify potential security incidents, as described in the *Communication* and *Monitoring* sections above. Confirmed incidents are documented, tracked, and responded to according to the Security Incident Response Plan (IR-02). Following an incident, a 'lessons learned' document is created and shared with relevant internal personnel to make any required changes (IR-03). The Security Incident Response Plan is tested annually to assess effectiveness, and management makes changes to the Security Incident Response Plan based on the test results (IR-04).

Subservice Organizations

The Company utilizes the subservice organizations in the below tables to achieve its objectives.

Subservice Organization	Services Provided
Google LLC (Google Workspace)	The subservice organization provides the Company with cloud infrastructure. This organization was carved out of the report.

Complementary Subservice Organization Controls

- The subservice organization performs periodic vulnerability assessments (CC 3.2).
- The subservice organization's data centers are protected by fire detection and suppression systems, air conditioning systems, uninterruptible power supply (UPS) units, and backup generators (CC 5.2).
- The subservice organization applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved (CC 5.2, CC 8.1).
- The subservice organization performs integrity checks of the data at rest (CC 5.2).

Subservice Organization	Services Provided
Google LLC (Google Workspace)	The subservice organization provides the Company with cloud infrastructure. This organization was carved out of the report.

Complementary Subservice Organization Controls

- The subservice organization implements redundancy and replication to ensure that the system is able to sustain the loss of a data center facility without interruption to the service (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains contingency planning and incident response procedures to reflect emerging continuity risks and lessons learned from past incidents (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains a capacity planning model to periodically assess infrastructure usage and demands (CC 5.2).
- The subservice organization ensures that logical IT access is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.1, CC 6.2, CC 6.3, CC 6.6).
- The subservice organization ensures that strong encryption keys are used to protect customer content and that master keys used for cryptographic operations are logically secured (CC 6.1).
- The subservice organization ensures that physical access to the data centers is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.4).
- The subservice organization ensures that data is encrypted in transit (CC 6.6, CC 6.7).
- The subservice organization has implemented monitoring to identify and notify personnel of potential issues and/or incidents (CC 7.1, CC 7.5).
- The subservice organization has implemented incident response procedures to identify, track, and respond to incidents (CC 7.3, CC 7.4, CC 7.5).
- The subservice organization ensures that customer information, including personal information, and customer content are not used in test and development environments (CC 8.1).
- The subservice organization maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact business objectives, regulatory requirements, and customers (CC 9.2).
- The subservice organization 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 (CC6.5).

Subservice Organization	Services Provided
PowerBI (Microsoft Azure)	The subservice organization provides the Company with data analytics services. This organization was carved out of the report.

Complementary Subservice Organization Controls

- The subservice organization's data centers are protected by fire detection and suppression systems, air conditioning systems, uninterruptible power supply (UPS) units, and backup generators (CC 5.2).
- The subservice organization applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved (CC 5.2, CC 8.1).
- The subservice organization performs integrity checks of the data at rest (CC 5.2).
- The subservice organization implements redundancy and replication to ensure that the system is able to sustain the loss of a data center facility without interruption to the service (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization ensures that logical IT access is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.1, CC 6.2, CC 6.3, CC 6.6).
- The subservice organization ensures that strong encryption keys are used to protect customer content and that master keys used for cryptographic operations are logically secured (CC 6.1).
- The subservice organization ensures that physical access to the data centers is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.4).
- The subservice organization ensures that data is encrypted in transit (CC 6.6, CC 6.7).
- The subservice organization 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 (CC6.5).

Subservice Organization	Services Provided
Verisk Analytics, Inc. (Xactimate)	The subservice organization provides the Company with Property Claims Estimating Software. This organization was carved out of the report.

Complementary Subservice Organization Controls

The subservice organization is responsible for providing the Xactimate product in a Software-as-a-Service model, which includes responsibility for the following Trust Services Criteria with respect to the Xactimate product, at a minimum:

- The subservice organization performs periodic vulnerability assessments (CC 3.2).
- The subservice organization's data centers are protected by fire detection and suppression systems, air conditioning systems, uninterruptible power supply (UPS) units, and backup generators (CC 5.2).
- The subservice organization applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved (CC 5.2, CC 8.1).
- The subservice organization performs integrity checks of the data at rest (CC 5.2).
- The subservice organization implements redundancy and replication to ensure that the system is able to sustain the loss of a data center facility without interruption to the service (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains contingency planning and incident response procedures to reflect emerging continuity risks and lessons learned from past incidents (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains a capacity planning model to periodically assess infrastructure usage and demands (CC 5.2).
- The subservice organization ensures that logical IT access is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.1, CC 6.2, CC 6.3, CC 6.6).
- The subservice organization ensures that strong encryption keys are used to protect customer content and that master keys used for cryptographic operations are logically secured (CC 6.1).
- The subservice organization ensures that physical access to the data centers is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.4).
- The subservice organization ensures that data is encrypted in transit (CC 6.6, CC 6.7).
- The subservice organization has implemented monitoring to identify and notify personnel of potential issues and/or incidents (CC 7.1, CC 7.5).

Subservice Organization	Services Provided
Verisk Analytics, Inc. (Xactimate)	The subservice organization provides the Company with Property Claims Estimating Software. This organization was carved out of the report.

Complementary Subservice Organization Controls

- The subservice organization has implemented incident response procedures to identify, track, and respond to incidents (CC 7.3, CC 7.4, CC 7.5).
- The subservice organization ensures that customer information, including personal information, and customer content are not used in test and development environments (CC 8.1).
- The subservice organization maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact business objectives, regulatory requirements, and customers (CC 9.2).
- The subservice organization 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 (CC6.5).

Attachment B: Actionable Insights Forum's Service Commitments and System Requirements

Actionable Insights Forum's Service Commitments and System Requirements

Actionable and its customers have a shared responsibility in maintaining the security of the Actionable Insights resources. Actionable has established principal service commitments, which are communicated to customers and consist of the following:

- Requires team members to go through employee security awareness training covering industry standard practices and information security topics such as phishing and password management.
- Requires all team members to adhere to a minimum set of password requirements and complexity for access. Additionally, implements single sign-on (SSO) and 2-factor authentication (2FA) where available.
- Utilizes a password manager to manage passwords and maintain password complexity.
- Enrolls all company-provided workstations in Mobile Device Management (MDM) to enforce security settings including full-disk encryption, screen lock, and strong password policy.
- Implements disaster recovery plans and tests them at least once per year.

Actionable has established system requirements, which are communicated to customers and consist of the following:

- Employee provisioning and deprovisioning standards
- Business continuity and disaster recovery plan