System and Organization Controls (SOC) 3 Report

Management's Report of Its Assertions on iRely, LLC's Solutions System Based on the Trust Services Criteria for Security, Availability, and Confidentiality

For the Period May 1, 2023 to October 31, 2023

Independent SOC 3 Report for Security, Availability, and Confidentiality Trust Services Criteria for iRely, LLC.

TABLE OF CONTENTS

SECTION ONE: REPORT OF INDEPENDENT ACCOUNTANTS

To: Management of iRely, LLC

Scope

We have examined management's assertion, contained within the accompanying "Management's Report of Its Assertions on the Effectiveness of Its Controls over iRely, LLC's Solutions System based on the Trust Services Criteria for Security, Availability, and Confidentiality" (Assertion) that iRely, LLC's controls over the Solutions System (System) were effective throughout the period May 1, 2023 to October 31, 2023, to provide reasonable assurance that its principal 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* (AICPA, *Trust Services Criteria*).

The Assertion also indicates that iRely, LLC 's ("Service Organization" or "iRely") controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of iRely's infrastructure's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

iRely uses a subservice organization to provide cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at iRely to achieve iRely's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system 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 suitable design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

iRely management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Solutions System and describing the boundaries of the System;

- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of the System; and
- Identifying, designing, implementing, operating, and monitoring effective controls over the Solutions System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Assertion, 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 our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes:

- Obtaining an understanding of iRely's Solutions System relevant to Security, Availability, and Confidentiality policies, procedures, and controls;
- Testing and evaluating the operating effectiveness of the controls; and
- Performing such other procedures as we considered necessary in the circumstances.

The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating iRely's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program. We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements related to our examination engagement.

Inherent Limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design and operating effectiveness of the controls to achieve iRely's Solutions System's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system of controls, may alter the validity of such evaluations.

Opinion

In our opinion, management’s assertion that the controls within iRely’s Solutions System were effective throughout the period May 1, 2023 to October 31, 2023 to provide reasonable assurance that iRely’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

CyberGuard Compliance, LLP

January 3, 2024
Las Vegas, Nevada

SECTION TWO: MANAGEMENT'S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER IRELY, LLC'S SOLUTIONS SYSTEM BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY, AVAILABILITY, AND CONFIDENTIALITY

January 3, 2024

Scope

We, as management of iRely, are responsible for:

- Identifying the iRely's Solutions System (System) and describing the boundaries of the System, which are presented in the section below (Attachment A) titled iRely, LLC's Description of the Solutions System (Description);
- Identifying our principal service commitments and system requirements (Attachment B);
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in the section below (Attachment B)
- Identifying, designing, implementing, operating, and monitoring effective controls over iRely's Solutions System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements; and
- Selecting the trust services categories that are the basis of our assertion.

In designing the controls over the System, we determined that certain trust services criteria can be met only if complementary user entity controls are suitably designed and operating effectively for the period May 1, 2023 to October 31, 2023.

iRely uses a subservice organization to provide cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at iRely, to achieve iRely's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization.

We assert that the controls within the system were effective throughout the period May 1, 2023 to October 31, 2023, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to Security, Availability, and Confidentiality set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy, if subservice organizations and user entities applied the complementary controls assumed in the design of iRely’s Solutions System controls throughout the period May 1, 2023 to October 31, 2023.

iRely, LLC

ATTACHMENT A: IRELY, LLC'S DESCRIPTION OF ITS SOLUTIONS SYSTEM

System Overview

The System is comprised of the following components:

- ***Infrastructure -*** The physical and hardware components of a system (facilities, equipment, and networks)
- ***Software -*** The programs and operating software of a system (systems, applications, and utilities)
- ***Data -*** The information used and supported by a system (transaction streams, files, databases, and tables)
- ***People -*** The personnel involved in the operation and use of a system (developers, operators, users, and managers)
- ***Procedures -*** The automated and manual procedures involved in the operation of a system

Infrastructure

The operations and corporate facilities are located in Fort Wayne, Indiana, USA. iRely utilizes a combination local area network ("LAN") / wide area network ("WAN") to share data among its employees. The IT data center is managed through Microsoft Azure and is monitored 24 hours a day, 7 days a week, and 365 days a year to authorized iRely personnel. iRely uses internal IT expertise and follows internal business and IT policies and procedures to support its daily IT administration and service operations.

iRely Solutions are hosted in Microsoft Azure across multiple Availability Zones for redundancy and disaster recovery purposes. iRely does not own or maintain any hardware in the Microsoft Azure data centers. Services operate within a shared security responsibility model, where Microsoft Azure is responsible for the security of the underlying cloud infrastructure, and iRely is responsible for securing iRely Solutions deployed in Azure (e.g., IAM, Azure IaaS virtual machines, Operating System and application security, Security Group configurations, network traffic monitoring).

Dedicated hosted customers are separated and have containerized production, staging, and development environments. Access to Azure production instances is allowed only through an encrypted VPN from iRely's corporate network to ensure the privacy and integrity of data transmitted over the public network. VPN connections are whitelisted to IRely's IPs and are secured using AES-128 bit or greater encryption. Access is restricted to authorized administrators, who must authenticate via an encrypted VPN through a secure SSH key, Microsoft IAM roles, and multi-factor authentication.

Production instances at Azure are logically and physically separate from IRely's internal corporate network. All container hosts and database servers run on virtual machines. Pulseway provides health, resource, and performance monitoring management of the production systems based on a defined template, which allows Integrate to deploy and configure consistently hardened instances.

All container hosts and database servers run on virtual machines that are secured via Network Security Groups. Agent based remote Security tools monitor incoming network traffic by analyzing data packets and filtering traffic based on an Integrate-defined ruleset. Access to manage the Security Groups is restricted to authorized IT personnel, and changes to these rulesets are governed by iRely's change management policy, which includes documenting, testing, and approving the change.

iRely Helpdesk Customer Portal

The user-facing Helpdesk portal is a front-end application for customers to access their services/channel. This application allots customers dedicated support staff.

Software

The iRely Solutions consists of the following components:

- *Commodity Procurement Software* – automates business processes, integrates seamlessly with ERP systems, and digitally connects customers to their business partners, simplifying global trade management.
- *Enterprise Petroleum Distribution Software* – a collaborative and comprehensive accounting solution suited for multi-line petroleum wholesalers, propane distributors, carriers, and convenience store management.
- *Retail Software* – a high margin inventory solution that integrates customer's merchandise tracking and consolidated and leveraged retail data.
- *Agribusiness Software* – field planning automation solution for integrated agricultural businesses.

Data

Inbound integrations to the iRely's i21 System are configured with third parties via iRely-developed APIs. Additionally, Media Partners, Publishers, and Sellers transfer contact data to iRely via manual upload within the front-end application.

iRely validates, stores, and processes contact data within the iRely i21 platform. Data is stored on database servers running SQL within the production virtual server. All data is encrypted at rest, and SSL encrypts data in transit between the container and databases. Data is also encrypted between iRely's internal and external technological resources. processing.

Processed contact data is provided to customers in various ways:

- Customers can access the processed contact data via the iRely Solutions.
- Reports of processed contact data can be configured to send to customers via SMTP, a cloud-based email delivery platform, on a defined schedule.
- Outbound integrations via APIs send processed contact data to third-party marketing automating platforms, CRMs, and Custom Data Platforms.

Under a managed services agreement, iRely manages the product on behalf of the customer. As part of these services, iRely typically provides reports of activity and change status to the customer, but if processed contact data needs to be shared with the customer outside of the platform, secure file sharing software is used.

People

The following functional roles/teams comprise the framework to support effective controls over governance, management, security, and operation:

- *The Board of Directors* establishes business and strategic objectives to meet the interests of stakeholders and provides independent oversight of financial and operational performance. The board of directors meets with the executive management team on a quarterly basis, or more frequently as needed. Management presents operational and third-party assessment results to the board of directors upon completion. Board attendance is tracked, and discussion points and decisions are documented in board minutes. The board operates under bylaws that define responsibilities, including the oversight of management's system of internal control. The board consists of sufficient members who are independent from management and are objective in making decisions.
- *Executive Management* oversees, and is ultimately responsible for, all aspects of service delivery and security commitments. Among other responsibilities, Executive Management ensures that controls are enforced, risk assessment/management activities are approved and prioritized, people are appropriately trained, and systems and processes are in place to meet security and service requirements.
- *Human Resources (HR)* is responsible for managing all functions related to recruiting and hiring, employee relations, performance management, training, and resource management. Human Resources partners proactively with Executive Management and business units to ensure that all initiatives are appropriately aligned with iRely mission, vision, and values.
- *Information Technology (IT)* management has overall responsibility and accountability for the enterprise computing environment. IT Technical personnel administer systems and perform services supporting key business processes, including architecting and maintaining secure and adequate infrastructure, monitoring network traffic, and deploying approved changes to production. The Development &

Engineering team is responsible for application development, initial testing of changes, and troubleshooting/resolving application issues.

- *Information Security* is responsible for performing assessing and managing risk, defining control objectives, monitoring performance of security controls, addressing and responding to security incidents, maintaining, and communicating updates to security policies, and conducting security awareness training of all users.
- *Customer Success Managers (CSM)* are responsible for initiating the creation of new customer instances on the iRely i21 System platform, adding users to new customer instances, providing user documentation to and coordinating training for new customers, and overall management of the account to ensure continued customer satisfaction.
- *Customer Support* is responsible for creating new customer instances on the iRely i21 System platform, fielding customer calls regarding iRely Solutions, initiating and responding to help desk tickets based on customer requests, and communicating with customers regarding any issues or outages.

iRely is committed to equal opportunity of employment, and all employment decisions are based on merit, qualifications, and abilities. Employment-related decisions are not influenced or affected by an employee's race, color, nationality, religion, sex, marital status, family status, sexual orientation, disability, or age. iRely endorses a work environment free from discrimination, harassment, and sexual harassment.

Procedures

iRely has a Chief Information Officer (CIO) who is responsible for the design and oversight of security and privacy initiatives. The CIO reports directly to the CTO and indirectly to the Chief Executive Officer (CEO). The IT policy framework describes the procedures followed to ensure the performance of consistent processes over the security, availability, confidentiality, and operation of all iRely Solutions. All IT policies are reviewed on an annual basis, or more frequently as needed, by the CIO.

All employees are expected to adhere to iRely's IT policy framework as acknowledged during new hire onboarding and during annual security awareness training. The IT policy framework includes procedures that provide guidance on the consistent performance of controls and processes necessary to meet service commitments and system requirements.

Incident Disclosure

No security incidents were detected or reported during the audit period that would affect IRely's service commitments or system requirements.

Complementary Subservice Organization Controls

Certain principal service commitments and system requirements can be met only if complementary subservice organization controls (CSOC) assumed in the design of iRely's controls are suitably designed and operating effectively at the subservice organizations, along with related controls at iRely.

Description of Complementary User Entity Controls

iRely controls were designed with the assumption that certain controls would be implemented by user entities (or "customers"). Certain requirements can be met only if complementary user entity controls assumed in the design of iRely's controls are suitably designed and operating effectively, along with related controls at iRely.

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Company Background

iRely, LLC was founded in 1983 with the objective of providing unified software solutions for agribusiness and petroleum distribution clients. Based upon objective business metrics such as return on investment, lower total cost of ownership and increased productivity. These solutions are delivered via a lifecycle services model that has been designed to help ensure excellence in execution, financial management, and customer satisfaction. The organization is based in Fort Wayne, Indiana. iRely's web-based services and their related controls, including system redundancy, are key differentiators in providing and maintaining high availability, and 24/7 access for customers.

Description of Services Provided

iRely's Technologies are divided into two divisions with industry solutions designed to address business needs for i21 Software Technology Services and iRely Cloud-based Hosting Services:

- iRely Technology Services provide technology solutions for Commodities, Retail, Agriculture, and Petroleum Distribution companies that need a web-based platform to perform their daily information management.
- iRely Cloud-based Services provide organizations with secured hosting and 24/7 support. At the same time, iRely also provides a web-based system for organizations to access, review, edit and perform other management activities related to their information.

The iRely Solutions consists of the following components:

- *Commodity Procurement Software* – automates business processes, integrates seamlessly with ERP systems, and digitally connects customers to their business partners, simplifying global trade management.
- *Enterprise Petroleum Distribution Software* – a collaborative and comprehensive accounting solution suited for multi-line petroleum wholesalers, propane distributors, carriers, and convenience store management.
- *Retail Software* – a high margin inventory solution that integrates customer's merchandise tracking and consolidated and leveraged retail data.
- *Agribusiness Software* – field planning automation solution for integrated agricultural businesses.

Principal Service Commitments and System Requirements

iRely's Security, Availability, and Confidentiality commitments to customers are documented and communicated to customers in the Master Services Agreement and the description of service document published on the customer-facing website. The principal Security, Availability, and Confidentiality commitments include, but are not limited to:

- Maintain appropriate administrative, physical, and technical safeguards to protect the security and integrity of the iRely Solutions and the customer data in accordance with iRely's security requirements.
- Perform annual third-party security and compliance audits of the environment, including, but not limited to:
  - Reporting on Controls at a Service Organization Relevant to Security, Availability, Confidentiality, Processing Integrity, or Privacy (SOC 2) examinations.
- Use formal HR processes, including background checks, code of conduct and company policy acknowledgements, security awareness training, disciplinary processes, and annual performance reviews.
- Follow formal access management procedures for the request, approval, provisioning, review, and revocation of iRely personnel with access to any production systems.
- Prevent malware from being introduced to production systems.
- Continuously monitor the production environment for vulnerabilities and malicious traffic.
- Use industry-standard secure encryption methods to protect customer data at rest and in transit.
- Transmit unique login credentials and customer data via encrypted connections.
- Maintain an availability SLA for customers of 99.5% uptime for each calendar quarter.
- Maintain a disaster recovery and business continuity plan to ensure availability of information following an interruption or failure of critical business processes.
- Maintain and adhere to a formal incident management process, including security incident escalation procedures.
- Maintain confidentiality of customer data and notify customers in the event of a data breach.
- Identify, classify, and properly dispose of confidential data when retention period is reached and/or upon notification of customer account cancellation.

iRely establishes system and operational requirements that support the achievement of the principal service commitments, applicable laws and regulations, and other system requirements. These requirements are communicated in iRely's policies and procedures, system design documentation, and/or in customer contracts. Information Security policies define how systems and data are protected. These policies are updated as appropriate based on evolving technologies, changes to the security threat landscape, and changes to industry standards, provided any updates do not materially reduce the service commitments or overall service provided to customers as described in the customer contracts.

iRely regularly reviews Security, Availability, and Confidentiality controls and performance metrics to ensure these commitments are met. If material changes occur that reduce the level of Security, Availability, and Confidentiality commitments within the agreement, iRely will notify the customer via the iRely website or directly via email.