Insight Assurance

SOC 2| ISO 27001 | PCI | HIPAA

System and Organization Controls 3 (SOC 3) Report

Report on Realized Holdings, Inc. Description of Its Investment Proprietary Wealth Management Services System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, Confidentiality, Privacy, and Processing Integrity Throughout the Period August 1, 2023 to October 31, 2023

REALIZED®

TABLE OF CONTENTS

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Realized Holdings, Inc.

Scope

We have examined Realized Holdings, Inc.'s ('Realized Holdings) accompanying assertion titled "Realized Holdings, Inc.'s Management Assertion" (assertion) that the controls within Realized Holdings' Platform were effective throughout the period August 1, 2023 to October 31, 2023, to provide reasonable assurance that Realized Holdings' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, Privacy, and Processing Integrity (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Privacy, and Processing Integrity, (With Revised Points of Focus—2022) in AICPA, Trust Services Criteria.

Realized Holdings uses a subservice organization to provide hosting services. The assertion indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Realized Holdings, to achieve Realized Holdings' service commitments and system requirements based on the applicable trust services criteria. Attachment A presents the types of complementary subservice organization controls assumed in the design of Realized Holdings' controls. Attachment A 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 assertion indicates that certain complementary user entities are necessary, along with controls at Realized Holdings, to achieve Realized Holdings' service commitments and system requirements based on the applicable trust services criteria. Attachment A presents the complementary user entity controls assumed in the design of Realized Holdings' 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.

Service Organization's Responsibilities

Realized Holdings 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 Realized Holdings service commitments and system requirements were achieved. Realized Holdings has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Realized Holdings 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 Auditor's 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 American Institute of

Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

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

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 are 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 Realized Holdings' Platform were effective throughout the period August 1, 2023, to October 31, 2023, if complementary subservice organization controls and complementary user entities controls were effective, to provide reasonable assurance that Realized Holdings' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Insight Assurance LLC
Tampa, Florida
March 1, 2024

REALIZED HOLDINGS, INC.'S MANAGEMENT ASSERTION

REALIZED

REALIZED HOLDINGS, INC.'S MANAGEMENT ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within Realized Holdings, Inc.'s ('Realized Holdings') Investment Proprietary Wealth Management Services System throughout the period August 1, 2023, to October 31, 2023, to provide reasonable assurance that Realized Holdings' service commitments and system requirements relevant to Security, Availability, Confidentiality, Privacy, and Processing Integrity were achieved. Our description of the boundaries of the system is presented in Attachment A, titled, "Realized Holdings, Inc.'s Management Description of its Investment Proprietary Wealth Management Services System", and identifies the aspects of the system covered by our assertion.

Realized Holdings uses a subservice organization to provide hosting services. Attachment A indicates that effective complementary subservice organization controls are necessary, along with controls at Realized Holdings, to achieve Realized Holdings' service commitments and system requirements based on the applicable trust services criteria. Attachment A presents the types of complementary subservice organization controls assumed in the design of Realized Holdings' controls. Attachment A does not disclose the actual controls at the subservice organization.

Attachment A indicates that complementary user entity controls are necessary, along with controls at Realized Holdings, to achieve Realized Holdings' service commitments and system requirements based on the applicable trust services criteria. Attachment A presents the complementary user entity controls assumed in the design of Realized Holdings 's controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period August 1, 2023 to October 31, 2023, to provide reasonable assurance that Realized Holdings' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, Privacy, and Processing Integrity (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Privacy, and Processing Integrity, (With Revised Points of Focus—2022) in AICPA, Trust Services Criteria. Realized Holdings' 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 titled "Realized Holdings, Inc.'s Principal Service Commitments and System Requirements".

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 1, 2023, to October 31, 2023, if complementary subservice organization controls and complementary user entity controls were effective, to provide reasonable assurance that Realized Holdings' service commitments and system requirements were achieved based on the applicable trust services criteria.

Realized Holdings, Inc.

March 1, 2024

ATTACHMENT A

REALIZED HOLDINGS, INC.'S DESCRIPTION OF ITS INVESTMENT PROPRIETARY WEALTH MANAGEMENT SERVICES SYSTEM

COMPANY BACKGROUND

Realized Holdings, Inc. ("Realized") is a privately held company established in March of 2015 that offers Investment Property Wealth Management (IPWM) Services. Realized is a corporation headquartered in Austin, Texas.

DESCRIPTION OF SERVICES OVERVIEW

The IPWM Services System provides an end-to-end platform for Wealth Managers, Brokers, and Registered Investment Advisors to manage their clients' investment property wealth assets including the following:

- Portfolio construction and analysis
- Risk quantification and analysis
- Investment options due diligence and underwriting
- Investment plan preparation and presentation
- Maintenance of client and account information
- Investment documents storage and retrieval
- Ongoing investment surveillance and valuation

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The system description is comprised of infrastructure, software, people, data, and procedures.

INFRASTRUCTURE

The Realized application infrastructure is located at Azure's data centers. Azure acts as a hosting subservice organization for the company. The subservice organization provides physical security and environmental protection controls, as well as managed services for Realized's infrastructure.

Azure's network security uses hardware and software-based intrusion prevention, advanced content filtering, anti-malware, and anti-spam modules.

In addition to the firewall, Realized's uses anti-virus and anti-spyware applications to protect systems from viruses.

Realized maintains a system inventory that includes virtual machines (Azure compute instances), computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, device type, vendor function, OS, location, and notes.

Multiple controls are installed to monitor traffic that could contain malicious programs or code. External perimeter scans are performed annually by a third-party vendor to expose potential vulnerabilities to the production environment and corporate data. Email is scanned at the gateway

and in the hosted email environment. Server operating systems utilize anti-virus and anti-spyware programs. All employee workstation computers have a minimum standard hardware and software configuration. Employees are not allowed to install any software on Realized-owned computers. The IT staff maintains several replacement computers that can replace workstations in need of repair or maintenance, thereby disrupting the employee's workday as little as possible.

SOFTWARE

Realized maintains a list of critical software in use within its environment. The organization also retains appropriate software license documentation.

- Microsoft Office 365
- Salesforce
- Hubspot
- Sharefile
- Github

PEOPLE

The Realized staff provides support to the above services. Realized employs dedicated team members to handle all major product functions, including operations, and support. The IT Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the Realized and its data secure.

Realized's corporate structure includes the following roles:

Chief Executive Officer (CEO) – Handles the strategic direction of the organization. The CEO assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments.

Chief Financial Officer (CFO) – Responsible for overseeing the Company's financial assets and strategy including financial planning, budgeting, reporting, and implementation of risk management programs.

Chief Marketing Officer (CMO) – Responsible for the outward communication of company initiatives. Primary role responsible for exposing new programs to prospects and existing customers and furthering the public reach of Realized.

Chief Revenue Officer (CRO) – This role is responsible for customer relations and working closely with both the CMO and Wealth Management personnel to ensure there is transparency between marketing and sales efforts.

Chief Compliance Officer (CCO) – This role is responsible for establishing, monitoring, and enforcing policies and procedures designed to ensure Realized complies with all regulatory requirements and ensures that clients' interests are protected.

Wealth Management - Primary role for outbound reach to prospects and completing sales. They are also responsible for the maintenance and renewal of existing customer contracts.

Chief Technology Officer (CTO) – Responsible for the technological direction and advancements of the organization. Directs the operations, engineering, and support teams to efficiently create/present new services, maintain existing ones, and help support the Realized customer base using the service.

Operations and Technical Support – These roles include the support team and cross-over to the engineering team. It is primarily responsible for daily support aspects of the business. This includes but is not limited to the support of end-users with day-to-day issues, as well as assisting in the onboarding, implementation, and migrations of new and existing customers as part of their ongoing maintenance.

DATA

Customer data is managed, processed, and stored by the relevant data protection and other regulations, with specific requirements formally established in customer agreements. Customer data is captured which is utilized by Realized in delivering its System.

The information takes many forms. It may be stored on computers, transmitted across networks, printed, or written on paper, and spoken in conversations. All employees and contractors of Realized are obligated to respect and, in all cases, to protect confidential and private data. Customer information, employment-related records, and other intellectual property-related records are subject to limited exceptions, and confidential as a matter of law. Many other categories of records, including company and other personnel records, and records relating to Realized's business and finances are, as a matter of Realized policy, treated as confidential. Responsibility for guaranteeing appropriate security for data, systems, and networks is shared by the Client Services and IT Departments. IT is responsible for designing, implementing, and maintaining security protection and retains responsibility for ensuring compliance with the policy. In addition to management and the technology staff, individual users are responsible for the equipment and resources under his or her control.

Realized has established guidelines for the retention and disposal of confidential and private information. These guidelines are reviewed at least annually. The destruction of data is a multi-step process. A ticket is created and assigned to the product team and system engineering team to coordinate the deletion of the data. First, all files received or generated from the client are identified and deleted by the system engineering team then the product team deletes all user-related data.

Electronic communications are treated with the same level of confidentiality and security as physical documents. Networks are protected by enterprise-class firewalls and appropriate enterprise-class virus protection is in place. Password protection with assigned user rights is required for access to the network, application, and databases. Access to the network, application, and databases is restricted to authorized internal and external users of the system to

prohibit unauthorized access to confidential data. Additionally, access to data is restricted to authorized applications to prevent unauthorized access outside the boundaries of the system.

PROCEDURES

Formal IT policies and procedures exist that describe logical access, computer operations, change management, incident management, and data communication standards to obtain the stated objectives for network and data security, data privacy, and integrity for both the company and its clients and define how services should be delivered. These are communicated to employees and are located within the organization's intranet.

Reviews and changes to these policies and procedures are performed annually and are approved by senior management.

Human Resources Policies and Procedures

Realized has formal hiring procedures that are designed to ensure that new team members can meet or exceed the job requirements and responsibilities. All candidates go through interviews and assessments of their education, professional experience, and certifications. Background checks are performed for all newly hired employees before the start date and include a review of their education and criminal records.

During the onboarding process, the new employees review the Employee Handbook, Code of Conduct, and any other relevant policies and procedures relevant to their role. Newly hired employees are required to sign an acknowledgment of receipt and understanding of the Employee Handbook and Code of Conduct. These policies and procedures are also available to employees through the internal policies repository. Security awareness training is also completed at least annually by all employees that include the areas of security and confidentiality to communicate the security implications around their roles and how their actions could affect the organization.

Ongoing performance feedback is provided to all employees and contractors. Formal performance reviews are completed semi-annually by management to discuss expectations, goals, and the employee's performance for the last fiscal year.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

Realized Holdings uses a subservice organization to provide hosting services. The management of Realized Holdings receives and reviews the SOC 2 report of Microsoft Azure on an annual basis. In addition, through its daily operational activities, the management of Realized Holdings monitors the services performed by Microsoft Azure to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively to meet Realized Holdings' service commitments and system requirements based upon the security, availability, confidentiality, privacy, and processing integrity trust services criteria.

The assertion indicates that certain applicable trust services criteria can be met only if the Subservice Organizations controls, assumed in the design of Realized Holdings controls, are suitably designed and operating effectively along with related controls at the service organization.

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

Realized Holdings' 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 Trust Services Criteria related to Realized Holdings' services to be solely achieved by Realized Holdings control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Realized Holdings.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services 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.

- Controls to provide reasonable assurance that user access including the provisioning and de-provisioning are designed appropriately and operating effectively.
- User entities are responsible for reporting issues with Realized Holdings systems and platforms.
- User entities are responsible for understanding and complying with their contractual obligations to Realized Holdings.
- User entities are responsible for notifying Realized Holdings of changes made to the administrative contact information

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Realized Holdings designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Realized Holdings makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Realized Holdings has established for the services. The system services are subject to security, availability, confidentiality, privacy, and processing integrity.

Realized Holdings' commitments to users are communicated through Service Agreements, online Privacy Policies, Information Security Policies, and in the description of the service offered provided online.

Commitments

Security, availability, confidentiality, privacy, and processing integrity commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

Security commitments include, but are not limited to, the following:

- System features and configuration settings are designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system.
- Regular vulnerability scans over the system and network
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Use of data retention and data disposal
- Uptime availability of production systems

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a reasonably timely manner.
- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities; and,
- Operational procedures supporting the achievement of availability commitments to user entities.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit.
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between Realized and user entities.

Privacy commitments include, but are not limited to, the following:

- The company defines documents, communicates, and assigns accountability for its privacy processes and procedures.
- The company provides notice about its privacy processes and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
- The company describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
- The company collects personal information only for the purposes identified in the notice.
- The company limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent.
- The company provides individuals with access to their personal information for review and updates.
- The company discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
- The company protects personal information against unauthorized access (both physical and logical).
- The company maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
- The company monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

Processing Integrity commitments include, but are not limited to, the following:

- Controls exist to prevent or detect and correct processing errors to meet the entity's processing integrity commitments and system requirements.
- System inputs are measured and recorded completely, accurately, and timely to meet the entity's processing integrity commitments and system requirements.
- Data is processed completely, accurately, and timely as authorized to meet the entity's processing integrity commitments and system requirements.
- Data is stored and maintained completely, accurately, and promptly for its specified life span to meet the entity's processing integrity commitments and system requirements.

- System output is complete, accurate, and distributed to meet the entity's processing integrity commitments and system requirements.
- Modification of data, other than routine transaction processing, is authorized and processed to meet the entity's processing integrity commitments and system requirements.

Realized Holdings establishes operational requirements that support the achievement of security, availability, confidentiality, privacy, processing integrity and relevant laws and regulations, and other system requirements. Such requirements are communicated in system policies and procedures, system design documentation, and agreements with customers. 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, how the internal business systems and networks are managed, and how employees are hired and trained. In addition, how to carry out specific manual and automated processes required in the operation and development of the System.