



REALIZED SOLUTIONS

THE COMPREHENSIVE IT SERVICES

SOC 3 REPORT

*Independent Service Auditor's Report
On a Service Organization's Description of
Its System and the Suitability of the Design
and Operating Effectiveness of Its Controls
Relevant to Security and Availability*

For the Period June 1, 2024 to May 31, 2025



INDEPENDENT SERVICE AUDITOR'S REPORT

TABLE OF CONTENTS

SECTION 1	INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2	MANAGEMENT ASSERTION OF RSI	4
SECTION 3	DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM	6
	OVERVIEW OF OPERATIONS	7
	Company Background	7
	Description of Services Provided	7
	Disaster Recovery	14
	CONTROL ENVIRONMENT	15
	Integrity and Ethical Values	15
	Commitment to Competence	15
	Board of Directors' Participation	16
	Management's Philosophy and Operating Style	16
	Organization Structure and Assignment of Authority and Responsibility	17
	Human Resource Policies and Practices	17

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Realized Solutions, Inc.,

Scope

We have examined Realized Solutions, Inc.'s (RSI) accompanying management's assertion found in Section 2 titled "Management Assertion of RSI" (assertion) that the comprehensive IT services and systems (system) were effective throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that RSI's principal service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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)*.

RSI uses various third-party data centers (subservice organizations) to house its critical production computer servers, applications and networking equipment. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at RSI, to achieve RSI's service commitments and system requirements based on the applicable trust services criteria. The description presents RSI's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of RSI's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Service Organization's Responsibilities

RSI 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 RSI's service commitments and system requirements were achieved. RSI has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, RSI 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 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, in all material respects, management's assertion is fairly stated. 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 risk that controls were not effective to achieve RSI'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 RSI'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 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 organizations' service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within RSI's comprehensive IT services were effective throughout the period June 1, 2024 to May 31, 2025 to provide reasonable assurance that RSI's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of RSI's controls were effective throughout that period.

The Moore Group CPA, LLC

Nashua, NH
July 2, 2025

SECTION 2
MANAGEMENT ASSERTION OF RSI



MANAGEMENT ASSERTION OF REALIZED SOLUTIONS

July 2, 2025

We are responsible for designing, implementing, operating, and maintaining effective controls within Realized Solutions, Inc.'s (RSI) comprehensive IT services and systems (system) throughout the period June 1, 2024 to May 31, 2025 to provide reasonable assurance that RSI's service commitments and system requirements relevant to security and availability (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented in Section 3 titled "Description of the Service Organization's System Provided by RSI Management" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that RSI's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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*). RSI's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements related to the applicable trust services criteria presented in Section 3.

RSI uses various third-party data centers (subservice organizations) to house its critical production computer servers, applications and networking equipment. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at RSI, to achieve RSI's service commitments and system requirements based on the applicable trust services criteria. The description presents RSI's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of RSI's controls. The description does not disclose the actual controls at the subservice organizations.

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

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 June 1, 2024 to May 31, 2025 to provide reasonable assurance that RSI's service commitments and system requirements were achieved based on the applicable trust services criteria.

SECTION 3

DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM PROVIDED BY RSI MANAGEMENT

OVERVIEW OF OPERATIONS

Company Background

Founded in 2003, Realized Solutions, Inc. (RSI) provides comprehensive information technology (IT) services and consulting to assist customers in optimizing their technology systems and improving their workflow procedures. By routinely reviewing internal processes and system applications, RSI works with customers to increase hardware and network reliability and implement creative solutions to increase efficiency and security. RSI looks for cost effective ways to eliminate duplicate entries, automate manual processes, improve data quality, increase reporting speed, and bridge systems to save customers time, effort, and resources. RSI's team works proactively to maintain customer systems to keep things running smoothly so that customers are able to focus on their core business.

Scope

The scope of this SOC report includes an assessment of the general organizational and information technology controls supporting the comprehensive IT services and systems of RSI. The scope explicitly excludes any evaluation, assurance, or commentary regarding the entity's banking operations, fraud prevention or detection mechanisms, cash receipts or disbursement processes, accounting functions, or any other internal or external financial responsibilities of RSI. In addition, this report does not constitute an audit, review, or examination of financial statements or financial information, nor does it provide any form of assurance regarding the integrity, accuracy, or completeness of financial reporting, anti-fraud measures, or compliance with financial regulations. The responsibility for the adequacy and effectiveness of controls related to financial operations, fraud prevention or detection, and regulatory compliance remains solely with RSI.

Users of this report should not rely on it as a substitute for performing their own due diligence or for obtaining other audits or assessments relevant to financial, operational, or regulatory matters outside the defined scope.

Description of Services Provided

RSI's services are broken down into two primary categories: Support Services and Development Services. The detailed services provided under these categories are as follows:

Support Services

- **Network Service Support** – RSI is a full-service IT supplier specializing in network services and hardware support. RSI can function as a company's IT Department or can act as a supplement to in-house IT staff to manage tasks such as establishing firewall security, updating desktop applications, managing system backups, setting up new users, overseeing the email system, or troubleshooting hardware issues.
- **Maintenance Plans** – RSI offers various levels of monthly support to meet the individual needs of businesses. From complete 24/7 network, hardware, and labor coverage on servers, desktops, and network devices to "cherry picked" coverage and monitoring service on selected units, RSI works with customers to create a proactive support plan that adequately fits their business needs and budget. RSI's proactive system monitoring provides automated alerts, allowing RSI to mitigate potential problems and keep businesses up and running before costly issues arise.

- **Backup and Disaster Recovery** – Implementing a business continuity plan protects businesses from the irreparable harm an unplanned event or natural disaster can have on a business. RSI helps customers establish a convenient and secure backup and disaster recovery plan. Advancements in technology, including the use of virtual servers, make backing up system data more secure, reliable, and convenient. Forward thinking companies are transitioning to increasingly secure backup models to preserve their historical data. These models allow businesses to be operational within only hours of a catastrophic event, including hardware failures, lightning strikes, power outages, etc., which significantly eliminates costly productivity and data losses that could have severe impacts on a business.
- **Cloud Computing** – Cloud computing is a hosted solution which does not require an on-site server. Instead, applications are hosted at a secure offsite data center, many of which offer guaranteed up time and accessibility. Cloud computing is a powerful, cost effective, and reliable option for many applications and business needs. Cloud-based or hosted applications free organizations from the expense of purchasing and maintaining an on-site server. They are generally budget friendly and are ideal for companies with multiple locations or those that wish to support telecommuting initiatives. RSI helps customers assess and determine what cloud-based applications make sense for customer objectives, needs, and budget.

Development Services

- **Analysis and Consultation** – RSI's experienced professionals assess business processes, operations, and systems to help companies find more efficient ways to process and utilize data. RSI identifies, prioritizes, and makes recommendations for areas that could be improved. These areas often include recommendations for automating manual processes, eliminating duplicate data entry, integrating multiple software systems, and suggestions for ways to improve data accuracy and reporting speeds.
- **Custom Software and Application Development** – RSI employs a team of certified software developers who are experienced with all aspects of software development, including the planning stage, design specification and engineering, development, implementation, deployment, and training process to ensure the success of a software development project.
- **System Integrations** – RSI helps businesses get more out of their existing software systems by building an interface or bridge between them. The interface allows information to flow from one system to another, facilitating improved data quality and reporting, limiting manual processes, and reducing duplicate data entry. Implementing simple interfaces can vastly improve a business' efficiency, freeing-up resources to dedicate their skills to more productive revenue generating activities.
- **Sage ERP** – RSI has extensive experience integrating with and building software utilities that work in conjunction with Sage's ERP accounting software. RSI has written supply chain management, global tracking, forecasting, inventory management, and claim systems that complement Sage's ERP software and improve functionality, increase communication, and broaden reporting capabilities.
- **Custom Software Support and Maintenance:** After deploying the custom software systems, integrations, or middleware RSI writes for customers, RSI offers monthly maintenance and support contracts for the software. These contracts cover bug fixes and platform updates on a customer's given software. Further, the contracts allow RSI to keep customer software current and increasingly secure on the newer supported versions of .Net, XML, etc. adding value and extending the life of their software system investment.

Principal Service Commitments and System Requirements

RSI makes service commitments to its customers and has established system requirements as part of the comprehensive IT services. Some of these commitments are principal to the performance of the service and relate to the applicable trust services criteria. RSI 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 RSI's service commitments and system requirements are achieved.

Service commitments to customers are documented and communicated in RSI's policies and procedures, system design documentation, customer agreements, or other written company materials provided to user entities as well as in the description of the service offering provided online. Service commitments include, but are not limited to, the following:

- **Security:** RSI has made commitments related to a secure information technology control environment and complying with relevant laws and regulations. These commitments are addressed through measures including data encryption, authentication mechanisms, physical security, and other relevant security controls.
- **Availability:** RSI has made commitments related to providing reliable and consistent uptime and connectivity for the IT systems used in the services offered by RSI. These commitments include, but are not limited to, design, development or acquisition, implementation, monitoring, and maintaining environmental protection of systems, software, data back-up processes, and recovery infrastructure to meet availability commitments.

RSI has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in its system policies and procedures, system design documentation, and customer agreements. 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 to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of various RSI services.

Components of the System

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the description of services and the components of infrastructure, software, people, procedures, and data.

The components of the system used to provide the services are as follows:

Infrastructure

RSI's main corporate office is located in Southington, CT. A physical key access system is utilized by RSI to provide authorized entry to external doors outside of normal business hours to employees. An electronic access system is used to gain entry into the corporate suite. Accesses are logged for further review.

The corporate suite utilizes intrusion detection and motion detection sensors located on exterior doors to alert upon entry outside of the main entrance. Office spaces with windows use motion detectors to detect unplanned activity. Certain events involving unplanned access to the facility trigger automatic alarms that notify the appropriate personnel.

A secure server room is maintained in the corporate suite for the internal network and development systems that are used for testing and quality assurance of customized application changes before they are rolled out to production or customer systems. The server room is monitored by surveillance cameras that automatically send an image capture via email to designated personnel whenever motion is detected. Video data is retained for future review.

Environmental controls include but are not limited to fire detection and wet pipe sprinkler systems throughout the facility. UPS systems provide power in the event of disruption of the main power feed, allowing for gradual, safe shutdown of critical computer systems.

Computer operations generally may be threatened with downtime in several areas:

- Equipment failure
- Catastrophic event
- Attack

RSI has implemented controls to mitigate these risks, including:

- Equipment maintenance contracts
- Inventory of spare equipment
- Systems redundancy
- Network redundancy
- Power redundancy
- Firewall Internet Load Balancing
- OS and critical application patches

Third-party enterprise monitoring applications are used to monitor system downtime and operations issues to help ensure that system downtime and performance does not exceed predefined levels. This includes monitoring of both critical network and server hardware, as well as processes and services. The enterprise monitoring application is configured to send alert notifications to operations personnel when predefined metrics are exceeded on monitored network devices. Alerts are communicated via SMS text or email to appropriate support personnel.

RSI employs two-factor authentication for authenticating to the internal network domain, administrative access to production systems in the cloud, and remote access into the internal network domain.

Servers and workstations utilize a third-party next generation antivirus, endpoint detection and response (EDR), and 24/7 threat hunting service. Windows Server operating system patches for critical production systems are updated automatically after adequate testing to ensure that no production interference will result. Other servers and workstations are automatically updated via a Remote Monitoring and Management (RMM) application, in which a central monitoring server pushes updates after approval.

Software

Subservice Organizations - A combination of custom developed and commercial applications is utilized to support the comprehensive IT services provided to user entities. The applications run on Windows operating systems located on enterprise grade server platforms with commercial databases to support the applications located in Amazon Web Services (AWS) cloud. RSI uses

ConnectWise to track time and progress on tickets for all projects and work events. Because all work is logged and tracked through a single point of entry, RSI is able to collect information about all aspects of services. ConnectWise is an industry-standard software that has been integrated into RSI's systems for years. This tool is used to reinforce RSI's managed maintenance methodology and to capture the metrics needed to track performance. RSI can then successfully use this information to improve upon business operations, efficiency and productivity. ConnectWise utilizes the services and controls of Amazon Web Services (AWS) to offer these services to manage customer systems and accounts. AWS had a SOC 2 audit completed for the review period October 1, 2023 to September 30, 2024. The scope of this audit does not include the controls of ConnectWise or Amazon Web Services.

RSI also utilizes the services and controls of Microsoft 365 for housing critical email communications and certain customer information. The Microsoft 365 data center had a SOC 1 Type 2 audit completed for the review period of October 1, 2023 to September 30, 2024. The scope of this audit does not include the controls of Microsoft 365.

Software consists of the programs and software that support the applications within the scope of the description. The list of software and ancillary software used to build, support, secure, maintain, and monitor the comprehensive IT services includes the following applications, as shown in the table below:

Component	Description
Hosting Systems	Microsoft Azure Microsoft 365 AWS Elastic Cloud Compute (EC2)
Storage, Database, and Backups	Microsoft OneDrive Microsoft SharePoint Microsoft SQL Server Veeam Backup and Replication
Network and Firewall	Cisco Meraki Firewall CrowdStrike Endpoint Detection and Response
Build, Release, Continuous Integration Systems, and Change Management	Azure DevOps Version Control ConnectWise PSA Change Management
Access Management	Windows Active Directory Azure Active Directory Duo Multifactor Authentication
Monitoring, Alerting, Analytics, and Ticketing	ConnectWise PSA Ticketing Kaseya Datto RMM Liongard Attack Surface Management Platform

Component	Description
Vulnerability Scanning	RapidFire Tools Vulnerability Scanning Network Detective
Human Resource	TriNet HR Management DISA Background Screening

People

RSI is led by its CEO, John W. Beyer, and executives in the departmental areas of Software Development, Project Management and Marketing. RSI's organization structure provides the overall framework for planning, directing, and controlling operations. Personnel and business functions are separated into departments according to job responsibilities. The structure provides defined responsibilities and lines of authority for reporting and communication. The assignment of roles and responsibilities within the various departments provides effective segregation of duties.

In the Control Environment section of this report, additional information is described related to organizational controls implemented at RSI. These organizational controls are intended to serve as the internal foundation for providing services to its customers.

Procedures

RSI has implemented processes and procedures to support the operations and controls over the services and systems provided to its customers. Specific examples of the relevant procedures include, but are not limited to, the following:

- Policies and procedures are in place to guide personnel regarding assessing risks on a periodic basis.
- Security policies are in place to guide personnel regarding physical and information security practices.
- Policies and procedures are in place for identifying the system security requirements of authorized users.
- Third-party enterprise monitoring applications are used to monitor system downtime and operations issues to help ensure that system downtime and performance does not exceed predefined levels.
- RSI has a documented Disaster Recovery plan and Business Continuity plan. The plans are periodically tested.
- An Incident Response Plan is in place to ensure RSI is taking appropriate steps to monitor, identify, and respond to potential IT security incidents that can negatively impact operations of the business.
- Policies and procedures are in place to guide personnel regarding addressing how complaints and requests relating to security issues are resolved.
- Policies and procedures are in place to assign responsibility and accountability for system changes and maintenance.
- Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.
- Management utilizes intrusion prevention systems (IPS) to prevent unauthorized intrusion into the production environment. The IPS subscription for the firewall system is kept current.

- RSI IT personnel utilize security issue monitoring services to keep abreast of recent critical issues, attacks and vulnerabilities that must be addressed immediately.
- Firewall systems are in place to screen data flow between external parties and the RSI network. All inbound and outbound data packets on all interfaces are intercepted and inspected. Packets that are not explicitly permitted by the security policy definition are rejected.
- Policies and procedures are in place to add new users, modify the access levels of existing users, and remove users who no longer need access.
- Production server users are required to authenticate with two-factor authentication utilizing a unique user ID and password and one-time use token before being granted access to the production environment.
- Application users are required to authenticate via an authorized unique user ID and password before being granted access to the production environment. Multifactor authentication is enabled.
- The request to create or modify user access to the hosted user application must be provided by an authorized customer end user.
- Physical security policies and procedures are in place to guide personnel regarding restricting access to the facility.
- Intrusion and motion alarm systems are in place and monitored for all entry/exit points of the facility, including doors and windows. An audible alarm sounds upon triggering.
- Third-party antivirus protection is installed at the network perimeter firewalls to mitigate exposure to virus attacks on the production equipment (perimeter protection).
- Management periodically performs internal security assessments, including reviews of server logs and other critical items.
- Policies and procedures are in place to ensure that design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.
- Policies and procedures are in place to ensure that change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by RSI and typically includes the following defined categories:

- PUBLIC – pertains to all data that does not require specific accountability and/or audit trails for use. The unauthorized disclosure of this data would not cause any adverse impact to RSI's reputation, financials, or client engagements. Such information includes non-strategic information, publicly available information, or non-specific application information.
- INTERNAL – pertains to all information created by an individual user of the internal system and not meant to be generally shared with others. The unauthorized disclosure of this information reasonably could be expected to cause low substantive damage to RSI's reputation, financials, or client relations. Such information and communication of it is intended by the creator for a specific audience only.
- INTERNAL SENSITIVE – pertains to all data having compromising or competitive elements or implications intended strictly for use within RSI. Such information includes but is not limited to basic financial, security, and audit information.

- CONFIDENTIAL – pertains to all data of the highest sensitivity due to its time and financial sensitivity or possible fraud potential. Such data includes all types of identifiable information, social security numbers, health records, account numbers, payroll, personal information, passwords, code, client relations/engagements, and contracts under negotiation.

Access to data is limited to authorized personnel in accordance with RSI's system security policies. RSI is also responsible for the overall availability of data, including system backups, monitoring of data processing, and file transmissions as well as identifying and resolving problems.

Encryption is utilized to protect data in transit, including TLS encryption over HTTPS connections utilized for secure communications between RSI production systems and customer end users. Certain IT engineers access internal network equipment remotely, via secure VPN tunnels protected by two-factor authentication, TLS and IPsec encryption. Laptops are secured with BitLocker disk encryption.

Controls in place specific to the data responsibilities of RSI include, but are not limited to, the following:

- Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.
- Firewall systems are in place to screen data flow between external parties and the RSI network. All inbound and outbound data packets on all interfaces are intercepted and inspected. Packets that are not explicitly permitted by the security policy definition are rejected.
- A secure VPN (Virtual Private Network) connection is used for remote external access to the internal network by authorized RSI employees. The use of VPN connection is restricted to authorized employees with two-factor authentication utilizing usernames and passwords, controlled by Active Directory, and one-time push notifications sent to the user's smart phone.
- VPN tunnels utilize encryption to protect customer and RSI data in transit, utilizing IPsec network layer encryption for site-to-site VPN connections.
- Policies and procedures are in place to guide personnel regarding sharing information with third parties.
- Communication sessions between RSI's servers/applications and external parties are secured using various encryption methods when applicable.
- Transaction processing that utilizes production server applications is secured through the use of TLS encryption over HTTPS connections.
- Transaction processing performed on web-based applications is secured through the use of the Transport Layer Security (TLS) encryption protocol over HTTPS connections.
 - This includes the use of the website file upload page.
 - Traffic directed to HTTP connections for this are redirected to HTTPS connections.

Disaster Recovery

RSI maintains a current Disaster Recovery Plan and Business Continuity plan. Disaster and business continuity emergency situations are ultimately managed through proper planning (crisis management, recovery and continuity) and response. Identified risks have been mitigated through prevention, minimization or rapid recovery resources and planning. RSI's disaster recovery and business continuity program helps to ensure that disruptive incidents are responded to quickly and effectively.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of RSI's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of RSI's ethical and behavioral standards, how they are communicated, and how they are reinforced in daily practice.

These standards include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, and by personal example.

Specific control activities that RSI has implemented in this area are described below.

- RSI maintains an employee handbook, which contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.
- Policies and procedures require that new employees sign an employee handbook acknowledgment form indicating that they have been given access to it and understand their responsibilities. The signed form is kept in the employee personnel file.
- Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.
- Comprehensive background checks are performed by an independent third party for certain positions as a component of the hiring process.
- Management personnel perform reference checks on all candidates being considered for certain positions within RSI.
- *Contract employees (1099)* must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.
- Comprehensive background checks are performed by an independent third party for *contract employees (1099)* as a component of the hiring process.
- Management maintains a commercial general liability insurance policy which includes employee dishonesty coverage.

Commitment to Competence

RSI's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. RSI's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

Specific control activities that RSI has implemented in this area are described below.

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written job descriptions.

- Roles and responsibilities for company personnel to interact with and monitor the activities of external third-party information technology vendors are defined in written job descriptions and communicated to personnel.
- Management has developed a training and development program for employees. This includes initial training/orientation with peers and supervisors in the period immediately after hire.
- Management encourages employees to complete and continue formal education and technical certification programs. (formally or informally)
- Certain approved professional development expenses incurred by the employees are paid by RSI. (training certs, classes, etc.)
- Each employee undergoes an annual performance review. A formal evaluation is prepared and maintained in the employee's HR file.
- Each new employee undergoes an initial 90 day probationary period and informal performance review to evaluate performance.
- RSI utilizes an independent CPA firm to prepare tax returns.

Board of Directors' Participation

RSI's control consciousness is influenced significantly by its Board of Directors participation. The Board of Directors oversees management activities and meets annually to discuss strategic, operational, and compliance issues.

Management's Philosophy and Operating Style

RSI's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward the comprehensive IT services, information processing, accounting functions and personnel. Management is periodically briefed on regulatory and industry changes affecting services provided. Management meetings are held on a periodic basis to discuss and monitor operational issues.

Specific control activities that RSI has implemented in this area are described below.

- Management communicates the importance of Information Security through ongoing Information Security related training for employees, documenting and implementing Information Security policies, and having frequent discussions with employees regarding the critical nature of Information Security including individual responsibilities for data and systems security.
- Management stays current on regulatory compliance or operational trends affecting the services provided by attending trade shows, utilizing trade and regulatory publications, journals, online news feeds or government sites, or belonging to industry associations.
- Operational meetings are held on a regular basis to discuss internal control responsibilities (*data and system security*) of individuals and performance measurement.
- RSI utilizes an independent CPA firm to prepare tax returns.

Organization Structure and Assignment of Authority and Responsibility

RSI's organization structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. RSI's management believes that establishing a relevant organization structure includes considering key areas of authority and responsibility and appropriate lines of reporting. RSI has developed an organization structure suited to its needs. This organization structure is based, in part, on its size and the nature of its activities.

RSI's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring that all personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that RSI has implemented in this area are described below.

- Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.
- RSI's organization structure is traditional, with clear lines of authority and responsibility. Autonomy within departments is allowed to a reasonable extent to provide for innovative approaches to managing the company, with close oversight maintained by senior management.

Human Resource Policies and Practices

RSI's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that RSI has implemented in this area are described below.

- Human Resources management utilizes a new hire checklist to ensure that specific elements of the hiring process are consistently executed. The checklist is stored electronically in the ConnectWise ticketing system.
- Comprehensive background checks are performed by an independent third party for certain positions as a component of the hiring process.
- Comprehensive background checks are performed by an independent third party for *contract employees (1099)* as a component of the hiring process.
- Management personnel perform reference checks on all candidates being considered for certain positions within RSI.
- RSI maintains an employee handbook, which contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.
- Management has developed a training and development program for employees. This includes initial training/orientation with peers and supervisors in the period immediately after hire.

- Each new employee undergoes an initial 90 day probationary period and informal performance review to evaluate performance.
- Each employee undergoes an annual performance review. A formal evaluation is prepared and maintained in the employee's HR file.
- Human Resources management utilizes a termination checklist to ensure that specific elements of the termination process are consistently executed. The checklist is stored electronically in the ConnectWise ticketing system.

END OF REPORT