EISNERAMPER

OutSolve, LLC's
Plan Management System

System and Organization Control Report
(SOC 2®)

SOC 2 Type 2
Security, Availability, Processing Integrity,
Confidentiality, and Privacy Categories

For the period April 1, 2024, to March 31, 2025

Table of Contents

Section Page

SECTION ONE

Assertion of the Management of OutSolve, LLC

SECTION ONE – ASSERTION OF THE MANAGEMENT OF OUTSOLVE, LLC

We have prepared the accompanying description in Section Three titled "OutSolve, LLC's Description of Its Plan Management System" throughout the period April 1, 2024, to March 31, 2025, (description), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, (AICPA Description Criteria) (description criteria). The description is intended to provide report users with information about the Plan Management System that may be useful when assessing the risks arising from interactions with OutSolve, LLC's (OutSolve or the service organization) system, particularly information about system controls that OutSolve has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (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).

OutSolve uses subservice organizations to provide data backup and backup monitoring, network management and security, intrusion monitoring, patching, anti-virus updates, and co-location facility services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at OutSolve, to achieve OutSolve's service commitments and system requirements based on the applicable trust services criteria. The description presents OutSolve's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of OutSolve's controls. The description does not disclose the actual controls at the subservice organizations.

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

a. the description presents OutSolve's Plan Management System that was designed and implemented throughout the period April 1, 2024, to March 31, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period April 1, 2024, to March 31, 2025, to provide reasonable assurance that OutSolve's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of OutSolve's controls throughout the period.
c. the controls stated in the description operated effectively throughout the period April 1, 2024, to March 31, 2025, to provide reasonable assurance that OutSolve's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of OutSolve's controls operated effectively throughout that period.

Signature: _____

Steve Claverie, Chief Technology Officer

Signature: _____

Baldwin Read, Chief Administrative Officer

SECTION TWO

Independent Service Auditor's Report
Report by EisnerAmper LLP

EisnerAmper LLP
One Galleria Blvd.
Suite 2100
Metairie, LA 70001
T 504.837.5990
F 504.834.3609
www.eisneramper.com

SECTION TWO – INDEPENDENT SERVICE AUDITOR'S REPORT

Report by EisnerAmper LLP

To Management of OutSolve, LLC

Scope

We have examined OutSolve, LLC's (OutSolve or the service organization) accompanying description of its Plan Management System titled "OutSolve, LLC's Description of Its Plan Management System" throughout the period April 1, 2024, to March 31, 2025 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2024, to March 31, 2025, to provide reasonable assurance that OutSolve's service commitments and system requirements were achieved based on trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

OutSolve uses subservice organizations to provide data backup and backup monitoring, network management and security, intrusion monitoring, patching, anti-virus updates, and co-location facility services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at OutSolve, to achieve OutSolve's service commitments and system requirements based on the applicable trust services criteria. The description presents OutSolve's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of OutSolve'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 information included in Section Five, "Other Information Provided by OutSolve, LLC That Is Not Covered by the Independent Service Auditor's Report" is presented by OutSolve's management to provide additional information and is not a part of OutSolve's description. Information about the development of a new cloud-based production system has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve OutSolve's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

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

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

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in Section Four of our report titled "Trust Services Security, Availability, Processing Integrity, Confidentiality, and Privacy Categories, Criteria, OutSolve, LLC's Related Controls, and Independent Service Auditor's Tests of Controls and Results."

Opinion

In our opinion, in all material respects,

a. The description presents OutSolve's Plan Management System that was designed and implemented throughout the period April 1, 2024, to March 31, 2025 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period April 1, 2024, to March 31, 2025, to provide reasonable assurance that OutSolve's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organizations applied the complementary controls assumed in the design of OutSolve's controls throughout the period.
c. The controls stated in the description operated effectively throughout the period April 1, 2024, to March 31, 2025, to provide reasonable assurance that OutSolve's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of OutSolve's controls operated effectively throughout the period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section Four, is intended solely for the information and use of OutSolve; user entities of OutSolve's Plan Management System during some or all of the period April 1, 2024, to March 31, 2025; business partners of OutSolve's subject to risks arising from interactions with OutSolve's Plan Management System; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties. If report recipients, other than these specified parties (herein referred to as a "non-specified user"), have obtained this report or have access to it, use of this report is the non-specified user's sole responsibility and is at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against EisnerAmper LLP as a result of such access. Further, EisnerAmper LLP does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

EisnerAmper LLP

EISNERAMPER LLP

Metairie, Louisiana

May 14, 2025

SECTION THREE

OutSolve, LLC's Description of Its Plan Management System

SECTION THREE – OUTSOLVE, LLC'S DESCRIPTION OF ITS PLAN MANAGEMENT SYSTEM

Overview of Operations and Services Provided

OutSolve, LLC (herein referred to as OutSolve, Organization, or Company) provides affirmative action planning and compliance services for federal contractors nationwide. OutSolve's corporate operations are located in Metairie, Louisiana with remote operations facilities located in Sacramento, California, Louisville, Kentucky, and Charleston, South Carolina. The Company is governed by a Board of Directors (Board), consisting of executive leadership and independent non-management individuals. OutSolve has a formally documented Board of Directors Charter that governs the make-up and authority of the Board.

Most employers contracted with the Federal Government are required to abide by the regulations set forth and enforced by the United States Office of Federal Contract Compliance Program (OFCCP). These regulations include specific annual reports that describe the makeup of the employer's workforce and provide statistics related to race, gender, protected veteran status, and individuals with disabilities counts, as well as indicate potential underutilization, hiring/promotion/termination disparities, or possible pay discrimination. As such, these reports can become a burden for the employer to produce on an annual basis as they usually require staff solely devoted to producing these reports. OutSolve provides a solution to this burden by allowing employers to outsource the production and support of the entire reporting process. While each employer is responsible for their compliance with nondiscrimination requirements, OutSolve's reporting process includes the review and compilation of provided workforce data to assemble Affirmative Action Plans. OutSolve is registered with the OFCCP to receive updates on regulatory requirement changes and updates.

OutSolve provides comprehensive services to its clients, including OFCCP audit support, HR compliance training, adverse impact analysis, compensation analysis, and regulatory reporting. OutSolve utilizes a custom, internally developed application, the OutSolve Plan Management system, to provide services tailored to the needs of its clients.

OutSolve uses the below service organizations (subservice organizations) to perform the noted services:

- ResTech Information Services, Inc. (ResTech) for data backup and backup monitoring, network management and security, intrusion monitoring, and patching and anti-virus updates.
- TierPoint, LLC (TierPoint) for co-location facility hosting services.

This description presents OutSolve's system; its controls relevant to the applicable trust services criteria; and the types of controls that OutSolve expects to be implemented, suitably designed, and operating effectively at the subservice organizations to meet certain applicable trust services criteria. The description does not include any of the controls expected to be implemented at the subservice organizations.

OutSolve completed a merger and acquisition of Federal Wage & Labor Law Institute on March 6, 2024, resulting in obtaining client opportunities and new product offerings. However, due to the timing of transitions and delayed onboarding of clients, this description is not applicable for prior Federal Wage & Labor Law Institute clients contracting with OutSolve for the related

services during the examination period. Additionally, OutSolve acquired a physical office location in Houston, Texas as part of the merger and acquisition that was subsequently closed on October 30, 2024. This physical office location and associated physical security controls were not included within the scope of the SOC 2 examination or this description.

OutSolve also completed a merger and acquisition of Labor Law Center (LLC) on September 3, 2024, resulting in obtaining client opportunities and product offerings. As part of the merger and acquisition, OutSolve acquired a physical office location in Santa Ana, California. This physical office location and associated physical security controls were not included within the scope of the SOC 2 examination or this description.

Principal Service Commitments and System Requirements

The relationship between OutSolve and its customers is contractual in nature. Customer contracts include relevant information regarding the design and operation of the system, including system boundaries, confidentiality requirements, and standard service commitments. Service commitments include:

- Maintaining a secure computing environment with access restricted to authorized individuals.
- Maintaining the confidentiality of client provided data in accordance with contractual commitments.
- Processing client provided data completely and accurately.
- Maintaining the availability of OutSolve systems to enable the delivery of the contracted services.
- Collecting, using, and disclosing client\employee Personal Information in accordance with our internal and external privacy policies.

OutSolve establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in policies and procedures and contracts 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 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 the system.

Components of the System Used to Provide the Services

OutSolve's Plan Management System is comprised of the following components:

- Infrastructure including the physical structures, IT, and other hardware,
- Software including application programs and IT system software that supports application programs,
- People including Executive Leadership, Finance & Administration, Sales, Marketing, and Technology

- Data including files, databases, and output used or processed by the system, and
- Procedures (automated and manual).

The boundaries of OutSolve's System include the services provided to a wide range of customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to OutSolve's customers are not included within the boundaries of its system.

Infrastructure and Software

OutSolve relies upon a custom, internally developed system, OutSolve Plan Management system, for processing client data and developing client deliverables. The OutSolve Plan Management system is managed internally by OutSolve's Chief Technology Officer (CTO), including custom development, change management, and user access provisioning. In addition, OutSolve utilizes an FTPS server and client web portal to manage the transfer of data from client organizations.

Management of OutSolve's IT environment, including local area network management and security, intrusion monitoring, patching and anti-virus updates, and back-up and recovery of significant files and programs, is outsourced to ResTech. As part of their managed services, ResTech logs, monitors, and reports system functionalities, including system performance, resource utilization, and unusual system activity. In addition, they ensure current anti-virus software is maintained on OutSolve owned equipment. The IT environment is designed to support the OutSolve Plan Management system and all other organizational systems and functions, including the operations at the remote facilities in Sacramento, California, Louisville, Kentucky, and Charleston, South Carolina. To document tasks assigned to address any needs, issues, and/or risks communicated during the quarterly meetings with the third-party IT support subservice organization, the IT support subservice organization creates a work ticket. OutSolve has the ability to monitor work ticket completion and will receive an update on any tickets and tasks during the subsequent quarterly meeting with the IT support vendor.

People

OutSolve has a staff of 100+ employees organized in the following functional areas:

- Executive Leadership – oversees organizational and functional operations and implements the strategic vision of the Board of Directors.
- Finance & Administration – responsible for personnel and financial management functions, including accounting, human resources, and other back-office areas.
- Sales – responsible for managing client relationships and identifying new client prospects.
- Operations – responsible for obtaining plan data from clients and preparing deliverable reports, in accordance with contracted services. The Operations area includes multiple oversight roles to manage the quality of client reports.
- Marketing – supports OutSolve's efforts to acquire clients through a variety of efforts including trainings and marketing campaigns.

- Technology – responsible for maintenance of the applications and infrastructure required to deliver the services to OutSolve customers in addition to the confidentiality, integrity, and availability of the applications.

Data

OutSolve customers expect controls to be applied over the sensitive data stored in OutSolve's systems, which includes the personal information of data subjects provided by customers or user entities to enable the delivery of the contracted services.

OutSolve provides a client web portal and FTPS server for clients to provide requested data. A unique username and password is required for end users to access the OutSolve client web portal. Requests for access to the OutSolve client web portal must come from an approved customer contact. Approved contacts for each client are maintained in the OutSolve Plan Management system. Requests from an unapproved source will be denied. To manage access to the secure FTP server, OutSolve sets up a unique user account for each user and requires users accessing the FTP server to authenticate using a username and password. In addition, each user must access the FTP server from a pre-approved IP address. OutSolve will only accept requests for new FTP server user accounts or IP addresses from an approved client contact, as documented in the OutSolve Plan Management system.

OutSolve has implemented network and system management and security configurations that are managed, monitored, and updated as necessary. Employee access for the network is managed by the IT environment management subservice provider through use of Active Directory and group policies. All access requests are reviewed and approved internally prior to submission by the CTO or the CAO. Employee user access rights are role based and are assigned based on job responsibilities. Each user is provided a unique username and must establish a complex password to access the network. On a quarterly basis, the IT environment management subservice organization provides OutSolve a listing of active network accounts. On an at least quarterly basis, OutSolve reviews the listing of network users to ensure only active employees have access to system resources and the access is reasonable based on the user's current job responsibilities. Any necessary network access adjustments are communicated to the IT environment management subservice organization.

Employee access requests for email and the OutSolve Plan Management System must be submitted by an authorized employee. Upon setup of employee access, Active Directory and group policy objects are used to manage user access.

Employee access to the network, email, and company systems is disabled at the time of termination. In the instance of an employee termination, OutSolve notifies key management personnel of the termination via email. In addition, OutSolve collects building access keys and any company equipment issued to the employee.

In an effort to protect sensitive client data from download, USB port access and use is restricted on OutSolve owned equipment. All employees can read from devices inserted into USB ports, but only the CAO and authorized members of the Information Technology Department have the ability to write to USB drives.

Remote users connect to OutSolve's network through a secure remote desktop connection which requires the use of a virtual private network (VPN) and two factor authentication. While connected,

employees operate from a terminal server desktop and are not able to copy data to network drives or their local machines. The Information Security Policy instructs employees to connect to a secure network, when working remotely, and provides direction on the requirement to maintain the security and confidentiality of sensitive information through encryption protocols. Company e-mail provides the option to encrypt any outgoing e-mail, as needed, to comply with company policy. In addition, workstation and laptop hard drives are encrypted.

Mobile Device Management software is in place to control the use of mobile devices that have access to company resources. OutSolve has the ability to remotely wipe devices in the event a device is lost or stolen.

Processes and Procedures

Expectations regarding organizational operations, integrity, and ethics have been established and are communicated to employees through various policies and procedures. Company policies and procedures are reviewed at least annually and revised, as necessary, by key management personnel for consistency with organizational processes and procedures, as well as alignment with integrity and ethics expectations and risk mitigation strategies. The following policies are made available to all employees on OutSolve's internal network:

- Business Continuity and Disaster Recovery Plan
- Change Management and Control Policy
- Information Security Policies and Procedures
- Network and Patch Management Policy
- OutSolve Code of Ethics

Internal Control Framework

Control Environment

Management Oversight

A company's internal control environment reflects the overall attitude, awareness, and actions of management and others concerning the importance of controls and the emphasis given to controls in a company's policies, procedures, methods, and organizational structure.

The control environment sets the tone of an organization, influencing the control consciousness of its employees. It is the foundation for all other components of internal control, providing discipline and structure. The control environment of OutSolve originates with and is the responsibility of the Board and key operational management personnel. OutSolve's Board and key operational management personnel provide strategic vision and company oversight. OutSolve's Board meets at least twice a year to discuss company risks, strategy, and various other organizational issues, to direct the development and performance of internal control.

Additionally, the Chief Operations Officer (COO) and the President meet on a monthly basis to evaluate production status updates and related resource and operational concerns. In addition, key management personnel meet on a periodic basis to evaluate information technology (IT) operations, strategy, risks, and other relevant topics. On a quarterly basis, the CTO, Chief Administrative Officer (CAO), and a representative from the IT support subservice organization, ResTech, meet to discuss IT

needs, opportunities, risks, and vulnerabilities. In addition to quarterly meetings, OutSolve may meet with key IT support providers as needed to address technology related risks or vulnerabilities. Key strategic initiatives and goals, as well as changes to company policies, procedures, commitments, and responsibilities, are communicated to all employees through company-wide emails, team meetings, and other communications.

Organization and Administration

Employees are required to complete and acknowledge annual training on information security. The annual security training is conducted in-house by the CTO. Data security topics covered during the security training include e-mail, passwords, internet security, personal device management, client data management, and confidentiality requirements. Internal policies such as the Code of Ethics, Confidentiality, Fraud and Identity Theft Prevention are discussed, in addition to procedures for properly requesting, receiving, and storing client data. In addition to security elements addressed during the annual training, employees are advised of policy and procedure revisions, including any specific commitment and responsibility changes.

Employment candidates undergo a screening process, which includes completing identity verification, reference checks, and criminal background checks. OutSolve contracts with a third-party organization to perform the criminal background checks. Employment with OutSolve is contingent upon the results of the screening process.

OutSolve has a formal employee performance management program that is documented within the Employee Handbook. Annual performance evaluations are based on Company objectives and job responsibilities communicated to employees through job related training, written policies, and documented standard operating procedures. Deviations from established performance and behavior expectations are documented and communicated to employees, and subject to disciplinary action.

OutSolve has implemented an online portal where employees can anonymously report issues, concerns, and/or suggestions. The portal is monitored by the Chief Administrative Officer and Chief Technology Officer. OutSolve documents any reported issues or concerns on an internal log that will be communicated to appropriate levels of management and/or the Board of Directors.

Processing Integrity

OutSolve requests that clients submit data in a standardized format utilizing the Requested Data Elements form. OutSolve requires clients to submit requested data in the appropriate electronic format (Microsoft Excel spreadsheet or CSV) to meet data processing timeliness objectives and increase the likelihood of data accuracy and completeness. OutSolve provides two secure options for clients to upload requested data, including the OutSolve client web portal and an FTPS server. While customers are able to provide data through other means, such as email, OutSolve encourages customers to utilize the available secure data transfer methods to better control the security of client data.

The OutSolve Plan Management system data import process includes an import error check, in which data values associated with preset fields are evaluated to determine if the type and format of imported data is acceptable. For any identified errors, OutSolve Consultants will adjust received data sets for basic formatting changes, as needed, but will obtain client approval prior to making any significant formatting or non-formatting changes. However, OutSolve Consultants can continue with the import

process if they determine the identified errors will not be detrimental to the processing of the data. If errors were identified and corrected during the initial import and error check process, the OutSolve Plan Management system performs another import error check prior to processing the updated imported data.

Once client data is fully imported into the OutSolve Plan Management system, compilation processes are initiated by OutSolve Consultants selecting report fields and parameters based on each client's plan reporting needs. Client reports are then generated based on client data compiled into the appropriate reporting fields. During the compilation process, the OutSolve Plan Management system records any potential data errors or warnings (e.g., duplicate employee identification numbers). After client data has been compiled in the report fields, the OutSolve Plan Management system provides configuration options to customize report formatting to meet the reporting expectations set forth by clients.

The client data uploaded into the OutSolve Plan Management system is used to generate reports, affirmative action plans, and other client deliverables. All client reports, including any reports customized to meet client needs and requests, are required to undergo an internal quality control review process before they can be released from the system and provided to a client. The OutSolve Plan Management system requires the quality control review to be performed by an employee other than the employee who completed the report within the system. A log of available quality control reviews and completed quality control reviews is tracked in the system. After a quality control review of a client report is performed, the original preparer is notified of any errors identified during the review. The preparer is responsible for correcting all identified errors before re-submitting the report for review and approval. In addition to the internal quality control review process for reports, OutSolve's client reporting process includes a billing oversight function to ensure client bills only include agreed upon and completed services. Any identified discrepancies are communicated to appropriate personnel.

OutSolve has developed various tools to assist employees in performing their job duties, including a user guide for the OutSolve Plan Management system to provide instructions for employees to process client data in accordance with commitments and company objectives. OutSolve has also developed various documented checklists and procedures to ensure that daily operations are performed accurately and completely. In addition, the OutSolve Plan Management system includes various error checks and required processing steps to ensure data is imported, compiled, and reported appropriately.

Logical Security

OutSolve has contracted with various third-party organizations to provide IT related services, including IT environment management and periodic internal and external network vulnerability and penetration assessments. Monthly vulnerability scans and penetration tests are performed by a third-party IT vendor. As part of their contracted network management services provided to OutSolve, the third-party IT vendor takes action based on the results of the scans. OutSolve monitors the status of the remediation items resulting from the vulnerability scans and penetration tests during quarterly meetings with the third-party IT vendor. In addition, the contracts or other provisions in place with the third-party IT related organizations includes formal documentation of any commitments and responsibilities, including confidentiality considerations.

Confidentiality

To support completed client reports and to meet industry and client data retention expectations, OutSolve has developed and implemented a Document and Data Retention policy which establishes documentation and disposal requirements. Additionally, the OutSolve Information Security Policies and Procedures address the disposal of decommissioned IT hardware. A third party vendor is used to dispose of decommissioned IT hardware.

Availability

OutSolve's contractual relationship with the IT environment management subservice provider includes management of backups of significant network files and programs, the client portal, and web servers on a daily basis. Backups are encrypted during the backup process. On a quarterly basis, a test restoration of a sample data set is performed by the IT environment management subservice provider to determine that backup data is recoverable. The co-location facility is owned and managed by a third-party subservice provider, TierPoint, LLC (TierPoint). OutSolve contracts with TierPoint to provide space for necessary IT hardware, continuous power and internet availability, environmental controls to protect the facility and OutSolve's equipment, year-round access to the facility, and assistance from onsite technical staff to perform tasks at the direction of OutSolve or OutSolve's IT environment management subservice provider. In addition, the contract with TierPoint includes physical security considerations, including limiting access to OutSolve equipment to only pre-approved individuals identified by OutSolve management personnel.

OutSolve has developed formal disaster recovery and incident response plans. These plans are reviewed by management annually and updated as necessary.

Change Management

OutSolve has developed a formal Change Management and Control Policy. The policy includes OutSolve's methodology regarding changes, including change requests, evaluation and approval of requested changes, and development, testing, approval, and implementation of changes.

OutSolve's IT environment management subservice provider notifies OutSolve of any necessary changes for the network. Non-critical changes to the network are reviewed and approved by OutSolve management prior to implementation. If critical or emergency network changes are necessary, the IT environment management subservice provider will implement the changes and retroactively notify OutSolve for review and approval. During the quarterly meetings with the IT environment management subservice provider, known or expected network updates or critical changes that have not been retroactively approved are discussed and approved, as appropriate.

For the OutSolve Plan Management system, the development and testing environments are isolated from the production environment. All development activities are logged and must be performed in the designated environment. Testing is performed prior to deploying the change to the production environment. The user requesting a change to the Plan Management system is responsible for performing user acceptance testing and notifies the CTO of any issues with the change. Access to the testing environment of the OutSolve Plan Management system and the ability to deploy changes into the production environment is restricted to appropriate personnel.

Upon removal of any IT hardware from production, it is securely stored by OutSolve until it is no longer needed and available for destruction and disposal. The OutSolve Information Security Policies and Procedures address the disposal of decommissioned IT hardware. A third-party vendor is used to dispose of decommissioned IT hardware.

Physical Security

OutSolve's corporate operations are located within a third party managed, multi-tenant office building in Metairie, Louisiana. OutSolve office doors at the Metairie, LA office location remain locked outside of normal business hours (Monday – Thursday: 8:30am – 4:30pm; Friday: 8:30am – 4:00pm). During business hours, OutSolve administration personnel monitor the front door of the Metairie office location. Visitors are required to enter through the front door and must be escorted by an OutSolve employee. Additional entry doors into the Metairie office location remain locked, and access is limited to authorized individuals based on unique access codes.

Within OutSolve's Metairie office location, access to secure areas, including the server room, is limited to authorized personnel. In addition, OutSolve has a security camera installed monitoring the server room. Any visitors to the secured areas within the office must be escorted by an authorized OutSolve employee.

OutSolve uses an independent air conditioning unit within the server room to regulate the room's temperature. OutSolve contracts with third party subservice providers to continuously monitor temperature levels within the server room and provide periodic air conditioner maintenance services. OutSolve utilizes an uninterruptible power supply (UPS) battery backup to protect equipment in the server room from short term power failures. Throughout the Metairie office location, hand-held fire extinguishers are available and smoke detectors have been strategically installed.

All OutSolve managed workstations are configured to lock after 15 minutes of inactivity.

OutSolve also has office locations in Sacramento, California, Louisville, Kentucky, and Mt. Pleasant, South Carolina. Access to OutSolve's Sacramento, CA, Louisville, KY, and Mt. Pleasant, SC, office locations is restricted to authorized personnel and points of entry are secured at all times.

Privacy

OutSolve is considered a data processor. Personal information of data subjects is provided by customers or user entities to support the operation of the System. Personal information that is collected by OutSolve includes, but is not limited to:

- Employee identifiers (name and contact information)
- Salary
- Hire Date
- Assigned Worksite
- Demographic information

Personal information is collected through various means, including via the OutSolve client portal and email communications. Data subjects' personal information is stored on OutSolve's network and servers during processing. OutSolve manages databases within the production environment to capture customer-entered data and process data output. Access to the data is limited to authorized

personnel in accordance with OutSolve policies. OutSolve is responsible for monitoring data processing and file transmission as well as identifying and resolving problems.

The responsibilities for and development of OutSolve's privacy practices are overseen by the CTO. OutSolve maintains an external privacy policy that is posted publicly so it is visible to data subjects. The external privacy policy informs data subjects of OutSolve's basis for consent, data subjects' choices regarding data collection, and how to submit data review, inventory, and/or deletion requests. Data requests from subjects are logged and tracked to resolution within OutSolve by the IT department The IT department also maintains an internal privacy policy that defines the procedures for data requests. Employees are required to read and acknowledge the internal privacy policy upon hire and annually thereafter.

Risk Assessment Process

OutSolve evaluates the risks that threaten its commitments and requirements through an annual risk assessment process. Recommendations resulting from the risk assessment are tracked and monitored.

In addition to the annual risk assessment process, OutSolve addresses key risks during various meetings of ownership and management, including:

- Board meetings at least twice a year consisting of OutSolve's President and other non-management owners. As a non-voting member, the CAO participates to provide key organizational updates.
- Monthly meetings between OutSolve's President and COO.
- Monthly meetings between OutSolve's department heads, including the CAO and the CTO.
- Quarterly meetings between OutSolve's CAO and CTO and OutSolve's third party IT support vendor, Restech.

During OutSolve's Board meetings, overall organizational risks, strategies, and operational processes are discussed. Based on his role with the organization, the CAO is able to provide updates on a variety of topics, including relevant risks, controls, etc. In addition, the President is involved in ongoing, monthly assessments of production data and updates which allows for him to provide updates to the Board. The operational insights of the CAO and President allow for the Board to make informed decisions.

The monthly meetings between the President and COO include an evaluation of production reporting, as well as discussions on action items to meet organizational commitments and requirements.

OutSolve's department heads meet on a monthly basis to give department updates and discuss any other relevant topics, as necessary. During this meeting, the CTO addresses ongoing IT needs, any issues management and/or the Board should be aware of, application of IT budget and any ongoing or emergency risks and how to address them.

OutSolve's CAO and CTO meet with Restech personnel to discuss IT needs, issues, and risks managed by Restech. During each quarterly meeting, reports over quarterly security and incident activities are discussed. The reports include updates on risks and issues identified, as well as opportunities for control and environment enhancement. In addition to the regular meetings, ad hoc meetings may occur based on risks and/or IT enhancements identified.

The various ownership and management meetings allow for OutSolve to evaluate their various organizational risks and develop and implement appropriate mitigation efforts. As part of this process, OutSolve has assessed the risks that could prevent their ability to achieve the in-scope Trust Services Criteria. As part of the assessment, OutSolve has identified current control activities in place to mitigate noted risks.

Based on the results of key OutSolve personnel meetings to discuss risks, OutSolve updates internal controls, processes, and related policies and procedures. Upon updating policies and procedures, they are made available to OutSolve employees for review.

OutSolve maintains liability insurance, including coverage for commercial general liability, as well as professional, privacy, and network security claims and events. The privacy liability coverage includes notification costs and regulatory defense coverage.

Information and Communication

Company values and behavioral standards have been established and are communicated to employees through required in person training sessions and documented policies and procedures. Employees are required to acknowledge that they have received and reviewed a confidentiality agreement regarding any client and OutSolve information and information security training, at hire and annually thereafter.

Monitoring

Management has implemented operational and security oversight, as well as employee on the job training over information security, confidentiality requirements, and organizational and security policies and procedures, at hire and annually thereafter, to set forth employment standards and establish integrity and ethics expectations.

OutSolve management personnel monitor internal control performance as part of their daily activities. In addition, OutSolve has developed organizational lines of reporting and responsibilities to provide for oversight and an internal separation of duties. Key operational areas, including operations in Sacramento, California, Louisville, Kentucky, and Mt. Pleasant, South Carolina, Technology, Sales, and Operations are overseen by Senior Vice Presidents who report directly to OutSolve's President. OutSolve's affirmative action planning workflow includes various segregation of duties, as well as multi-level quality review systems. OutSolve also facilitates client monitoring and satisfaction systems by generating and reviewing regular internal production reports and completing new client surveys to verify completion of contracted services.

Monitoring of production and internal performance is incorporated into the daily activities of OutSolve employees. A Team Lead is assigned to each client and is responsible for monitoring production and ensuring client commitments are fulfilled. Additionally, the COO generates reports

monthly to collect information necessary to monitor production and identify necessary employee feedback and actions to meet company objectives. After the reports are generated, the COO meets with the President to discuss the status of all outstanding projects and action items to meet commitments and requirements.

In addition to monitoring production and internal performance, OutSolve communicates with its clients on a regular basis to understand project requirements and track performance of the project team. OutSolve maintains a listing of approved contacts for each client. OutSolve will only contact approved client contacts to discuss client data. Client draft and final reports are only provided to approved client contacts. In addition to project requirements, data request, and project team performance communications, OutSolve notifies clients of any office closures and extended system downtime through a newsletter or other communication, as appropriate.

In addition to monitoring of internal operations and client communication, OutSolve has processes in place to evaluate and monitor potential and ongoing vendor relationships. OutSolve has a documented Third-Party Management policy and process to evaluate third party organizations prior to contracting with them for services and periodically thereafter to determine their achievement of contracted responsibilities, including standards of conduct that align with OutSolve's organizational expectations. OutSolve has contracts or other provisions in place with key third party organizations to document their responsibilities and requirements, including standards of conduct that align with OutSolve's organizational expectations. As part of ongoing monitoring and communications, OutSolve will provide necessary feedback to third party organizations if their personnel and/or service offerings are not meeting contractual requirements and expectations. Changes in services, commitments, or requirements require an appropriate addendum to the existing contract or a new contract to be executed.

Subservice Organizations

OutSolve uses certain subservice organizations to perform the services specified below and previously reported. As part of the annual due diligence reviews performed for ResTech and TierPoint and through daily operational activities, OutSolve monitors the services performed by the subservice organizations to ensure that operations and controls expected to be implemented at the subservice organizations are functioning effectively. In addition, OutSolve meets with the subservice organizations periodically to discuss services provided and to communicate any issues or concerns.

OutSolve uses the below service organizations (subservice organizations) to perform the noted services:

- ResTech Information Services, Inc. (ResTech) for data backup and backup monitoring, network management and security, intrusion monitoring, and patching and anti-virus updates.
- TierPoint, LLC (TierPoint) for co-location facility hosting services.

Incidents

There were no security incidents that met the reporting requirements under the 2018 description criteria for a description of a service organization's system in a SOC 2® report during the period of April 1, 2024, to March 31, 2025. These include incidents that a) were the result of controls that were

not suitably designed or operating effectively to provide reasonable assurance that one or more of the service organization's service commitments and system requirements were achieved or b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements.

Changes to the System During the Period

Other than those that were disclosed within this description, there were no changes that are likely to affect report users' understanding of the plan management system provided during the period April 1, 2024, through March 31, 2025.

Trust Services Security, Availability, Processing Integrity, Confidentiality, and Privacy Categories, Criteria, and Related Controls

OutSolve has specified the controls that are designed to achieve the applicable trust services criteria. The specified controls are presented in Section Four, "Trust Services Security, Availability, Processing Integrity, Confidentiality, and Privacy Categories, Criteria, OutSolve, LLC's Related Controls, and Independent Service Auditor's Tests of Controls and Results" and are an integral component of OutSolve's plan management system.

Complementary Subservice Organization Controls

OutSolve relies on services provided by the above subservice organizations. This description includes only the applicable Trust Services Criteria and related control activities pertaining to the System and excludes the applicable Trust Services Criteria and related control activities of the subservice organizations. Our examination herein did not extend to controls of these subservice organizations. The services provided by these subservice organizations and the related complementary subservice organizations controls expected to be implemented at the subservice organizations for the services reported are described below.

ResTech: Data backup and backup monitoring, network management, intrusion monitoring, and patching and anti-virus updates.

	Complementary Subservice Organization Controls	Related Trust Services Criteria
1	The subservice organization maintains an incident response policy.	CC 7.4
2	The subservice organization safeguards and restricts access to user credentials to the OutSolve network and systems.	CC 6.1
3	The subservice organization timely removes access rights to the OutSolve network and systems for any terminated subservice organization employee.	CC 6.1, CC 6.2
4	The subservice organization performs timely and complete security updates for the OutSolve network and managed connectivity tools (e.g., VPN).	CC 6.1, CC 6.6
5	The subservice organization restricts physical and logical access to backup media stored by the subservice organization.	CC 6.1, CC 6.4
6	The subservice organization notifies OutSolve of failed network backups that cannot be remediated in a timely manner.	A 1.2, A 1.3
7	The subservice organization implements recommendations identified during monthly penetration tests of network infrastructure and communicated by OutSolve.	CC 6.1, CC 6.6, CC 6.8, CC 7.1, CC 7.2
8	The subservice organization is provides network management and monitoring, including the following: -SIEM monitoring -patching -anti-virus updates -firewall management and monitoring -monitoring system performance, capacity, and resource utilization	CC 6.6, CC 7.1, CC 7.2, A 1.1

TierPoint: Co-location facility hosting services.

	Complementary Subservice Organization Controls	Related Trust Services Criteria
1	The subservice organization performs environmental systems maintenance, power plant maintenance, and other services that are reasonably required to maintain the co-location facility in good condition suitable for the placement of OutSolve equipment.	A 1.2, A 1.3, PI 1.5
2	The subservice organization maintains a co-location facility that is monitored 24 hours per day, 365 days per year by on-site staff, with card key and biometric reader access and closed-circuit TV monitoring or similar protocols.	CC 6.4, A 1.2, A 1.3, PI 1.5
3	The subservice organization provides a co-location facility that is maintained at ambient temperatures acceptable for the operation of OutSolve equipment.	A 1.2, A 1.3, PI 1.5
4	The subservice organization ensures the availability of internet access and power at the co-location facility.	A 1.2, A 1.3, PI 1.5
5	The subservice organization restricts access to OutSolve equipment to pre-approved individuals.	CC 6.4, A 1.2, A 1.3, PI 1.5

Complementary User Entity Controls

There are no controls at the user entity that are necessary, in combination with OutSolve's controls, to provide reasonable assurance that OutSolve's service commitments and system requirements were achieved based on the applicable trust services criteria (complementary user entity controls).

User Entity Responsibilities

There are, however, certain responsibilities that users of the system must fulfill for the user entity to derive the intended benefits of the services of OutSolve's Plan Management System. The user entity responsibilities presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities. User entities are responsible for their own control environments and their operational effectiveness.

USER ENTITY RESPONSIBILITIES

Control	Relevant Trust Services Criteria
User entities are responsible for using secure methods for data transmissions, including use of the methods provided by OutSolve, the client web portal and secure FTP server.	CC: 6.7 PI: 1.1 - 1.4
User entities are responsible for implementing and maintaining controls to ensure physical and logical security of systems that accumulate and transmit or receive data with OutSolve. This includes ensuring appropriate firewalls, anti-virus, and anti-spam software are implemented, properly configured, and maintained with appropriate updates.	CC: 6.6 and 6.7 PI: 1.1 - 1.3
Users are responsible for notifying OutSolve of any security breaches that may compromise confidential data and associated systems or adversely impact data flow.	CC: 6.1 - 6.3 and 6.6 – 6.7 PI: 1.1 - 1.3
User entities are responsible for providing accurate and complete plan related data in a usable format. User entities should consider providing data in the preferred methods as listed on the Requested Data Elements form.	PI: 1.1 - 1.5
Users are responsible for notifying OutSolve, in a timely manner, of any changes in communications or connectivity or related procedures that may affect the manner data is secured and transmitted.	CC: 6.1, 6.3, 6.6, and 6.7 PI: 1.1 and 1.2
User entities are responsible for maintaining and providing to OutSolve an up-to-date list of individuals who are authorized to make decisions on behalf of their organization. This includes notifying OutSolve when an authorized individual has terminated.	CC: 3.3, 6.2, 6.3, 6.6, 6.7 PI: 1.3

USER ENTITY RESPONSIBILITIES (continued)

Control	Relevant Trust Services Criteria
User entities are responsible for authorizing all non-format changes to the plan data provided.	CC: 3.3 PI: 1.3
User entities are responsible for performing periodic access reviews to determine whether access to OutSolve systems remains appropriate for each user's job functions.	CC: 6.1 - 6.3 and 6.6 - 6.8
User entities are responsible for limiting and controlling their personnel's access and use of assigned OutSolve system IDs and passwords.	CC: 6.1 - 6.3 and 6.6 - 6.8
User entities are responsible for notifying OutSolve of terminated users' access requirements.	CC: 6.1 - 6.3 and 6.6 - 6.8
User entities are responsible for providing complete and accurate feedback during new customer service follow up calls.	CC: 2.3 and 4.1 PI: 1.3 and 1.4
User entities are responsible for reviewing the input and output of reports provided by OutSolve.	PI: 1.1 - 1.4
User entities are responsible for communicating any specific retention and/or storage requirements for data sets and/or information provided to OutSolve.	PI: 1.5 C: 1.2

SECTION FOUR

Trust Services Security, Availability, Processing Integrity, Confidentiality, and Privacy Categories, Criteria, OutSolve, LLC's Related Controls, and Independent Service Auditor's Tests of Controls and Results

SECTION FOUR – TRUST SERVICES SECURITY, AVAILABILITY, PROCESSING INTEGRITY, CONFIDENTIALITY, AND PRIVACY CATEGORIES, CRITERIA, OUTSOLVE LLC'S RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S TESTS OF CONTROLS AND RESULTS

Information Provided by the Independent Service Auditor

The potential types of tests performed of the operational effectiveness of OutSolve, LLC's (OutSolve) Plan Management System controls detailed in Section Four are briefly described below:

Type of Test	General Description of Test
Inquiry	Inquiry of appropriate personnel and corroboration with management.
Observation	Observation of the application, performance, or existence of the control.
Inspection	Inspection of the documents and reports indicating performance of the control.
Reperformance	Reperformance of the control.

In addition, as required by paragraph .36 of AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*), when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes. The procedures performed included, but are not limited to, observation of the evidence being generated, inspection of queries used to generate the evidence, and inquiry with appropriate personnel.

Applicable Trust Services Categories, Criteria, OutSolve LLC's Controls, and Independent Service Auditor's Tests of Controls and Results

The following table describes the tests of operating effectiveness that were performed. The criteria, along with the controls, were specified by the management of OutSolve, LLC

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC1.0: Common Criteria Related to Control Environments			
CC1.1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Management has implemented operational and security oversight, as well as employee on the job training over information security, confidentiality requirements, and organizational and security policies and procedures, at hire and annually thereafter, to set forth employment standards and establish integrity and ethics expectations.	Inspected training material utilized for new hire and annual training to determine inclusion of information security, confidentiality requirements, and organizational and security policies and procedures.	No exceptions noted.
		For a selection of new hire employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that new hires completed training over information security, confidentiality requirements, and organizational and security policies and procedures.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		For a selection of current employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that employees completed training over information security, confidentiality requirements, and organizational and security policies and procedures, annually.	No exceptions noted.
CC1.1.2	OutSolve has a documented Third Party Management policy and process to evaluate third party organizations prior to contracting with them for services and periodically thereafter to determine their achievement of contracted responsibilities, including standards of conduct that align with OutSolve's organizational expectations.	Inspected the Third Party Management policy to determine that it addresses the third party organization evaluations performed prior to contracting for services and periodically thereafter.	No exceptions noted.
		There were no new vendors for the period. Therefore, the portion of the control related to the performance of a vendor review prior to contracting with new vendors did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no new vendors during the period, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC1.1.3	Employees are required to sign a confidentiality agreement regarding any client and OutSolve information at hire and sign an acknowledgement of the agreement annually.	For a selection of new hires, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine new hires acknowledged the Confidentiality Agreement during the onboarding process.	No exceptions noted.
		For a selection of current employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that employees acknowledged the Confidentiality Agreement on an annual basis.	No exceptions noted.
CC1.1.4	OutSolve has developed various policies and procedures (Including Code of Ethics, Information Security, Disaster Recovery, Patch Management, and Change Management Policies and Procedures), and made them available to all employees on a shared drive to establish organizational operations, integrity, and ethics expectations. At least annually, company policies are reviewed by management for consistency with organizational processes and procedures, as well as alignment with integrity and ethics expectations and risk mitigation strategies.	Inspected the OutSolve Code of Ethics, Information Security Policy, Business Continuity and Disaster Recovery Plan, Incident Response Plan, Network and Patch Management Policy, Change Management and Control Policy, Third Party Management Policy, and Human Resources Background Check and Exit Policy to determine that OutSolve policies and procedures were reviewed by management at least annually.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected the shared drive and its permissions to determine that OutSolve policies and procedures were made available to all employees on a shared drive.	No exceptions noted.
CC1.1.5	OutSolve has contracts or other provisions in place with key third party organizations to document their responsibilities and requirements, including standards of conduct that align with OutSolve's organizational expectations. As part of ongoing monitoring and communications, OutSolve will provide necessary feedback to third party organizations if their personnel and/or service offerings are not meeting contractual requirements and expectations. Changes in services, commitments, or requirements require an appropriate addendum to the existing contract or a new contract to be executed.	There were no new instances of new key third party organizations contracted during the examination period to determine existence and inclusion of documented responsibilities and requirements. Therefore, no substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period that a new third party organization was contracted to perform services, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no instances during the exam period in which a third party organization needed to be contacted regarding contractual requirements and expectations not being met. Therefore, no further substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which a third party organization needed to be contacted regarding contractual requirements and expectations not being met, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no instances during the exam period in which an existing third party organization's services, commitments, or requirements changed. Therefore, no further substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which a third party organization's services, commitments, or requirements changed, performed corroborative inquiry with multiple members of management. No instances were reported.
		Inspected the vendor contract for a selection of key third party organizations to determine that OutSolve has contracts or other provisions in place with key third party organizations to document their responsibilities and requirements.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC1.1.6	OutSolve has a formal employee performance management program that is documented within the Employee Handbook. Annual performance evaluations are based on Company objectives and job responsibilities communicated to employees through job related training, written policies, and documented standard operating procedures. Deviations from established performance and behavior expectations are documented and communicated to employees, and subject to disciplinary action.	Inspected OutSolve's Employee Handbook to determine that it formally documented an employee performance management program.	No exceptions noted.
		For a selection of active employees, inspected the completed 2024 Performance Evaluation template to determine that the annual performance evaluations were completed.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no instances where an employee's performance deviated from established performance and behavior expectations during the period. Therefore, the portion of the control related to deviations from established performance and behavior expectation did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which employee's performance deviated from established performance and behavior expectations during the period, performed corroborative inquiry with multiple members of management. No instances were reported.
CC1.1.7	At the time of hire, employees undergo a screening process, which includes completing identity verification and background checks. Employment is contingent upon the results of the screening process.	For a selection of new hires, inspected the identity verification and background check reports to determine that the new hire screening process, including identity verification and background checks, was completed for new hires.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC1.2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	OutSolve has a formally documented Board of Directors Charter that directs the make-up and authority of the Board. The Board is configured of non-management and ownership individuals, as designated in the Board of Directors Charter.	Inspected the Board of Directors Charter to determine that the charter directs the make-up and authority of the Board, including being configured of non-management and ownership individuals.	No exceptions noted.
CC1.2.2	OutSolve's Board meets at least twice a year to discuss company risks, strategy, and various other organizational issues, to direct the development and performance of internal control.	For a selection of board meetings, inspected calendar invitation details, meeting agenda, and board meeting minutes to determine that Board meetings were held at least twice a year to discuss company risks, strategy, and various other organizational issues.	No exceptions noted.
CC1.2.3	OutSolve has developed organizational lines of reporting and responsibility that provide for internal separation of duties and oversight. Within each functional area, organizational and reporting hierarchies have been defined, and responsibilities have been assigned.	Inspected OutSolve's organization chart to determine that designed organizational lines of reporting and responsibility provided for internal separation of duties and oversight. In addition, inspected the organization chart to determine that it included the key management level personnel responsible for overseeing the functional areas which address the various elements of OutSolve's organizational operations.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected written job descriptions for the Team Lead and Consultant roles to determine that job responsibilities were documented.	No exceptions noted.
CC1.3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	OutSolve has developed organizational lines of reporting and responsibility that provide for internal separation of duties and oversight. Within each functional area, organizational and reporting hierarchies have been defined, and responsibilities have been assigned.	Inspected OutSolve's organization chart to determine that designed organizational lines of reporting and responsibility provided for internal separation of duties and oversight. In addition, inspected the organization chart to determine that it included the key management level personnel responsible for overseeing the functional areas which address the various elements of OutSolve's organizational operations.	No exceptions noted.
		Inspected written job descriptions for the Team Lead and Consultant roles to determine that job responsibilities were documented.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC1.3.2	Management has implemented operational and security oversight, as well as employee on the job training over information security, confidentiality requirements, and organizational and security policies and procedures, at hire and annually thereafter, to set forth employment standards and establish integrity and ethics expectations.	Inspected training material utilized for new hire and annual training to determine inclusion of information security, confidentiality requirements, and organizational and security policies and procedures.	No exceptions noted.
		For a selection of new hire employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that new hires completed training over information security, confidentiality requirements, and organizational and security policies and procedures.	No exceptions noted.
		For a selection of current employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that employees completed training over information security, confidentiality requirements, and organizational and security policies and procedures, annually.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC1.3.3	OutSolve's Board meets at least twice a year to discuss company risks, strategy, and various other organizational issues, to direct the development and performance of internal control.	For a selection of board meetings, inspected calendar invitation details, meeting agenda, and board meeting minutes to determine that Board meetings were held at least twice a year to discuss company risks, strategy, and various other organizational issues.	No exceptions noted.
CC1.3.4	OutSolve has a documented Third Party Management policy and process to evaluate third party organizations prior to contracting with them for services and periodically thereafter to determine their achievement of contracted responsibilities, including standards of conduct that align with OutSolve's organizational expectations.	Inspected the Third Party Management policy to determine that it addresses the third party organization evaluations performed prior to contracting for services and periodically thereafter.	No exceptions noted.
		There were no new vendors for the period. Therefore, the portion of the control related to the performance of a vendor review prior to contracting with new vendors did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no new vendors during the period, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	At the time of hire, employees undergo a screening process, which includes completing identity verification and background checks. Employment is contingent upon the results of the screening process.	For a selection of new hires, inspected the identity verification and background check reports to determine that the new hire screening process, including identity verification and background checks, was completed for new hires.	No exceptions noted.
CC1.4.2	Management has implemented operational and security oversight, as well as employee on the job training over information security, confidentiality requirements, and organizational and security policies and procedures, at hire and annually thereafter, to set forth employment standards and establish integrity and ethics expectations.	Inspected training material utilized for new hire and annual training to determine inclusion of information security, confidentiality requirements, and organizational and security policies and procedures.	No exceptions noted.
		For a selection of new hire employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that new hires completed training over information security, confidentiality requirements, and organizational and security policies and procedures.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		For a selection of current employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that employees completed training over information security, confidentiality requirements, and organizational and security policies and procedures, annually.	No exceptions noted.
CC1.4.3	OutSolve has a formal employee performance management program that is documented within the Employee Handbook. Annual performance evaluations are based on Company objectives and job responsibilities communicated to employees through job related training, written policies, and documented standard operating procedures. Deviations from established performance and behavior expectations are documented and communicated to employees, and subject to disciplinary action.	Inspected OutSolve's Employee Handbook to determine that it formally documented an employee performance management program.	No exceptions noted.
		For a selection of active employees, inspected the completed 2024 Performance Evaluation template to determine that the annual performance evaluations were completed.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no instances where an employee's performance deviated from established performance and behavior expectations during the period. Therefore, the portion of the control related to deviations from established performance and behavior expectation did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which employee's performance deviated from established performance and behavior expectations during the period, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC1.5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	OutSolve has a formal employee performance management program that is documented within the Employee Handbook. Annual performance evaluations are based on Company objectives and job responsibilities communicated to employees through job related training, written policies, and documented standard operating procedures. Deviations from established performance and behavior expectations are documented and communicated to employees, and subject to disciplinary action.	Inspected OutSolve's Employee Handbook to determine that it formally documented an employee performance management program.	No exceptions noted.
		For a selection of active employees, inspected the completed 2024 Performance Evaluation template to determine that the annual performance evaluations were completed.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no instances where an employee's performance deviated from established performance and behavior expectations during the period. Therefore, the portion of the control related to deviations from established performance and behavior expectation did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which employee's performance deviated from established performance and behavior expectations during the period, performed corroborative inquiry with multiple members of management. No instances were reported.
CC1.5.2	The Chief Operations Officer generates reports monthly to collect information necessary to monitor production and identify necessary employee feedback and actions to meet company objectives. After the reports are generated, the Chief Operations Officer meets with the President to discuss the status of all outstanding projects and action items to meet commitments and requirements.	For a selection of months, inspected calendar details and the monthly production report to determine that the Chief Operations Officer and the President had a recurring monthly production review meeting scheduled and the Chief Operations Officer generated monthly reports to collect information necessary to monitor production and identify necessary employee feedback and actions to meet company objectives.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC2.0: Common Criteria Related to Communication and Information			
CC2.1: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	The Chief Operations Officer generates reports monthly to collect information necessary to monitor production and identify necessary employee feedback and actions to meet company objectives. After the reports are generated, the Chief Operations Officer meets with the President to discuss the status of all outstanding projects and action items to meet commitments and requirements.	For a selection of months, inspected calendar details and the monthly production report to determine that the Chief Operations Officer and the President had a recurring monthly production review meeting scheduled and the Chief Operations Officer generated monthly reports to collect information necessary to monitor production and identify necessary employee feedback and actions to meet company objectives.	No exceptions noted.
CC2.1.2	At the time client data is uploaded to the OutSolve Plan Management System and after data processing and report generation, data validation is performed by the system to reasonably ensure client provided data is complete and accurate. Upon completion of the data validation process, an error log is generated for review by an OutSolve employee. Identified errors are researched and corrected.	For a selection of completed client reports, inspected the error log generated after the completion of data validation to determine that data validation is performed by the system.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC2.1.3	All client reports undergo a quality control review. This quality control review must be performed by an employee other than the employee who completed the report. A log of available quality control reviews and completed quality control reviews is tracked in the OutSolve Plan Management System.	Inspected the Data Quality Control Queue to determine that the OutSolve Plan Management System tracked the quality control review process.	No exceptions noted.
		For a selection of completed client reports, inspected the quality control completion e-mail notification to determine that quality control reviews were completed by an employee that did not complete the report.	No exceptions noted.
CC2.1.4	OutSolve requests client data utilizing the Requested Data Elements form. OutSolve requires clients to submit requested data in the appropriate electronic format to meet data processing timeliness objectives and increase the likelihood of data accuracy and completeness.	Inspected the Requested Data Elements form to determine existence and to gain an understanding of the data submission specifications.	No exceptions noted.
		Inspected instructions provided to a customer to determine that a customer was requested to utilize the Requested Data Elements form to provide requested data in the appropriate electronic format.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC2.2: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Management has implemented operational and security oversight, as well as employee on the job training over information security, confidentiality requirements, and organizational and security policies and procedures, at hire and annually thereafter, to set forth employment standards and establish integrity and ethics expectations.	Inspected training material utilized for new hire and annual training to determine inclusion of information security, confidentiality requirements, and organizational and security policies and procedures.	No exceptions noted.
		For a selection of new hire employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that new hires completed training over information security, confidentiality requirements, and organizational and security policies and procedures.	No exceptions noted.
		For a selection of current employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that employees completed training over information security, confidentiality requirements, and organizational and security policies and procedures, annually.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC2.2.2	OutSolve has developed various policies and procedures (Including Code of Ethics, Information Security, Disaster Recovery, Patch Management, and Change Management Policies and Procedures), and made them available to all employees on a shared drive to establish organizational operations, integrity, and ethics expectations. At least annually, company policies are reviewed by management for consistency with organizational processes and procedures, as well as alignment with integrity and ethics expectations and risk mitigation strategies.	Inspected the OutSolve Code of Ethics, Information Security Policy, Business Continuity and Disaster Recovery Plan, Incident Response Plan, Network and Patch Management Policy, Change Management and Control Policy, Third Party Management Policy, and Human Resources Background Check and Exit Policy to determine that OutSolve policies and procedures were reviewed by management at least annually.	No exceptions noted.
		Inspected the shared drive and its permissions to determine that OutSolve policies and procedures were made available to all employees on a shared drive.	No exceptions noted.
CC2.2.3	OutSolve's Board meets at least twice a year to discuss company risks, strategy, and various other organizational issues, to direct the development and performance of internal control.	For a selection of board meetings, inspected calendar invitation details, meeting agenda, and board meeting minutes to determine that Board meetings were held at least twice a year to discuss company risks, strategy, and various other organizational issues.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC2.2.4	The Chief Operations Officer generates reports monthly to collect information necessary to monitor production and identify necessary employee feedback and actions to meet company objectives. After the reports are generated, the Chief Operations Officer meets with the President to discuss the status of all outstanding projects and action items to meet commitments and requirements.	For a selection of months, inspected calendar details and the monthly production report to determine that the Chief Operations Officer and the President had a recurring monthly production review meeting scheduled and the Chief Operations Officer generated monthly reports to collect information necessary to monitor production and identify necessary employee feedback and actions to meet company objectives.	No exceptions noted.
CC2.2.5	Employees are required to sign a confidentiality agreement regarding any client and OutSolve information at hire and sign an acknowledgement of the agreement annually.	For a selection of new hires, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine new hires acknowledged the Confidentiality Agreement during the onboarding process.	No exceptions noted.
		For a selection of current employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that employees acknowledged the Confidentiality Agreement on an annual basis.	No exceptions noted.
CC2.2.6	OutSolve has developed a Document and Data Retention policy to establish documentation retention and disposal requirements to meet confidentiality commitments and system requirements.	Inspected the Document and Data Retention policy to determine that the policy addressed documentation retention and disposal requirements.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC2.2.7	OutSolve holds periodic staff meetings, at least quarterly, to communicate key company initiatives, updates, and/or concerns or risks.	For a selection of quarters, inspected calendar invitation details and meeting agenda to determine that staff meetings were held at least quarterly.	No exceptions noted.
CC2.2.8	An OutSolve Plan Management System user guide is available to provide instructions for employees to process client data in accordance with commitments and company objectives.	Inspected the OutSolve Plan Management System user guide to determine the existence and inclusion of processing instructions.	No exceptions noted.
		Observed the shared network folder and its permissions to determine that the OutSolve Plan Management System instructional manual was made available to all employees.	No exceptions noted.
CC2.2.9	OutSolve has developed various documented procedures to ensure that daily operations are performed accurately and completely in accordance with company commitments and requirements.	Inspected the documented procedures to determine the existence and inclusion of information to assist OutSolve employees in performing daily operations accurately and completely.	No exceptions noted.
		Observed the shared network folder and its permissions to determine that the documented procedures were made available to all employees.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC2.3: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The Chief Technology Officer, the Chief Administrative Officer, and a representative from the third party IT support subservice organization meet on a quarterly basis to discuss information technology needs, issues, and risks managed by the third party service provider. In addition and as possible, identified system technology enhancement opportunities are discussed.	For a selection of quarters, inspected calendar invitation details and meeting materials to determine that OutSolve's Chief Technology Officer and Chief Administrative Officer met with a representative from the third party IT subservice organization to discuss information technology needs, issues, and risks.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC2.3.2	OutSolve has contracts or other provisions in place with key third party organizations to document their responsibilities and requirements, including standards of conduct that align with OutSolve's organizational expectations. As part of ongoing monitoring and communications, OutSolve will provide necessary feedback to third party organizations if their personnel and/or service offerings are not meeting contractual requirements and expectations. Changes in services, commitments, or requirements require an appropriate addendum to the existing contract or a new contract to be executed.	There were no new instances of new key third party organizations contracted during the examination period to determine existence and inclusion of documented responsibilities and requirements. Therefore, no substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period that a new third party organization was contracted to perform services, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no instances during the exam period in which a third party organization needed to be contacted regarding contractual requirements and expectations not being met. Therefore, no further substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which a third party organization needed to be contacted regarding contractual requirements and expectations not being met, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no instances during the exam period in which an existing third party organization's services, commitments, or requirements changed. Therefore, no further substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which a third party organization's services, commitments, or requirements changed, performed corroborative inquiry with multiple members of management. No instances were reported.
		Inspected the vendor contract for a selection of key third party organizations to determine that OutSolve has contracts or other provisions in place with key third party organizations to document their responsibilities and requirements.	No exceptions noted.
CC2.3.3	OutSolve follows up with all first year clients via email to verify completion of contracted services.	For a selection of first year clients, inspected e-mail communication to determine first year clients were contacted to verify completion of contracted services.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC2.3.4	Changes to the network made by the third party IT support vendor are reviewed and approved by OutSolve management.	For a selection of network changes made by the third party IT support, inspected support tickets to determine that network changes made by the third party IT support vendor were approved by OutSolve management prior to implementation.	No exceptions noted.
CC2.3.5	The relationship between OutSolve and its customers is contractual in nature. Customer contracts include relevant information regarding the design and operation of the system, including system boundaries, confidentiality requirements, and standard service commitments.	For a selection of new customers, inspected new customer contracts to determine that customer contracts included standard, as well as customer specific service commitments and customer responsibilities along with relevant information regarding design and operation of the system, including system boundaries, confidentiality requirements, and standard service commitments.	No exceptions noted.
CC2.3.6	OutSolve requests client data utilizing the Requested Data Elements form. OutSolve requires clients to submit requested data in the appropriate electronic format to meet data processing timeliness objectives and increase the likelihood of data accuracy and completeness.	Inspected the Requested Data Elements form to determine existence and to gain an understanding of the data submission specifications.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected instructions provided to a customer to determine that a customer was requested to utilize the Requested Data Elements form to provide requested data in the appropriate electronic format.	No exceptions noted.
CC2.3.7	OutSolve provides a secure client portal and a FTPS server for client data uploads.	Observed that a secure client portal and a FTPS server were provided for client data uploads.	No exceptions noted.
		Inspected instructions provided to a customer to determine that a customer was informed of the secure client portal.	No exceptions noted.
CC3.0: Common Criteria Related to Risk Assessment			
CC3.1: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	OutSolve's Board meets at least twice a year to discuss company risks, strategy, and various other organizational issues, to direct the development and performance of internal control.	For a selection of board meetings, inspected calendar invitation details, meeting agenda, and board meeting minutes to determine that Board meetings were held at least twice a year to discuss company risks, strategy, and various other organizational issues.	No exceptions noted.
CC3.1.2	Key management personnel meet on a periodic basis to discuss IT operations, strategy, risks, and other relevant topics.	For a selection of months, inspected calendar invitation details and the meeting agenda to determine that key management personnel met on a periodic basis to discuss IT operations, strategy, risks, and other relevant topics.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC3.1.3	OutSolve has a documented Third Party Management policy and process to evaluate third party organizations prior to contracting with them for services and periodically thereafter to determine their achievement of contracted responsibilities, including standards of conduct that align with OutSolve's organizational expectations.	Inspected the Third Party Management policy to determine that it addresses the third party organization evaluations performed prior to contracting for services and periodically thereafter.	No exceptions noted.
		There were no new vendors for the period. Therefore, the portion of the control related to the performance of a vendor review prior to contracting with new vendors did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no new vendors during the period, performed corroborative inquiry with multiple members of management. No instances were reported.
CC3.1.4	OutSolve evaluates the risks that threaten its commitments and requirements through an annual risk assessment process. Recommendations resulting from the risk assessment are tracked and monitored.	Inspected the completed annual risk assessment to determine that OutSolve evaluated the risks that threaten its commitments and requirements through an annual risk assessment process.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected the risk assessment recommendation update presentation to determine that recommendations resulting from the risk assessment were tracked and monitored.	No exceptions noted.
CC3.2: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	OutSolve evaluates the risks that threaten its commitments and requirements through an annual risk assessment process. Recommendations resulting from the risk assessment are tracked and monitored.	Inspected the completed annual risk assessment to determine that OutSolve evaluated the risks that threaten its commitments and requirements through an annual risk assessment process.	No exceptions noted.
		Inspected the risk assessment recommendation update presentation to determine that recommendations resulting from the risk assessment were tracked and monitored.	No exceptions noted.
CC3.2.2	OutSolve's Board meets at least twice a year to discuss company risks, strategy, and various other organizational issues, to direct the development and performance of internal control.	For a selection of board meetings, inspected calendar invitation details, meeting agenda, and board meeting minutes to determine that Board meetings were held at least twice a year to discuss company risks, strategy, and various other organizational issues.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC3.3: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	OutSolve evaluates the risks that threaten its commitments and requirements through an annual risk assessment process. Recommendations resulting from the risk assessment are tracked and monitored.	Inspected the completed annual risk assessment to determine that OutSolve evaluated the risks that threaten its commitments and requirements through an annual risk assessment process.	No exceptions noted.
		Inspected the risk assessment recommendation update presentation to determine that recommendations resulting from the risk assessment were tracked and monitored.	No exceptions noted.
CC3.3.2	OutSolve has implemented an online portal where employees can anonymously report issues, concerns, and/or suggestions. The portal is monitored by the Chief Administrative Officer and Chief Technology Officer. OutSolve documents any reported issues or concerns on an internal log that will be communicated to appropriate levels of management and/or the Board of Directors.	Observed the online portal where employees can anonymously report issues, concerns, and/or suggestions.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no issues, concerns, or suggestions reported via the online portal during the examination period. Therefore, the portion of the control related to communication of issues, concerns, or suggestions to appropriate levels of management and/or the Board of Directors did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which issues, concerns, or suggestions were reported via the online portal, performed inquiry with management and observed that no incidents were logged within the incident portal.
CC3.3.3	OutSolve has developed organizational lines of reporting and responsibility that provide for internal separation of duties and oversight. Within each functional area, organizational and reporting hierarchies have been defined, and responsibilities have been assigned.	Inspected OutSolve's organization chart to determine that designed organizational lines of reporting and responsibility provided for internal separation of duties and oversight. In addition, inspected the organization chart to determine that it included the key management level personnel responsible for overseeing the functional areas which address the various elements of OutSolve's organizational operations.	No exceptions noted.
		Inspected written job descriptions for the Team Lead and Consultant roles to determine that job responsibilities were documented.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC3.4: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	OutSolve evaluates the risks that threaten its commitments and requirements through an annual risk assessment process. Recommendations resulting from the risk assessment are tracked and monitored.	Inspected the completed annual risk assessment to determine that OutSolve evaluated the risks that threaten its commitments and requirements through an annual risk assessment process.	No exceptions noted.
		Inspected the risk assessment recommendation update presentation to determine that recommendations resulting from the risk assessment were tracked and monitored.	No exceptions noted.
CC3.4.2	OutSolve's Board meets at least twice a year to discuss company risks, strategy, and various other organizational issues, to direct the development and performance of internal control.	For a selection of board meetings, inspected calendar invitation details, meeting agenda, and board meeting minutes to determine that Board meetings were held at least twice a year to discuss company risks, strategy, and various other organizational issues.	No exceptions noted.
CC4.0: Common Criteria Related to Monitoring Activities			
CC4.1: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	OutSolve's Board meets at least twice a year to discuss company risks, strategy, and various other organizational issues, to direct the development and performance of internal control.	For a selection of board meetings, inspected calendar invitation details, meeting agenda, and board meeting minutes to determine that Board meetings were held at least twice a year to discuss company risks, strategy, and various other organizational issues.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC4.1.2	The Chief Technology Officer, the Chief Administrative Officer, and a representative from the third party IT support subservice organization meet on a quarterly basis to discuss information technology needs, issues, and risks managed by the third party service provider. In addition and as possible, identified system technology enhancement opportunities are discussed.	For a selection of quarters, inspected calendar invitation details and meeting materials to determine that OutSolve's Chief Technology Officer and Chief Administrative Officer met with a representative from the third party IT subservice organization to discuss information technology needs, issues, and risks.	No exceptions noted.
CC4.1.3	Quarterly reviews of network users for appropriateness are performed by the Chief Technology Officer and the Chief Administrative Officer to determine controls over user access are operating as expected.	For a selection of quarters, inspected the meeting invitation and network user listing to determine that the third party IT support vendor provided a network user listing for review on a quarterly basis to the Chief Technology Officer and the Chief Administrative Officer and the provided network user listing included identification of network user accounts for discussion during quarterly meetings attended by the Chief Technology Officer, the Chief Administrative Officer, and the third party IT support vendor.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC4.1.4	Monthly vulnerability scans and penetration tests are performed by a third-party IT vendor. As part of their contracted network management services provided to OutSolve, the third party IT vendor takes action based on the results of the scans. OutSolve monitors the status of the remediation items resulting from the vulnerability scans and penetration tests during quarterly meetings with the third party IT vendor.	For a selection of months, inspected vulnerability scans and penetration test reports to determine that vulnerability scans and penetration tests of OutSolve's network infrastructure were performed by a third party IT vendor on a monthly basis.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no critical or high risk vulnerabilities identified during scans and penetration tests that required remediation. As such, the portion of the control related to remediation did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no critical or high risk external or internal vulnerabilities noted during the period, corroborative inquiry with multiple members of management and inspection of 'External Pentest + Vuln Assessment Executive Summary' report and 'Internal Pentest + Vuln Assessment Executive Summary' report was performed. No indication of critical or high risk vulnerabilities during the period was noted.
CC4.1.5	A quarterly test restoration of a sample data set is performed to verify that backup data is recoverable.	On a sample basis, inspected quarterly email notifications from the IT support vendor to determine that test restorations of sampled backed up data sets were completed and communicated to OutSolve. In addition, inspected supporting documentation to determine that restorations of sampled backed up data sets were successful.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC4.1.6	OutSolve follows up with all first year clients via email to verify completion of contracted services.	For a selection of first year clients, inspected e-mail communication to determine first year clients were contacted to verify completion of contracted services.	No exceptions noted.
CC4.1.7	Changes to the network made by the third party IT support vendor are reviewed and approved by OutSolve management.	For a selection of network changes made by the third party IT support, inspected support tickets to determine that network changes made by the third party IT support vendor were approved by OutSolve management prior to implementation.	No exceptions noted.
CC4.1.8	The Chief Operations Officer generates reports monthly to collect information necessary to monitor production and identify necessary employee feedback and actions to meet company objectives. After the reports are generated, the Chief Operations Officer meets with the President to discuss the status of all outstanding projects and action items to meet commitments and requirements.	For a selection of months, inspected calendar details and the monthly production report to determine that the Chief Operations Officer and the President had a recurring monthly production review meeting scheduled and the Chief Operations Officer generated monthly reports to collect information necessary to monitor production and identify necessary employee feedback and actions to meet company objectives.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC4.2: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	The Chief Technology Officer, the Chief Administrative Officer, and a representative from the third party IT support subservice organization meet on a quarterly basis to discuss information technology needs, issues, and risks managed by the third party service provider. In addition and as possible, identified system technology enhancement opportunities are discussed.	For a selection of quarters, inspected calendar invitation details and meeting materials to determine that OutSolve's Chief Technology Officer and Chief Administrative Officer met with a representative from the third party IT subservice organization to discuss information technology needs, issues, and risks.	No exceptions noted.
CC4.2.2	Quarterly reviews of network users for appropriateness are performed by the Chief Technology Officer and the Chief Administrative Officer to determine controls over user access are operating as expected.	For a selection of quarters, inspected the meeting invitation and network user listing to determine that the third party IT support vendor provided a network user listing for review on a quarterly basis to the Chief Technology Officer and the Chief Administrative Officer and the provided network user listing included identification of network user accounts for discussion during quarterly meetings attended by the Chief Technology Officer, the Chief Administrative Officer, and the third party IT support vendor.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC4.2.3	Monthly vulnerability scans and penetration tests are performed by a third-party IT vendor. As part of their contracted network management services provided to OutSolve, the third party IT vendor takes action based on the results of the scans. OutSolve monitors the status of the remediation items resulting from the vulnerability scans and penetration tests during quarterly meetings with the third party IT vendor.	For a selection of months, inspected vulnerability scans and penetration test reports to determine that vulnerability scans and penetration tests of OutSolve's network infrastructure were performed by a third party IT vendor on a monthly basis.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no critical or high risk vulnerabilities identified during scans and penetration tests that required remediation. As such, the portion of the control related to remediation did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no critical or high risk external or internal vulnerabilities noted during the period, corroborative inquiry with multiple members of management and inspection of 'External Pentest + Vuln Assessment Executive Summary' report and 'Internal Pentest + Vuln Assessment Executive Summary' report was performed. No indication of critical or high risk vulnerabilities during the period was noted.
CC4.2.4	A quarterly test restoration of a sample data set is performed to verify that backup data is recoverable.	On a sample basis, inspected quarterly email notifications from the IT support vendor to determine that test restorations of sampled backed up data sets were completed and communicated to OutSolve. In addition, inspected supporting documentation to determine that restorations of sampled backed up data sets were successful.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC4.2.5	The Chief Operations Officer generates reports monthly to collect information necessary to monitor production and identify necessary employee feedback and actions to meet company objectives. After the reports are generated, the Chief Operations Officer meets with the President to discuss the status of all outstanding projects and action items to meet commitments and requirements.	For a selection of months, inspected calendar details and the monthly production report to determine that the Chief Operations Officer and the President had a recurring monthly production review meeting scheduled and the Chief Operations Officer generated monthly reports to collect information necessary to monitor production and identify necessary employee feedback and actions to meet company objectives.	No exceptions noted.
CC4.2.6	Changes to the network made by the third party IT support vendor are reviewed and approved by OutSolve management.	For a selection of network changes made by the third party IT support, inspected support tickets to determine that network changes made by the third party IT support vendor were approved by OutSolve management prior to implementation.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC4.2.7	To document tasks assigned to address any needs, issues, and/or risks communicated during the quarterly meetings with the third party IT support subservice organization, the IT support subservice organization creates a work ticket. OutSolve has the ability to monitor work ticket completion and will receive an update on any tickets and tasks during the subsequent quarterly meeting with the IT support subservice organization.	Observed OutSolve personnel login to the third party IT support subservice organization's ticketing system and review ticket details for an example ticket to determine that OutSolve has the ability to monitor work ticket completion.	No exceptions noted.
		For a selection of quarters, inspected the meeting agenda and material to determine that an update on any tickets and tasks was provided during the subsequent quarterly meeting with the IT support subservice organization.	No exceptions noted.
CC4.2.8	OutSolve's Board meets at least twice a year to discuss company risks, strategy, and various other organizational issues, to direct the development and performance of internal control.	For a selection of board meetings, inspected calendar invitation details, meeting agenda, and board meeting minutes to determine that Board meetings were held at least twice a year to discuss company risks, strategy, and various other organizational issues.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC5.0: Common Criteria Related to Control Activities			
CC5.1: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	OutSolve evaluates the risks that threaten its commitments and requirements through an annual risk assessment process. Recommendations resulting from the risk assessment are tracked and monitored.	Inspected the completed annual risk assessment to determine that OutSolve evaluated the risks that threaten its commitments and requirements through an annual risk assessment process.	No exceptions noted.
		Inspected the risk assessment recommendation update presentation to determine that recommendations resulting from the risk assessment were tracked and monitored.	No exceptions noted.
CC5.1.2	OutSolve's Board meets at least twice a year to discuss company risks, strategy, and various other organizational issues, to direct the development and performance of internal control.	For a selection of board meetings, inspected calendar invitation details, meeting agenda, and board meeting minutes to determine that Board meetings were held at least twice a year to discuss company risks, strategy, and various other organizational issues.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC5.1.3	The Chief Technology Officer, the Chief Administrative Officer, and a representative from the third party IT support subservice organization meet on a quarterly basis to discuss information technology needs, issues, and risks managed by the third party service provider. In addition and as possible, identified system technology enhancement opportunities are discussed.	For a selection of quarters, inspected calendar invitation details and meeting materials to determine that OutSolve's Chief Technology Officer and Chief Administrative Officer met with a representative from the third party IT subservice organization to discuss information technology needs, issues, and risks.	No exceptions noted.
CC5.1.4	Key management personnel meet on a periodic basis to discuss IT operations, strategy, risks, and other relevant topics.	For a selection of months, inspected calendar invitation details and the meeting agenda to determine that key management personnel met on a periodic basis to discuss IT operations, strategy, risks, and other relevant topics.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC5.2: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	OutSolve has developed various policies and procedures (Including Code of Ethics, Information Security, Disaster Recovery, Patch Management, and Change Management Policies and Procedures), and made them available to all employees on a shared drive to establish organizational operations, integrity, and ethics expectations. At least annually, company policies are reviewed by management for consistency with organizational processes and procedures, as well as alignment with integrity and ethics expectations and risk mitigation strategies.	Inspected the OutSolve Code of Ethics, Information Security Policy, Business Continuity and Disaster Recovery Plan, Incident Response Plan, Network and Patch Management Policy, Change Management and Control Policy, Third Party Management Policy, and Human Resources Background Check and Exit Policy to determine that OutSolve policies and procedures were reviewed by management at least annually.	No exceptions noted.
		Inspected the shared drive and its permissions to determine that OutSolve policies and procedures were made available to all employees on a shared drive.	No exceptions noted.
CC5.2.2	An OutSolve Plan Management System user guide is available to provide instructions for employees to process client data in accordance with commitments and company objectives.	Inspected the OutSolve Plan Management System user guide to determine the existence and inclusion of processing instructions.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Observed the shared network folder and its permissions to determine that the OutSolve Plan Management System instructional manual was made available to all employees.	No exceptions noted.
CC5.2.3	Quarterly reviews of network users for appropriateness are performed by the Chief Technology Officer and the Chief Administrative Officer to determine controls over user access are operating as expected.	For a selection of quarters, inspected the meeting invitation and network user listing to determine that the third party IT support vendor provided a network user listing for review on a quarterly basis to the Chief Technology Officer and the Chief Administrative Officer and the provided network user listing included identification of network user accounts for discussion during quarterly meetings attended by the Chief Technology Officer, the Chief Administrative Officer, and the third party IT support vendor.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC5.2.4	A unique username and password is required for users to access the OutSolve network and the OutSolve Plan Management System. Password parameters enforce the following: - Minimum password length - Complexity - Expiration - Re-use restrictions - Account lockout after a predetermined number of failed login attempts In addition, user access to the OutSolve client web portal requires a unique username and password that enforces complexity and minimum password length.	Inspected the user access listings for the OutSolve network, Plan Management System, and client web portal to determine whether users were assigned unique user IDs.	No exceptions noted.
		Inspected supporting the password parameters for the OutSolve network to determine they consisted of the following: - Minimum password length - Complexity - Expiration - Re-use restrictions - Account lockout after a predetermined number of failed login attempts	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected system configurations to determine that the OutSolve Plan Management System used Active Directory authentication.	No exceptions noted.
		Inspected password parameters to determine that user access to the OutSolve client web portal required a password that enforced complexity and minimum password length.	No exceptions noted.
		Inspected the listing of active directory users to determine that employee and third party vendor users with enabled active directory accounts had passwords that were last set within the timeframe required by the OutSolve Information Security Policies and Procedures.	No exceptions noted.
CC5.2.5	OutSolve's Information Security Policies and Procedures require encryption to be used, where appropriate, to protect sensitive information at rest and in transit. Company e-mail provides the option to encrypt any outgoing e-mail, as needed, to comply with company policy.	Inspected OutSolve's Information Security Policy to determine that it required encryption to be used, where appropriate, to protect sensitive information at rest and in transit.	No exceptions noted.
		Inspected e-mail configurations to determine that Company e-mail provides the option to encrypt any outgoing e-mail to comply with company policy.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC5.2.6	Access to OutSolve systems (network, OutSolve Plan Management System, and client web portal) is restricted through the use of defined application and database user roles, which require a unique username and password. In addition, user access rights are assigned based on job responsibilities.	Inspected supporting documentation to determine that separate user groups were setup in the Active Directory and separate roles existed in the Plan Management System and client web portal.	No exceptions noted.
		For a selection of new hires, inspected user access permissions to determine that new hire user access rights for the OutSolve network were assigned based on job responsibilities.	No exceptions noted.
CC5.2.7	New employee access requests for the network, email, and company systems must be submitted and approved by an authorized employee.	For a selection of new hires, inspected the new hire access request ticket to determine that new employee access for the network, email, and company systems was submitted and approved by an authorized employee.	No exceptions noted.
CC5.2.8	Employee access to the network, email, and company systems is disabled at the time of termination.	For a selection of terminated employees, inspected supporting documentation to determine that user access to the network, email and company systems was disabled or removed at the time of termination.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC5.2.9	Monthly vulnerability scans and penetration tests are performed by a third-party IT vendor. As part of their contracted network management services provided to OutSolve, the third party IT vendor takes action based on the results of the scans. OutSolve monitors the status of the remediation items resulting from the vulnerability scans and penetration tests during quarterly meetings with the third party IT vendor.	For a selection of months, inspected vulnerability scans and penetration test reports to determine that vulnerability scans and penetration tests of OutSolve's network infrastructure were performed by a third party IT vendor on a monthly basis.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no critical or high risk vulnerabilities identified during scans and penetration tests that required remediation. As such, the portion of the control related to remediation did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no critical or high risk external or internal vulnerabilities noted during the period, corroborative inquiry with multiple members of management and inspection of 'External Pentest + Vuln Assessment Executive Summary' report and 'Internal Pentest + Vuln Assessment Executive Summary' report was performed. No indication of critical or high risk vulnerabilities during the period was noted.
CC5.2.10	Current anti-virus software is maintained on OutSolve owned equipment.	Inspected anti-virus software configurations to determine that current anti-virus software was maintained on OutSolve owned equipment.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC5.2.11	Key management personnel meet on a periodic basis to discuss IT operations, strategy, risks, and other relevant topics.	For a selection of months, inspected calendar invitation details and the meeting agenda to determine that key management personnel met on a periodic basis to discuss IT operations, strategy, risks, and other relevant topics.	No exceptions noted.
CC5.2.12	The Chief Technology Officer, the Chief Administrative Officer, and a representative from the third party IT support subservice organization meet on a quarterly basis to discuss information technology needs, issues, and risks managed by the third party service provider. In addition and as possible, identified system technology enhancement opportunities are discussed.	For a selection of quarters, inspected calendar invitation details and meeting materials to determine that OutSolve's Chief Technology Officer and Chief Administrative Officer met with a representative from the third party IT subservice organization to discuss information technology needs, issues, and risks.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Management has implemented operational and security oversight, as well as employee on the job training over information security, confidentiality requirements, and organizational and security policies and procedures, at hire and annually thereafter, to set forth employment standards and establish integrity and ethics expectations.	Inspected training material utilized for new hire and annual training to determine inclusion of information security, confidentiality requirements, and organizational and security policies and procedures.	No exceptions noted.
		For a selection of new hire employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that new hires completed training over information security, confidentiality requirements, and organizational and security policies and procedures.	No exceptions noted.
		For a selection of current employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that employees completed training over information security, confidentiality requirements, and organizational and security policies and procedures, annually.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC5.3.2	OutSolve has developed various policies and procedures (Including Code of Ethics, Information Security, Disaster Recovery, Patch Management, and Change Management Policies and Procedures), and made them available to all employees on a shared drive to establish organizational operations, integrity, and ethics expectations. At least annually, company policies are reviewed by management for consistency with organizational processes and procedures, as well as alignment with integrity and ethics expectations and risk mitigation strategies.	Inspected the OutSolve Code of Ethics, Information Security Policy, Business Continuity and Disaster Recovery Plan, Incident Response Plan, Network and Patch Management Policy, Change Management and Control Policy, Third Party Management Policy, and Human Resources Background Check and Exit Policy to determine that OutSolve policies and procedures were reviewed by management at least annually.	No exceptions noted.
		Inspected the shared drive and its permissions to determine that OutSolve policies and procedures were made available to all employees on a shared drive.	No exceptions noted.
CC5.3.3	OutSolve has developed various documented procedures to ensure that daily operations are performed accurately and completely in accordance with company commitments and requirements.	Inspected the documented procedures to determine the existence and inclusion of information to assist OutSolve employees in performing daily operations accurately and completely.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Observed the shared network folder and its permissions to determine that the documented procedures were made available to all employees.	No exceptions noted.
CC5.3.4	An OutSolve Plan Management System user guide is available to provide instructions for employees to process client data in accordance with commitments and company objectives.	Inspected the OutSolve Plan Management System user guide to determine the existence and inclusion of processing instructions.	No exceptions noted.
		Observed the shared network folder and its permissions to determine that the OutSolve Plan Management System instructional manual was made available to all employees.	No exceptions noted.
CC5.3.5	OutSolve has developed a Document and Data Retention policy to establish documentation retention and disposal requirements to meet confidentiality commitments and system requirements.	Inspected the Document and Data Retention policy to determine that the policy addressed documentation retention and disposal requirements.	No exceptions noted.
CC5.3.6	OutSolve has developed organizational lines of reporting and responsibility that provide for internal separation of duties and oversight. Within each functional area, organizational and reporting hierarchies have been defined, and responsibilities have been assigned.	Inspected OutSolve's organization chart to determine that designed organizational lines of reporting and responsibility provided for internal separation of duties and oversight. In addition, inspected the organization chart to determine that it included the key management level personnel responsible for overseeing the functional areas which address the various elements of OutSolve's organizational operations.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected written job descriptions for the Team Lead and Consultant roles to determine that job responsibilities were documented.	No exceptions noted.
CC5.3.7	OutSolve has developed formal disaster recovery and incident response plans. These plans are reviewed by management annually, and updated as necessary, to accurately reflect current processes and procedures in place to address company commitments and requirements.	Inspected the disaster recovery and incident response plans to determine that they have been developed and were reviewed by management at least annually.	No exceptions noted.
CC5.3.8	OutSolve has a formal employee performance management program that is documented within the Employee Handbook. Annual performance evaluations are based on Company objectives and job responsibilities communicated to employees through job related training, written policies, and documented standard operating procedures. Deviations from established performance and behavior expectations are documented and communicated to employees, and subject to disciplinary action.	Inspected OutSolve's Employee Handbook to determine that it formally documented an employee performance management program.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		For a selection of active employees, inspected the completed 2024 Performance Evaluation template to determine that the annual performance evaluations were completed.	No exceptions noted.
		There were no instances where an employee's performance deviated from established performance and behavior expectations during the period. Therefore, the portion of the control related to deviations from established performance and behavior expectation did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which employee's performance deviated from established performance and behavior expectations during the period, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC6.0: Common Criteria Related to Logical and Physical Access Controls			
CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	Access to OutSolve systems (network, OutSolve Plan Management System, and client web portal) is restricted through the use of defined application and database user roles, which require a unique username and password. In addition, user access rights are assigned based on job responsibilities.	Inspected supporting documentation to determine that separate user groups were setup in the Active Directory and separate roles existed in the Plan Management System and client web portal.	No exceptions noted.
		For a selection of new hires, inspected user access permissions to determine that new hire user access rights for the OutSolve network were assigned based on job responsibilities.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC6.1.2	A unique username and password is required for users to access the OutSolve network and the OutSolve Plan Management System. Password parameters enforce the following: - Minimum password length - Complexity - Expiration - Re-use restrictions - Account lockout after a predetermined number of failed login attempts In addition, user access to the OutSolve client web portal requires a unique username and password that enforces complexity and minimum password length.	Inspected the user access listings for the OutSolve network, Plan Management System, and client web portal to determine whether users were assigned unique user IDs.	No exceptions noted.
		Inspected supporting the password parameters for the OutSolve network to determine they consisted of the following: - Minimum password length - Complexity - Expiration - Re-use restrictions - Account lockout after a predetermined number of failed login attempts	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected system configurations to determine that the OutSolve Plan Management System used Active Directory authentication.	No exceptions noted.
		Inspected password parameters to determine that user access to the OutSolve client web portal required a password that enforced complexity and minimum password length.	No exceptions noted.
		Inspected the listing of active directory users to determine that employee and third party vendor users with enabled active directory accounts had passwords that were last set within the timeframe required by the OutSolve Information Security Policies and Procedures.	No exceptions noted.
CC6.1.3	To manage access to the FTPS server used by clients to upload data, OutSolve requires clients to have a unique username and password and the server must be accessed from a pre-approved IP address.	Inspected the FTPS server configurations to determine that client authentication required the use of a unique username and password.	No exceptions noted.
		Inspected the FTPS server configurations to determine that IP addresses must be added to an approved list before the server can be accessed.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no new IP addresses added to the pre-approved list of IP addresses with access to the FTPS server. As such, the portion of the control related to additions to the pre-approved list of IP addresses did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no new IP addresses added to the pre-approved list of IP addresses with access to the FTP server during the period, corroborative inquiry with multiple members of management and inspection of list of IP addresses available in Progress WS_FTP Server tool was performed. No indication of new IP address during the period was noted.
CC6.1.4	Remote users connect to OutSolve's network through a secure remote desktop connection which requires the use of a VPN and two factor authentication. While connected, employees operate from a terminal server desktop and are not able to copy data to network drives and/or their local machines.	Inspected remote desktop connection configurations to determine that employees were unable to copy data to network drives or their local machines.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected system configurations to determine that the remote desktop connection was established via VPN and required two factor authentication.	No exceptions noted.
CC6.1.5	Current anti-virus software is maintained on OutSolve owned equipment.	Inspected anti-virus software configurations to determine that current anti-virus software was maintained on OutSolve owned equipment.	No exceptions noted.
CC6.1.6	Significant network files and programs, the client portal, and web server are backed up on a daily basis. Backups are encrypted during the backup process. Backups remain encrypted while being replicated to OutSolve's co-location facility.	Inspected backup configurations to determine that backups of significant network files and programs, the client portal, and web server were configured to be performed on a daily basis.	No exceptions noted.
		Inspected backup configurations to determine that backups were configured to be encrypted at the time of back up and while being replicated to OutSolve's co-location facility.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC6.1.7	Monthly vulnerability scans and penetration tests are performed by a third-party IT vendor. As part of their contracted network management services provided to OutSolve, the third party IT vendor takes action based on the results of the scans. OutSolve monitors the status of the remediation items resulting from the vulnerability scans and penetration tests during quarterly meetings with the third party IT vendor.	For a selection of months, inspected vulnerability scans and penetration test reports to determine that vulnerability scans and penetration tests of OutSolve's network infrastructure were performed by a third party IT vendor on a monthly basis.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no critical or high risk vulnerabilities identified during scans and penetration tests that required remediation. As such, the portion of the control related to remediation did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no critical or high risk external or internal vulnerabilities noted during the period, corroborative inquiry with multiple members of management and inspection of 'External Pentest + Vuln Assessment Executive Summary' report and 'Internal Pentest + Vuln Assessment Executive Summary' report was performed. No indication of critical or high risk vulnerabilities during the period was noted.
CC6.1.8	OutSolve's Information Security Policies and Procedures require encryption to be used, where appropriate, to protect sensitive information at rest and in transit. Company e-mail provides the option to encrypt any outgoing e-mail, as needed, to comply with company policy.	Inspected OutSolve's Information Security Policy to determine that it required encryption to be used, where appropriate, to protect sensitive information at rest and in transit.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected e-mail configurations to determine that Company e-mail provides the option to encrypt any outgoing e-mail to comply with company policy.	No exceptions noted.
CC6.1.9	All employee workstations are configured to lock after 15 minutes of inactivity.	Inspected workstation configuration settings to determine that employee workstations were configured to lock after 15 minutes of inactivity.	No exceptions noted.
		Inspected the OutSolve Information Security Policies and Procedures to determine that the policy required all employee workstations to be configured to lock after 15 minutes of inactivity.	No exceptions noted.
CC6.1.10	Mobile Device Management software is in place to control the use of mobile devices that have access to company resources. OutSolve has the ability to remotely wipe devices in the event a device is lost or stolen.	Inspected Mobile Device Management software configurations to determine that mobile device management was in place to control the use of mobile devices that have access to company resources and that OutSolve had the ability to remotely wipe devices in the event a device was lost or stolen.	No exceptions noted.
CC6.1.11	USB port access and use is restricted on OutSolve owned equipment.	Inspected OutSolve User Security configurations to determine that USB port access and use was restricted on OutSolve owned equipment.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC6.1.12	OutSolve has developed a Document and Data Retention policy to establish documentation retention and disposal requirements to meet confidentiality commitments and system requirements.	Inspected the Document and Data Retention policy to determine that the policy addressed documentation retention and disposal requirements.	No exceptions noted.
CC6.1.13	Workstation and laptop hard drives are encrypted.	Inspected system configurations to determine that workstation and laptop hard drives were encrypted.	No exceptions noted.
CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	Access to OutSolve systems (network, OutSolve Plan Management System, and client web portal) is restricted through the use of defined application and database user roles, which require a unique username and password. In addition, user access rights are assigned based on job responsibilities.	Inspected supporting documentation to determine that separate user groups were setup in the Active Directory and separate roles existed in the Plan Management System and client web portal.	No exceptions noted.
		For a selection of new hires, inspected user access permissions to determine that new hire user access rights for the OutSolve network were assigned based on job responsibilities.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC6.2.2	New employee access requests for the network, email, and company systems must be submitted and approved by an authorized employee.	For a selection of new hires, inspected the new hire access request ticket to determine that new employee access for the network, email, and company systems was submitted and approved by an authorized employee.	No exceptions noted.
CC6.2.3	Requests for new user access or changes to existing access to the OutSolve client web portal must come from an approved customer contact. Requests from an unidentified source will be denied.	For a selection of access requests to the OutSolve client web portal, inspected the access request to determine that the requests for access to the OutSolve client web portal were submitted by an approved customer contact.	No exceptions noted.
CC6.2.4	Employee access to the network, email, and company systems is disabled at the time of termination.	For a selection of terminated employees, inspected supporting documentation to determine that user access to the network, email and company systems was disabled or removed at the time of termination.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC6.2.5	Quarterly reviews of network users for appropriateness are performed by the Chief Technology Officer and the Chief Administrative Officer to determine controls over user access are operating as expected.	For a selection of quarters, inspected the meeting invitation and network user listing to determine that the third party IT support vendor provided a network user listing for review on a quarterly basis to the Chief Technology Officer and the Chief Administrative Officer and the provided network user listing included identification of network user accounts for discussion during quarterly meetings attended by the Chief Technology Officer, the Chief Administrative Officer, and the third party IT support vendor.	No exceptions noted.
CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	Access to OutSolve systems (network, OutSolve Plan Management System, and client web portal) is restricted through the use of defined application and database user roles, which require a unique username and password. In addition, user access rights are assigned based on job responsibilities.	Inspected supporting documentation to determine that separate user groups were setup in the Active Directory and separate roles existed in the Plan Management System and client web portal.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		For a selection of new hires, inspected user access permissions to determine that new hire user access rights for the OutSolve network were assigned based on job responsibilities.	No exceptions noted.
CC6.3.2	To manage access to the FTPS server used by clients to upload data, OutSolve requires clients to have a unique username and password and the server must be accessed from a pre-approved IP address.	Inspected the FTPS server configurations to determine that client authentication required the use of a unique username and password.	No exceptions noted.
		Inspected the FTPS server configurations to determine that IP addresses must be added to an approved list before the server can be accessed.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no new IP addresses added to the pre-approved list of IP addresses with access to the FTPS server. As such, the portion of the control related to additions to the pre-approved list of IP addresses did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no new IP addresses added to the pre-approved list of IP addresses with access to the FTP server during the period, corroborative inquiry with multiple members of management and inspection of list of IP addresses available in Progress WS_FTP Server tool was performed. No indication of new IP address during the period was noted.
CC6.3.3	Requests for new user access or changes to existing access to the OutSolve client web portal must come from an approved customer contact. Requests from an unidentified source will be denied.	For a selection of access requests to the OutSolve client web portal, inspected the access request to determine that the requests for access to the OutSolve client web portal were submitted by an approved customer contact.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC6.3.4	New employee access requests for the network, email, and company systems must be submitted and approved by an authorized employee.	For a selection of new hires, inspected the new hire access request ticket to determine that new employee access for the network, email, and company systems was submitted and approved by an authorized employee.	No exceptions noted.
CC6.3.5	Quarterly reviews of network users for appropriateness are performed by the Chief Technology Officer and the Chief Administrative Officer to determine controls over user access are operating as expected.	For a selection of quarters, inspected the meeting invitation and network user listing to determine that the third party IT support vendor provided a network user listing for review on a quarterly basis to the Chief Technology Officer and the Chief Administrative Officer and the provided network user listing included identification of network user accounts for discussion during quarterly meetings attended by the Chief Technology Officer, the Chief Administrative Officer, and the third party IT support vendor.	No exceptions noted.
CC6.3.6	Employee access to the network, email, and company systems is disabled at the time of termination.	For a selection of terminated employees, inspected supporting documentation to determine that user access to the network, email and company systems was disabled or removed at the time of termination.	No exceptions noted.
CC6.3.7	USB port access and use is restricted on OutSolve owned equipment.	Inspected OutSolve User Security configurations to determine that USB port access and use was restricted on OutSolve owned equipment.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4.1	OutSolve administration personnel monitor the front door of the Metairie office location. Visitors are required to enter through the front door, and must be escorted by an OutSolve employee. Additional entry doors into the Metairie office location remain locked, and access is limited to authorized individuals based on unique access codes.	Observed that administration personnel monitored the front door of the Metairie office location, visitors were required to enter through the front door, and additional entry doors into the office location remained locked with key code accessibility.	No exceptions noted.
		For a selection of employees with a unique key code for the additional entry doors into the Metairie office location, compared the employee names to the active employee listing to determine that access was limited to authorized individuals.	No exceptions noted.
CC6.4.2	Access to OutSolve's Sacramento, CA, Louisville, KY, and Charleston, SC office locations is restricted to authorized personnel and points of entry are secured at all times.	Observed the points of entry for the Sacramento, CA, Louisville, KY, and Charleston, SC office locations to determine that they were secured.	No exceptions noted.
CC6.4.3	OutSolve office doors at the Metairie, LA office location remain locked outside of normal business hours.	Observed that the OutSolve office doors at the Metairie, LA office location were locked outside of normal business hours.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC6.4.4	OutSolve contracts with a third party service provider to provide a co-location facility in Dallas, TX and access to OutSolve equipment is restricted to pre-approved individuals.	Inspected the master services agreement with the third party service provider to determine that the service provider was contracted to provide a co-location facility in Dallas, TX.	No exceptions noted.
		Inspected the listing of individuals who were pre-approved to access OutSolve equipment at the third party service provider co-location facility to determine that the listing was restricted to authorized individuals.	No exceptions noted.
CC6.4.5	Upon employee termination, OutSolve restricts office access and collects any company equipment issued to the employee.	For a selection of terminated employees, inspected the termination checklist and building access listing to determine that office access was restricted and company equipment was collected from terminated employees at the time of termination.	No exceptions noted.
CC6.4.6	Access to the server room in the Metairie, LA office location is limited to authorized personnel. Visitors to the server room must be escorted by an authorized OutSolve employee.	Observed that the server room in the Metairie, LA office location was locked and an access code was required to open the door. In addition, observed that visitors were escorted by an authorized OutSolve employee with access to the server room.	No exceptions noted.
		Inspected the listing of individuals with access to the server room to determine that access was limited to authorized personnel.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	OutSolve has developed a Document and Data Retention policy to establish documentation retention and disposal requirements to meet confidentiality commitments and system requirements.	Inspected the Document and Data Retention policy to determine that the policy addressed documentation retention and disposal requirements.	No exceptions noted.
CC6.5.2	The OutSolve Information Security Policies and Procedures address the disposal of decommissioned IT hardware. A third party vendor is used to dispose of decommissioned IT hardware.	Inspected a sample certificate of destruction to determine that OutSolve used a third party vendor to dispose of decommissioned IT hardware.	No exceptions noted.
		Inspected the OutSolve Information Security Policies and Procedures to determine that the policy addressed the disposal of decommissioned IT hardware.	No exceptions noted.
CC6.5.3	For critical technology infrastructure no longer in use in a production environment, OutSolve securely stores the hardware until it is no longer necessary.	Observed that equipment not in use was securely stored.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Access to OutSolve systems (network, OutSolve Plan Management System, and client web portal) is restricted through the use of defined application and database user roles, which require a unique username and password. In addition, user access rights are assigned based on job responsibilities.	Inspected supporting documentation to determine that separate user groups were setup in the Active Directory and separate roles existed in the Plan Management System and client web portal.	No exceptions noted.
		For a selection of new hires, inspected user access permissions to determine that new hire user access rights for the OutSolve network were assigned based on job responsibilities.	No exceptions noted.
CC6.6.2	To manage access to the FTPS server used by clients to upload data, OutSolve requires clients to have a unique username and password and the server must be accessed from a pre-approved IP address.	Inspected the FTPS server configurations to determine that client authentication required the use of a unique username and password.	No exceptions noted.
		Inspected the FTPS server configurations to determine that IP addresses must be added to an approved list before the server can be accessed.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no new IP addresses added to the pre-approved list of IP addresses with access to the FTPS server. As such, the portion of the control related to additions to the pre-approved list of IP addresses did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no new IP addresses added to the pre-approved list of IP addresses with access to the FTP server during the period, corroborative inquiry with multiple members of management and inspection of list of IP addresses available in Progress WS_FTP Server tool was performed. No indication of new IP address during the period was noted.
CC6.6.3	Remote users connect to OutSolve's network through a secure remote desktop connection which requires the use of a VPN and two factor authentication. While connected, employees operate from a terminal server desktop and are not able to copy data to network drives and/or their local machines.	Inspected remote desktop connection configurations to determine that employees were unable to copy data to network drives or their local machines.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected system configurations to determine that the remote desktop connection was established via VPN and required two factor authentication.	No exceptions noted.
CC6.6.4	Current anti-virus software is maintained on OutSolve owned equipment.	Inspected anti-virus software configurations to determine that current anti-virus software was maintained on OutSolve owned equipment.	No exceptions noted.
CC6.6.5	Quarterly reviews of network users for appropriateness are performed by the Chief Technology Officer and the Chief Administrative Officer to determine controls over user access are operating as expected.	For a selection of quarters, inspected the meeting invitation and network user listing to determine that the third party IT support vendor provided a network user listing for review on a quarterly basis to the Chief Technology Officer and the Chief Administrative Officer and the provided network user listing included identification of network user accounts for discussion during quarterly meetings attended by the Chief Technology Officer, the Chief Administrative Officer, and the third party IT support vendor.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC6.6.6	Monthly vulnerability scans and penetration tests are performed by a third-party IT vendor. As part of their contracted network management services provided to OutSolve, the third party IT vendor takes action based on the results of the scans. OutSolve monitors the status of the remediation items resulting from the vulnerability scans and penetration tests during quarterly meetings with the third party IT vendor.	For a selection of months, inspected vulnerability scans and penetration test reports to determine that vulnerability scans and penetration tests of OutSolve's network infrastructure were performed by a third party IT vendor on a monthly basis.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no critical or high risk vulnerabilities identified during scans and penetration tests that required remediation. As such, the portion of the control related to remediation did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no critical or high risk external or internal vulnerabilities noted during the period, corroborative inquiry with multiple members of management and inspection of 'External Pentest + Vuln Assessment Executive Summary' report and 'Internal Pentest + Vuln Assessment Executive Summary' report was performed. No indication of critical or high risk vulnerabilities during the period was noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC6.6.7	The Chief Technology Officer, the Chief Administrative Officer, and a representative from the third party IT support subservice organization meet on a quarterly basis to discuss information technology needs, issues, and risks managed by the third party service provider. In addition and as possible, identified system technology enhancement opportunities are discussed.	For a selection of quarters, inspected calendar invitation details and meeting materials to determine that OutSolve's Chief Technology Officer and Chief Administrative Officer met with a representative from the third party IT subservice organization to discuss information technology needs, issues, and risks.	No exceptions noted.
CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Access to OutSolve systems (network, OutSolve Plan Management System, and client web portal) is restricted through the use of defined application and database user roles, which require a unique username and password. In addition, user access rights are assigned based on job responsibilities.	Inspected supporting documentation to determine that separate user groups were setup in the Active Directory and separate roles existed in the Plan Management System and client web portal.	No exceptions noted.
		For a selection of new hires, inspected user access permissions to determine that new hire user access rights for the OutSolve network were assigned based on job responsibilities.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC6.7.2	USB port access and use is restricted on OutSolve owned equipment.	Inspected OutSolve User Security configurations to determine that USB port access and use was restricted on OutSolve owned equipment.	No exceptions noted.
CC6.7.3	OutSolve provides a secure client portal and a FTPS server for client data uploads.	Observed that a secure client portal and a FTPS server were provided for client data uploads.	No exceptions noted.
		Inspected instructions provided to a customer to determine that a customer was informed of the secure client portal.	No exceptions noted.
CC6.7.4	To manage access to the FTPS server used by clients to upload data, OutSolve requires clients to have a unique username and password and the server must be accessed from a pre-approved IP address.	Inspected the FTPS server configurations to determine that client authentication required the use of a unique username and password.	No exceptions noted.
		Inspected the FTPS server configurations to determine that IP addresses must be added to an approved list before the server can be accessed.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no new IP addresses added to the pre-approved list of IP addresses with access to the FTPS server. As such, the portion of the control related to additions to the pre-approved list of IP addresses did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no new IP addresses added to the pre-approved list of IP addresses with access to the FTP server during the period, corroborative inquiry with multiple members of management and inspection of list of IP addresses available in Progress WS_FTP Server tool was performed. No indication of new IP address during the period was noted.
CC6.7.5	OutSolve's Information Security Policies and Procedures require encryption to be used, where appropriate, to protect sensitive information at rest and in transit. Company e-mail provides the option to encrypt any outgoing e-mail, as needed, to comply with company policy.	Inspected OutSolve's Information Security Policy to determine that it required encryption to be used, where appropriate, to protect sensitive information at rest and in transit.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected e-mail configurations to determine that Company e-mail provides the option to encrypt any outgoing e-mail to comply with company policy.	No exceptions noted.
CC6.7.6	The OutSolve Information Security Policies and Procedures address the disposal of decommissioned IT hardware. A third party vendor is used to dispose of decommissioned IT hardware.	Inspected a sample certificate of destruction to determine that OutSolve used a third party vendor to dispose of decommissioned IT hardware.	No exceptions noted.
		Inspected the OutSolve Information Security Policies and Procedures to determine that the policy addressed the disposal of decommissioned IT hardware.	No exceptions noted.
CC6.7.7	OutSolve maintains a listing of approved customer contacts who are authorized to discuss customer data and receive reports.	Inspected the list of approved customer contacts to determine that OutSolve maintained a listing of approved customer contacts who were authorized to discuss customer data and receive reports.	No exceptions noted.
		For a selection of completed customer reports, inspected the report delivery email and approved customer contact listing to determine that customer reports were provided to approved customer contacts.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC6.7.8	Significant network files and programs, the client portal, and web server are backed up on a daily basis. Backups are encrypted during the backup process. Backups remain encrypted while being replicated to OutSolve's co-location facility.	Inspected backup configurations to determine that backups of significant network files and programs, the client portal, and web server were configured to be performed on a daily basis.	No exceptions noted.
		Inspected backup configurations to determine that backups were configured to be encrypted at the time of back up and while being replicated to OutSolve's co-location facility.	No exceptions noted.
CC6.7.9	Mobile Device Management software is in place to control the use of mobile devices that have access to company resources. OutSolve has the ability to remotely wipe devices in the event a device is lost or stolen.	Inspected Mobile Device Management software configurations to determine that mobile device management was in place to control the use of mobile devices that have access to company resources and that OutSolve had the ability to remotely wipe devices in the event a device was lost or stolen.	No exceptions noted.
CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	Current anti-virus software is maintained on OutSolve owned equipment.	Inspected anti-virus software configurations to determine that current anti-virus software was maintained on OutSolve owned equipment.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC6.8.2	The Chief Technology Officer, the Chief Administrative Officer, and a representative from the third party IT support subservice organization meet on a quarterly basis to discuss information technology needs, issues, and risks managed by the third party service provider. In addition and as possible, identified system technology enhancement opportunities are discussed.	For a selection of quarters, inspected calendar invitation details and meeting materials to determine that OutSolve's Chief Technology Officer and Chief Administrative Officer met with a representative from the third party IT subservice organization to discuss information technology needs, issues, and risks.	No exceptions noted.
CC6.8.3	To document tasks assigned to address any needs, issues, and/or risks communicated during the quarterly meetings with the third party IT support subservice organization, the IT support subservice organization creates a work ticket. OutSolve has the ability to monitor work ticket completion and will receive an update on any tickets and tasks during the subsequent quarterly meeting with the IT support subservice organization.	Observed OutSolve personnel login to the third party IT support subservice organization's ticketing system and review ticket details for an example ticket to determine that OutSolve has the ability to monitor work ticket completion.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		For a selection of quarters, inspected the meeting agenda and material to determine that an update on any tickets and tasks was provided during the subsequent quarterly meeting with the IT support subservice organization.	No exceptions noted.
CC6.8.4	OutSolve has developed a formal Change Management and Control Policy. The policy includes OutSolve's methodology regarding changes, including change requests, evaluation and approval of requested changes, and development, testing, approval, and implementation of changes.	Inspected the Change Management and Control Policy to determine that it addressed change requests, development of changes, and testing, approval, and implementation of changes.	No exceptions noted.
CC6.8.5	Monthly vulnerability scans and penetration tests are performed by a third-party IT vendor. As part of their contracted network management services provided to OutSolve, the third party IT vendor takes action based on the results of the scans. OutSolve monitors the status of the remediation items resulting from the vulnerability scans and penetration tests during quarterly meetings with the third party IT vendor.	For a selection of months, inspected vulnerability scans and penetration test reports to determine that vulnerability scans and penetration tests of OutSolve's network infrastructure were performed by a third party IT vendor on a monthly basis.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no critical or high risk vulnerabilities identified during scans and penetration tests that required remediation. As such, the portion of the control related to remediation did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no critical or high risk external or internal vulnerabilities noted during the period, corroborative inquiry with multiple members of management and inspection of 'External Pentest + Vuln Assessment Executive Summary' report and 'Internal Pentest + Vuln Assessment Executive Summary' report was performed. No indication of critical or high risk vulnerabilities during the period was noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC7.0: Common Criteria Related to System Operations			
CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	The Chief Technology Officer, the Chief Administrative Officer, and a representative from the third party IT support subservice organization meet on a quarterly basis to discuss information technology needs, issues, and risks managed by the third party service provider. In addition and as possible, identified system technology enhancement opportunities are discussed.	For a selection of quarters, inspected calendar invitation details and meeting materials to determine that OutSolve's Chief Technology Officer and Chief Administrative Officer met with a representative from the third party IT subservice organization to discuss information technology needs, issues, and risks.	No exceptions noted.
CC7.1.2	To document tasks assigned to address any needs, issues, and/or risks communicated during the quarterly meetings with the third party IT support subservice organization, the IT support subservice organization creates a work ticket. OutSolve has the ability to monitor work ticket completion and will receive an update on any tickets and tasks during the subsequent quarterly meeting with the IT support subservice organization.	Observed OutSolve personnel login to the third party IT support subservice organization's ticketing system and review ticket details for an example ticket to determine that OutSolve has the ability to monitor work ticket completion.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		For a selection of quarters, inspected the meeting agenda and material to determine that an update on any tickets and tasks was provided during the subsequent quarterly meeting with the IT support subservice organization.	No exceptions noted.
CC7.1.3	Monthly vulnerability scans and penetration tests are performed by a third-party IT vendor. As part of their contracted network management services provided to OutSolve, the third party IT vendor takes action based on the results of the scans. OutSolve monitors the status of the remediation items resulting from the vulnerability scans and penetration tests during quarterly meetings with the third party IT vendor.	For a selection of months, inspected vulnerability scans and penetration test reports to determine that vulnerability scans and penetration tests of OutSolve's network infrastructure were performed by a third party IT vendor on a monthly basis.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no critical or high risk vulnerabilities identified during scans and penetration tests that required remediation. As such, the portion of the control related to remediation did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no critical or high risk external or internal vulnerabilities noted during the period, corroborative inquiry with multiple members of management and inspection of 'External Pentest + Vuln Assessment Executive Summary' report and 'Internal Pentest + Vuln Assessment Executive Summary' report was performed. No indication of critical or high risk vulnerabilities during the period was noted.
CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	Current anti-virus software is maintained on OutSolve owned equipment.	Inspected anti-virus software configurations to determine that current anti-virus software was maintained on OutSolve owned equipment.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC7.2.2	Monthly vulnerability scans and penetration tests are performed by a third-party IT vendor. As part of their contracted network management services provided to OutSolve, the third party IT vendor takes action based on the results of the scans. OutSolve monitors the status of the remediation items resulting from the vulnerability scans and penetration tests during quarterly meetings with the third party IT vendor.	For a selection of months, inspected vulnerability scans and penetration test reports to determine that vulnerability scans and penetration tests of OutSolve's network infrastructure were performed by a third party IT vendor on a monthly basis.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no critical or high risk vulnerabilities identified during scans and penetration tests that required remediation. As such, the portion of the control related to remediation did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no critical or high risk external or internal vulnerabilities noted during the period, corroborative inquiry with multiple members of management and inspection of 'External Pentest + Vuln Assessment Executive Summary' report and 'Internal Pentest + Vuln Assessment Executive Summary' report was performed. No indication of critical or high risk vulnerabilities during the period was noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC7.2.3	The Chief Technology Officer, the Chief Administrative Officer, and a representative from the third party IT support subservice organization meet on a quarterly basis to discuss information technology needs, issues, and risks managed by the third party service provider. In addition and as possible, identified system technology enhancement opportunities are discussed.	For a selection of quarters, inspected calendar invitation details and meeting materials to determine that OutSolve's Chief Technology Officer and Chief Administrative Officer met with a representative from the third party IT subservice organization to discuss information technology needs, issues, and risks.	No exceptions noted.
CC7.2.4	To document tasks assigned to address any needs, issues, and/or risks communicated during the quarterly meetings with the third party IT support subservice organization, the IT support subservice organization creates a work ticket. OutSolve has the ability to monitor work ticket completion and will receive an update on any tickets and tasks during the subsequent quarterly meeting with the IT support subservice organization.	Observed OutSolve personnel login to the third party IT support subservice organization's ticketing system and review ticket details for an example ticket to determine that OutSolve has the ability to monitor work ticket completion.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		For a selection of quarters, inspected the meeting agenda and material to determine that an update on any tickets and tasks was provided during the subsequent quarterly meeting with the IT support subservice organization.	No exceptions noted.
CC7.2.5	OutSolve has developed formal disaster recovery and incident response plans. These plans are reviewed by management annually, and updated as necessary, to accurately reflect current processes and procedures in place to address company commitments and requirements.	Inspected the disaster recovery and incident response plans to determine that they have been developed and were reviewed by management at least annually.	No exceptions noted.
CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	OutSolve has developed formal disaster recovery and incident response plans. These plans are reviewed by management annually, and updated as necessary, to accurately reflect current processes and procedures in place to address company commitments and requirements.	Inspected the disaster recovery and incident response plans to determine that they have been developed and were reviewed by management at least annually.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	OutSolve has developed formal disaster recovery and incident response plans. These plans are reviewed by management annually, and updated as necessary, to accurately reflect current processes and procedures in place to address company commitments and requirements.	Inspected the disaster recovery and incident response plans to determine that they have been developed and were reviewed by management at least annually.	No exceptions noted.
CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	OutSolve has developed formal disaster recovery and incident response plans. These plans are reviewed by management annually, and updated as necessary, to accurately reflect current processes and procedures in place to address company commitments and requirements.	Inspected the disaster recovery and incident response plans to determine that they have been developed and were reviewed by management at least annually.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC8.0: Common Criteria Related to Change Management			
CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	OutSolve has developed a formal Change Management and Control Policy. The policy includes OutSolve's methodology regarding changes, including change requests, evaluation and approval of requested changes, and development, testing, approval, and implementation of changes.	Inspected the Change Management and Control Policy to determine that it addressed change requests, development of changes, and testing, approval, and implementation of changes.	No exceptions noted.
CC8.1.2	Changes to the network made by the third party IT support vendor are reviewed and approved by OutSolve management.	For a selection of network changes made by the third party IT support, inspected support tickets to determine that network changes made by the third party IT support vendor were approved by OutSolve management prior to implementation.	No exceptions noted.
CC8.1.3	The user requesting a change to the OutSolve Plan Management System performs user acceptance testing and notifies the Chief Technology Officer of any issues with the change.	For a selection of changes to the OutSolve Plan Management System, inspected e-mail correspondence to determine that user acceptance testing was performed by the user requesting the change and the Chief Technology Officer was notified of any issues with the change.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC8.1.4	For the OutSolve Plan Management System, the development and testing environment is isolated from production. All development activities must be performed in the designated environment. Testing is performed prior to deploying the change to the production environment.	Inspected screenshots of the development, testing, and production environment permissions to determine that for the OutSolve Plan Management System, the development and testing environment was isolated from the production environment.	No exceptions noted.
		For a selection of changes to the OutSolve Plan Management System, inspected e-mail correspondence and the published date of the change to determine that testing was performed prior to deploying the change to production.	No exceptions noted.
CC8.1.5	OutSolve has implemented a log to document all changes to the OutSolve Plan Management System.	Inspected the OutSolve Application Change Log for existence.	No exceptions noted.
		Inspected the OutSolve Plan Management production environment and observed that all changes in the production environment corresponded to entries recorded in the OutSolve Application Change Log.	No exceptions noted.
CC8.1.6	Access to the testing environment of the OutSolve Plan Management System and the ability to deploy changes into the production environment is restricted to authorized personnel.	Inspected the OutSolve Plan Management System configurations to determine testing environment access and the ability to deploy changes into the production environment was restricted to authorized personnel.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC9.0: Common Criteria Related to Risk Mitigation			
CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	OutSolve evaluates the risks that threaten its commitments and requirements through an annual risk assessment process. Recommendations resulting from the risk assessment are tracked and monitored.	Inspected the completed annual risk assessment to determine that OutSolve evaluated the risks that threaten its commitments and requirements through an annual risk assessment process.	No exceptions noted.
		Inspected the risk assessment recommendation update presentation to determine that recommendations resulting from the risk assessment were tracked and monitored.	No exceptions noted.
CC9.1.2	OutSolve maintains insurance coverage for commercial general liability, as well as professional, privacy, and network security claims and events.	Inspected insurance certificates to determine that insurance coverage was maintained for commercial general liability, as well as professional, privacy, and network security claims and events.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC9.2: The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	OutSolve has a documented Third Party Management policy and process to evaluate third party organizations prior to contracting with them for services and periodically thereafter to determine their achievement of contracted responsibilities, including standards of conduct that align with OutSolve's organizational expectations.	Inspected the Third Party Management policy to determine that it addresses the third party organization evaluations performed prior to contracting for services and periodically thereafter.	No exceptions noted.
		There were no new vendors for the period. Therefore, the portion of the control related to the performance of a vendor review prior to contracting with new vendors did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no new vendors during the period, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
CC9.2.2	OutSolve has contracts or other provisions in place with key third party organizations to document their responsibilities and requirements, including standards of conduct that align with OutSolve's organizational expectations. As part of ongoing monitoring and communications, OutSolve will provide necessary feedback to third party organizations if their personnel and/or service offerings are not meeting contractual requirements and expectations. Changes in services, commitments, or requirements require an appropriate addendum to the existing contract or a new contract to be executed.	There were no new instances of new key third party organizations contracted during the examination period to determine existence and inclusion of documented responsibilities and requirements. Therefore, no substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period that a new third party organization was contracted to perform services, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no instances during the exam period in which a third party organization needed to be contacted regarding contractual requirements and expectations not being met. Therefore, no further substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which a third party organization needed to be contacted regarding contractual requirements and expectations not being met, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no instances during the exam period in which an existing third party organization's services, commitments, or requirements changed. Therefore, no further substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which a third party organization's services, commitments, or requirements changed, performed corroborative inquiry with multiple members of management. No instances were reported.
		Inspected the vendor contract for a selection of key third party organizations to determine that OutSolve has contracts or other provisions in place with key third party organizations to document their responsibilities and requirements.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
A1.0: Additional Criteria Related to Availability			
A1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	The Chief Technology Officer, the Chief Administrative Officer, and a representative from the third party IT support subservice organization meet on a quarterly basis to discuss information technology needs, issues, and risks managed by the third party service provider. In addition and as possible, identified system technology enhancement opportunities are discussed.	For a selection of quarters, inspected calendar invitation details and meeting materials to determine that OutSolve's Chief Technology Officer and Chief Administrative Officer met with a representative from the third party IT subservice organization to discuss information technology needs, issues, and risks.	No exceptions noted.
A1.1.2	To document tasks assigned to address any needs, issues, and/or risks communicated during the quarterly meetings with the third party IT support subservice organization, the IT support subservice organization creates a work ticket. OutSolve has the ability to monitor work ticket completion and will receive an update on any tickets and tasks during the subsequent quarterly meeting with the IT support subservice organization.	Observed OutSolve personnel login to the third party IT support subservice organization's ticketing system and review ticket details for an example ticket to determine that OutSolve has the ability to monitor work ticket completion.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		For a selection of quarters, inspected the meeting agenda and material to determine that an update on any tickets and tasks was provided during the subsequent quarterly meeting with the IT support subservice organization.	No exceptions noted.
A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A1.2.1	Access to the server room in the Metairie, LA office location is limited to authorized personnel. Visitors to the server room must be escorted by an authorized OutSolve employee.	Observed that the server room in the Metairie, LA office location was locked and an access code was required to open the door. In addition, observed that visitors were escorted by an authorized OutSolve employee with access to the server room.	No exceptions noted.
		Inspected the listing of individuals with access to the server room to determine that access was limited to authorized personnel.	No exceptions noted.
A1.2.2	The server room temperature is regulated using an independent air conditioner. Temperature monitoring is configured to alert OutSolve personnel if temperatures exceed the preestablished threshold.	Observed the existence of an independent air conditioner in the server room.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected temperature monitoring configurations to determine that temperature monitoring was configured to alert OutSolve personnel if temperatures exceeded the preestablished threshold.	No exceptions noted.
A1.2.3	Hand-held fire extinguishers are located throughout the Metairie, LA office space. In addition, smoke detectors are strategically located throughout the Metairie facility.	Observed that smoke detectors and fire extinguishers were located throughout the Metairie, LA office location.	No exceptions noted.
A1.2.4	An Uninterruptible Power Supply (UPS) is installed to protect the server room in the Metairie, LA office location from short-term power failures.	Observed that a UPS device was installed in the Metairie, LA office location server room.	No exceptions noted.
A1.2.5	OutSolve contracts with a third party organization to provide periodic air conditioning maintenance services for the equipment in the server room in the Metairie, LA office location.	For a selection of periodic maintenance dates, inspected service invoices from the third party maintenance provider to determine the air conditioning equipment in the server room received maintenance services during the exam period.	No exceptions noted.
A1.2.6	OutSolve has developed formal disaster recovery and incident response plans. These plans are reviewed by management annually, and updated as necessary, to accurately reflect current processes and procedures in place to address company commitments and requirements.	Inspected the disaster recovery and incident response plans to determine that they have been developed and were reviewed by management at least annually.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
A1.2.7	Significant network files and programs, the client portal, and web server are backed up on a daily basis. Backups are encrypted during the backup process. Backups remain encrypted while being replicated to OutSolve's co-location facility.	Inspected backup configurations to determine that backups of significant network files and programs, the client portal, and web server were configured to be performed on a daily basis.	No exceptions noted.
		Inspected backup configurations to determine that backups were configured to be encrypted at the time of back up and while being replicated to OutSolve's co-location facility.	No exceptions noted.
A1.2.8	A quarterly test restoration of a sample data set is performed to verify that backup data is recoverable.	On a sample basis, inspected quarterly email notifications from the IT support vendor to determine that test restorations of sampled backed up data sets were completed and communicated to OutSolve. In addition, inspected supporting documentation to determine that restorations of sampled backed up data sets were successful.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	OutSolve has developed formal disaster recovery and incident response plans. These plans are reviewed by management annually, and updated as necessary, to accurately reflect current processes and procedures in place to address company commitments and requirements.	Inspected the disaster recovery and incident response plans to determine that they have been developed and were reviewed by management at least annually.	No exceptions noted.
A1.3.2	A quarterly test restoration of a sample data set is performed to verify that backup data is recoverable.	On a sample basis, inspected quarterly email notifications from the IT support vendor to determine that test restorations of sampled backed up data sets were completed and communicated to OutSolve. In addition, inspected supporting documentation to determine that restorations of sampled backed up data sets were successful.	No exceptions noted.
A1.3.3	Significant network files and programs, the client portal, and web server are backed up on a daily basis. Backups are encrypted during the backup process. Backups remain encrypted while being replicated to OutSolve's co-location facility.	Inspected backup configurations to determine that backups of significant network files and programs, the client portal, and web server were configured to be performed on a daily basis.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected backup configurations to determine that backups were configured to be encrypted at the time of back up and while being replicated to OutSolve's co-location facility.	No exceptions noted.
C1.0: Additional Criteria Related to Confidentiality			
C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	Employees are required to sign a confidentiality agreement regarding any client and OutSolve information at hire and sign an acknowledgement of the agreement annually.	For a selection of new hires, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine new hires acknowledged the Confidentiality Agreement during the onboarding process.	No exceptions noted.
		For a selection of current employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that employees acknowledged the Confidentiality Agreement on an annual basis.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
C1.1.2	OutSolve has contracts or other provisions in place with key third party organizations to document their responsibilities and requirements, including standards of conduct that align with OutSolve's organizational expectations. As part of ongoing monitoring and communications, OutSolve will provide necessary feedback to third party organizations if their personnel and/or service offerings are not meeting contractual requirements and expectations. Changes in services, commitments, or requirements require an appropriate addendum to the existing contract or a new contract to be executed.	There were no new instances of new key third party organizations contracted during the examination period to determine existence and inclusion of documented responsibilities and requirements. Therefore, no substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period that a new third party organization was contracted to perform services, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no instances during the exam period in which a third party organization needed to be contacted regarding contractual requirements and expectations not being met. Therefore, no further substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which a third party organization needed to be contacted regarding contractual requirements and expectations not being met, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no instances during the exam period in which an existing third party organization's services, commitments, or requirements changed. Therefore, no further substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which a third party organization's services, commitments, or requirements changed, performed corroborative inquiry with multiple members of management. No instances were reported.
		Inspected the vendor contract for a selection of key third party organizations to determine that OutSolve has contracts or other provisions in place with key third party organizations to document their responsibilities and requirements.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
C1.1.3	Quarterly reviews of network users for appropriateness are performed by the Chief Technology Officer and the Chief Administrative Officer to determine controls over user access are operating as expected.	For a selection of quarters, inspected the meeting invitation and network user listing to determine that the third party IT support vendor provided a network user listing for review on a quarterly basis to the Chief Technology Officer and the Chief Administrative Officer and the provided network user listing included identification of network user accounts for discussion during quarterly meetings attended by the Chief Technology Officer, the Chief Administrative Officer, and the third party IT support vendor.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
C1.1.4	A unique username and password is required for users to access the OutSolve network and the OutSolve Plan Management System. Password parameters enforce the following: - Minimum password length - Complexity - Expiration - Re-use restrictions - Account lockout after a predetermined number of failed login attempts In addition, user access to the OutSolve client web portal requires a unique username and password that enforces complexity and minimum password length.	Inspected the user access listings for the OutSolve network, Plan Management System, and client web portal to determine whether users were assigned unique user IDs.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected supporting the password parameters for the OutSolve network to determine they consisted of the following: - Minimum password length - Complexity - Expiration - Re-use restrictions - Account lockout after a predetermined number of failed login attempts	No exceptions noted.
		Inspected system configurations to determine that the OutSolve Plan Management System used Active Directory authentication.	No exceptions noted.
		Inspected password parameters to determine that user access to the OutSolve client web portal required a password that enforced complexity and minimum password length.	No exceptions noted.
		Inspected the listing of active directory users to determine that employee and third party vendor users with enabled active directory accounts had passwords that were last set within the timeframe required by the OutSolve Information Security Policies and Procedures.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
C1.1.5	OutSolve's Information Security Policies and Procedures require encryption to be used, where appropriate, to protect sensitive information at rest and in transit. Company e-mail provides the option to encrypt any outgoing e-mail, as needed, to comply with company policy.	Inspected OutSolve's Information Security Policy to determine that it required encryption to be used, where appropriate, to protect sensitive information at rest and in transit.	No exceptions noted.
		Inspected e-mail configurations to determine that Company e-mail provides the option to encrypt any outgoing e-mail to comply with company policy.	No exceptions noted.
C1.1.6	OutSolve has developed a Document and Data Retention policy to establish documentation retention and disposal requirements to meet confidentiality commitments and system requirements.	Inspected the Document and Data Retention policy to determine that the policy addressed documentation retention and disposal requirements.	No exceptions noted.
C1.1.7	The relationship between OutSolve and its customers is contractual in nature. Customer contracts include relevant information regarding the design and operation of the system, including system boundaries, confidentiality requirements, and standard service commitments.	For a selection of new customers, inspected new customer contracts to determine that customer contracts included standard, as well as customer specific service commitments and customer responsibilities along with relevant information regarding design and operation of the system, including system boundaries, confidentiality requirements, and standard service commitments.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
C1.2: The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	OutSolve has developed a Document and Data Retention policy to establish documentation retention and disposal requirements to meet confidentiality commitments and system requirements.	Inspected the Document and Data Retention policy to determine that the policy addressed documentation retention and disposal requirements.	No exceptions noted.
C1.2.2	The OutSolve Information Security Policies and Procedures address the disposal of decommissioned IT hardware. A third party vendor is used to dispose of decommissioned IT hardware.	Inspected a sample certificate of destruction to determine that OutSolve used a third party vendor to dispose of decommissioned IT hardware.	No exceptions noted.
		Inspected the OutSolve Information Security Policies and Procedures to determine that the policy addressed the disposal of decommissioned IT hardware.	No exceptions noted.
PI1.1: The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.			
PI1.1.1	OutSolve requests client data utilizing the Requested Data Elements form. OutSolve requires clients to submit requested data in the appropriate electronic format to meet data processing timeliness objectives and increase the likelihood of data accuracy and completeness.	Inspected the Requested Data Elements form to determine existence and to gain an understanding of the data submission specifications.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected instructions provided to a customer to determine that a customer was requested to utilize the Requested Data Elements form to provide requested data in the appropriate electronic format.	No exceptions noted.
PI1.1.2	An OutSolve Plan Management System user guide is available to provide instructions for employees to process client data in accordance with commitments and company objectives.	Inspected the OutSolve Plan Management System user guide to determine the existence and inclusion of processing instructions.	No exceptions noted.
		Observed the shared network folder and its permissions to determine that the OutSolve Plan Management System instructional manual was made available to all employees.	No exceptions noted.
PI1.1.3	OutSolve has developed various documented procedures to ensure that daily operations are performed accurately and completely in accordance with company commitments and requirements.	Inspected the documented procedures to determine the existence and inclusion of information to assist OutSolve employees in performing daily operations accurately and completely.	No exceptions noted.
		Observed the shared network folder and its permissions to determine that the documented procedures were made available to all employees.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
PI1.1.4	Management has implemented operational and security oversight, as well as employee on the job training over information security, confidentiality requirements, and organizational and security policies and procedures, at hire and annually thereafter, to set forth employment standards and establish integrity and ethics expectations.	Inspected training material utilized for new hire and annual training to determine inclusion of information security, confidentiality requirements, and organizational and security policies and procedures.	No exceptions noted.
		For a selection of new hire employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that new hires completed training over information security, confidentiality requirements, and organizational and security policies and procedures.	No exceptions noted.
		For a selection of current employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that employees completed training over information security, confidentiality requirements, and organizational and security policies and procedures, annually.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
PI1.1.5	The relationship between OutSolve and its customers is contractual in nature. Customer contracts include relevant information regarding the design and operation of the system, including system boundaries, confidentiality requirements, and standard service commitments.	For a selection of new customers, inspected new customer contracts to determine that customer contracts included standard, as well as customer specific service commitments and customer responsibilities along with relevant information regarding design and operation of the system, including system boundaries, confidentiality requirements, and standard service commitments.	No exceptions noted.
PI1.2: The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.			
PI1.2.1	OutSolve requests client data utilizing the Requested Data Elements form. OutSolve requires clients to submit requested data in the appropriate electronic format to meet data processing timeliness objectives and increase the likelihood of data accuracy and completeness.	Inspected the Requested Data Elements form to determine existence and to gain an understanding of the data submission specifications.	No exceptions noted.
		Inspected instructions provided to a customer to determine that a customer was requested to utilize the Requested Data Elements form to provide requested data in the appropriate electronic format.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
PI1.2.2	At the time client data is uploaded to the OutSolve Plan Management System and after data processing and report generation, data validation is performed by the system to reasonably ensure client provided data is complete and accurate. Upon completion of the data validation process, an error log is generated for review by an OutSolve employee. Identified errors are researched and corrected.	For a selection of completed client reports, inspected the error log generated after the completion of data validation to determine that data validation is performed by the system.	No exceptions noted.
PI1.2.3	All client reports undergo a quality control review. This quality control review must be performed by an employee other than the employee who completed the report. A log of available quality control reviews and completed quality control reviews is tracked in the OutSolve Plan Management System.	Inspected the Data Quality Control Queue to determine that the OutSolve Plan Management System tracked the quality control review process.	No exceptions noted.
		For a selection of completed client reports, inspected the quality control completion e-mail notification to determine that quality control reviews were completed by an employee that did not complete the report.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
PI1.2.4	After a quality control review of a client report is performed, the original preparer is notified of any errors noted during the review. The preparer is responsible for correcting all identified errors. Upon completion of necessary error corrections, the preparer updates a field in the OutSolve Plan Management System to indicate report completion.	For a selection of completed client reports, inspected the quality control completion e-mail notification and the report completion date within the system to determine that the original preparer of a client report was notified of any errors identified during the quality control review and that the client report was updated after the completion of the quality control review.	No exceptions noted.
PI1.2.5	OutSolve has developed various documented procedures to ensure that daily operations are performed accurately and completely in accordance with company commitments and requirements.	Inspected the documented procedures to determine the existence and inclusion of information to assist OutSolve employees in performing daily operations accurately and completely.	No exceptions noted.
		Observed the shared network folder and its permissions to determine that the documented procedures were made available to all employees.	No exceptions noted.
PI1.2.6	Prior to making non-format changes to customer provided data, OutSolve obtains customer approval from an authorized customer contact.	Inspected the documented customer approval that was obtained from an authorized customer contact for a non-format change.	No exceptions noted.
PI1.2.7	A Team Lead is assigned to each client. The Team Lead is responsible for monitoring production and ensuring client commitments are fulfilled.	For a selection of new clients, inspected production reports to determine that a Team Lead was assigned to each client.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected the Team Lead job description to determine that the Team Leads were responsible for monitoring production and ensuring client commitments are fulfilled.	No exceptions noted.
PI1.2.8	The Chief Operations Officer generates reports monthly to collect information necessary to monitor production and identify necessary employee feedback and actions to meet company objectives. After the reports are generated, the Chief Operations Officer meets with the President to discuss the status of all outstanding projects and action items to meet commitments and requirements.	For a selection of months, inspected calendar details and the monthly production report to determine that the Chief Operations Officer and the President had a recurring monthly production review meeting scheduled and the Chief Operations Officer generated monthly reports to collect information necessary to monitor production and identify necessary employee feedback and actions to meet company objectives.	No exceptions noted.
PI1.3: The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.			
PI1.3.1	Management has implemented operational and security oversight, as well as employee on the job training over information security, confidentiality requirements, and organizational and security policies and procedures, at hire and annually thereafter, to set forth employment standards and establish integrity and ethics expectations.	Inspected training material utilized for new hire and annual training to determine inclusion of information security, confidentiality requirements, and organizational and security policies and procedures.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		For a selection of new hire employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that new hires completed training over information security, confidentiality requirements, and organizational and security policies and procedures.	No exceptions noted.
		For a selection of current employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that employees completed training over information security, confidentiality requirements, and organizational and security policies and procedures, annually.	No exceptions noted.
PI1.3.2	An OutSolve Plan Management System user guide is available to provide instructions for employees to process client data in accordance with commitments and company objectives.	Inspected the OutSolve Plan Management System user guide to determine the existence and inclusion of processing instructions.	No exceptions noted.
		Observed the shared network folder and its permissions to determine that the OutSolve Plan Management System instructional manual was made available to all employees.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
PI1.3.3	OutSolve has developed various documented procedures to ensure that daily operations are performed accurately and completely in accordance with company commitments and requirements.	Inspected the documented procedures to determine the existence and inclusion of information to assist OutSolve employees in performing daily operations accurately and completely.	No exceptions noted.
		Observed the shared network folder and its permissions to determine that the documented procedures were made available to all employees.	No exceptions noted.
PI1.3.4	OutSolve requests client data utilizing the Requested Data Elements form. OutSolve requires clients to submit requested data in the appropriate electronic format to meet data processing timeliness objectives and increase the likelihood of data accuracy and completeness.	Inspected the Requested Data Elements form to determine existence and to gain an understanding of the data submission specifications.	No exceptions noted.
		Inspected instructions provided to a customer to determine that a customer was requested to utilize the Requested Data Elements form to provide requested data in the appropriate electronic format.	No exceptions noted.
PI1.4: The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.			
PI1.4.1	OutSolve provides a secure client portal and a FTPS server for client data uploads.	Observed that a secure client portal and a FTPS server were provided for client data uploads.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		Inspected instructions provided to a customer to determine that a customer was informed of the secure client portal.	No exceptions noted.
PI1.4.2	OutSolve follows up with all first year clients via email to verify completion of contracted services.	For a selection of first year clients, inspected e-mail communication to determine first year clients were contacted to verify completion of contracted services.	No exceptions noted.
PI1.4.3	An OutSolve Plan Management System user guide is available to provide instructions for employees to process client data in accordance with commitments and company objectives.	Inspected the OutSolve Plan Management System user guide to determine the existence and inclusion of processing instructions.	No exceptions noted.
		Observed the shared network folder and its permissions to determine that the OutSolve Plan Management System instructional manual was made available to all employees.	No exceptions noted.
PI1.4.4	At the time client data is uploaded to the OutSolve Plan Management System and after data processing and report generation, data validation is performed by the system to reasonably ensure client provided data is complete and accurate. Upon completion of the data validation process, an error log is generated for review by an OutSolve employee. Identified errors are researched and corrected.	For a selection of completed client reports, inspected the error log generated after the completion of data validation to determine that data validation is performed by the system.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
PI1.4.5	All client reports undergo a quality control review. This quality control review must be performed by an employee other than the employee who completed the report. A log of available quality control reviews and completed quality control reviews is tracked in the OutSolve Plan Management System.	Inspected the Data Quality Control Queue to determine that the OutSolve Plan Management System tracked the quality control review process.	No exceptions noted.
		For a selection of completed client reports, inspected the quality control completion e-mail notification to determine that quality control reviews were completed by an employee that did not complete the report.	No exceptions noted.
PI1.4.6	After a quality control review of a client report is performed, the original preparer is notified of any errors noted during the review. The preparer is responsible for correcting all identified errors. Upon completion of necessary error corrections, the preparer updates a field in the OutSolve Plan Management System to indicate report completion.	For a selection of completed client reports, inspected the quality control completion e-mail notification and the report completion date within the system to determine that the original preparer of a client report was notified of any errors identified during the quality control review and that the client report was updated after the completion of the quality control review.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
PI1.4.7	OutSolve has developed various documented procedures to ensure that daily operations are performed accurately and completely in accordance with company commitments and requirements.	Inspected the documented procedures to determine the existence and inclusion of information to assist OutSolve employees in performing daily operations accurately and completely.	No exceptions noted.
		Observed the shared network folder and its permissions to determine that the documented procedures were made available to all employees.	No exceptions noted.
PI1.4.8	A Team Lead is assigned to each client. The Team Lead is responsible for monitoring production and ensuring client commitments are fulfilled.	For a selection of new clients, inspected production reports to determine that a Team Lead was assigned to each client.	No exceptions noted.
		Inspected the Team Lead job description to determine that the Team Leads were responsible for monitoring production and ensuring client commitments are fulfilled.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
PI1.4.9	The Chief Operations Officer generates reports monthly to collect information necessary to monitor production and identify necessary employee feedback and actions to meet company objectives. After the reports are generated, the Chief Operations Officer meets with the President to discuss the status of all outstanding projects and action items to meet commitments and requirements.	For a selection of months, inspected calendar details and the monthly production report to determine that the Chief Operations Officer and the President had a recurring monthly production review meeting scheduled and the Chief Operations Officer generated monthly reports to collect information necessary to monitor production and identify necessary employee feedback and actions to meet company objectives.	No exceptions noted.
PI1.4.10	OutSolve's client reporting process includes a billing oversight function to ensure client bills only include agreed upon and completed services. Any identified discrepancies are communicated to appropriate personnel.	For a selection of completed client reports, inspected supporting documentation to determine that bills for client reporting were reviewed by appropriate personnel to ensure the bills only included agreed upon and completed services.	No exceptions noted.
		Inspected example follow up communication related to a discrepancy identified during a bill review to determine that discrepancies identified during the bill review process were communicated to appropriate personnel.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
PI1.5: The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.			
PI1.5.1	Significant network files and programs, the client portal, and web server are backed up on a daily basis. Backups are encrypted during the backup process. Backups remain encrypted while being replicated to OutSolve's co-location facility.	Inspected backup configurations to determine that backups of significant network files and programs, the client portal, and web server were configured to be performed on a daily basis.	No exceptions noted.
		Inspected backup configurations to determine that backups were configured to be encrypted at the time of back up and while being replicated to OutSolve's co-location facility.	No exceptions noted.
PI1.5.2	A quarterly test restoration of a sample data set is performed to verify that backup data is recoverable.	On a sample basis, inspected quarterly email notifications from the IT support vendor to determine that test restorations of sampled backed up data sets were completed and communicated to OutSolve. In addition, inspected supporting documentation to determine that restorations of sampled backed up data sets were successful.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
PI1.5.3	OutSolve has developed formal disaster recovery and incident response plans. These plans are reviewed by management annually, and updated as necessary, to accurately reflect current processes and procedures in place to address company commitments and requirements.	Inspected the disaster recovery and incident response plans to determine that they have been developed and were reviewed by management at least annually.	No exceptions noted.
P1.1: The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.			
P1.1.1	The external privacy policy is posted on a website and is visible to data subjects.	Inspected OutSolve' s privacy policy on the OutSolve external website to determine that the external privacy policy was posted on a website and was visible to data subjects.	No exceptions noted.
P1.1.2	The external privacy policy is reviewed annually by management.	Inspected OutSolve's privacy policy on the OutSolve external website to determine that the external privacy policy was reviewed annually by management.	No exceptions noted.
P1.1.3	The external privacy policy has a clear version stamp allowing data subjects to determine whether any changes have been applied since their last use of the system.	Inspected OutSolve's privacy policy on the OutSolve external website to determine that the external privacy policy had a clear version stamp allowing data subjects to determine whether any changes have been applied since their last use of the system.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P2.1: The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.			
P2.1.1	Data subjects are informed of their choices regarding data collection and the consequences of each choice, through the posted external privacy policy.	Inspected OutSolve's privacy policy on the OutSolve external website to determine that the data subjects were informed of their choices regarding data collection and the consequences of each choice, through the posted external privacy policy.	No exceptions noted.
P2.1.2	The external privacy policy is posted on a website and is visible to data subjects.	Inspected OutSolve' s privacy policy on the OutSolve external website to determine that the external privacy policy was posted on a website and was visible to data subjects.	No exceptions noted.
P2.1.3	The basis for consent on behalf of data subjects is described in the posted external privacy policy.	Inspected OutSolve's privacy policy on the OutSolve external website to determine that the basis for consent on behalf of data subjects was described in the posted external privacy policy.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P3.1: Personal information is collected consistent with the entity's objectives related to privacy.			
P3.1.1	The internal privacy policy defines the privacy objectives as well as the roles and responsibilities of internal personnel. The internal privacy policy is available to employees on an internal site.	Inspected OutSolve's internal privacy policy to determine that the internal privacy policy defined the privacy objectives as well as the roles and responsibilities of internal personnel. Also, inspected the intranet to determine that the internal privacy policy was made available to employees on an internal site.	No exceptions noted.
P3.1.2	The internal privacy policy is reviewed annually by management.	Inspected OutSolve's internal privacy policy to determine that the internal privacy policy was reviewed annually by management.	No exceptions noted.
P3.1.3	The Personally Identifiable Information Handling Procedures policy document is reviewed annually by management.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document was reviewed annually by management.	No exceptions noted.
P3.1.4	The Personally Identifiable Information Handling Procedures policy document is available to employees on an internal site.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document was made available to employees on an internal site.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P3.1.5	Employees are required to read and acknowledge their understanding of the internal privacy policy within 30 days of hire and annually thereafter.	For a selection of current employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that employees read and acknowledged the internal privacy policy annually.	No exceptions noted.
		For a selection of new hire employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that new hire employees read and acknowledged the internal privacy policy within 30 days of their hire date.	No exceptions noted.
P3.1.6	The basis for consent on behalf of data subjects is described in the posted external privacy policy.	Inspected OutSolve's privacy policy on the OutSolve external website to determine that the basis for consent on behalf of data subjects was described in the posted external privacy policy.	No exceptions noted.
P3.2: For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.			
P3.2.1	The basis for consent on behalf of data subjects is described in the posted external privacy policy.	Inspected OutSolve's privacy policy on the OutSolve external website to determine that the basis for consent on behalf of data subjects was described in the posted external privacy policy.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P3.2.2	The external privacy policy is posted on a website and is visible to data subjects.	Inspected OutSolve' s privacy policy on the OutSolve external website to determine that the external privacy policy was posted on a website and was visible to data subjects.	No exceptions noted.
P3.2.3	Data subjects are informed of their choices regarding data collection and the consequences of each choice, through the posted external privacy policy.	Inspected OutSolve's privacy policy on the OutSolve external website to determine that the data subjects were informed of their choices regarding data collection and the consequences of each choice, through the posted external privacy policy.	No exceptions noted.
P4.1: The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.			
P4.1.1	The internal privacy policy defines the privacy objectives as well as the roles and responsibilities of internal personnel. The internal privacy policy is available to employees on an internal site.	Inspected OutSolve's internal privacy policy to determine that the internal privacy policy defined the privacy objectives as well as the roles and responsibilities of internal personnel. Also, inspected the intranet to determine that the internal privacy policy was made available to employees on an internal site.	No exceptions noted.
P4.1.2	The internal privacy policy is reviewed annually by management.	Inspected OutSolve's internal privacy policy to determine that the internal privacy policy was reviewed annually by management.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P4.1.3	The Personally Identifiable Information Handling Procedures policy document is reviewed annually by management.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document was reviewed annually by management.	No exceptions noted.
P4.1.4	The Personally Identifiable Information Handling Procedures policy document is available to employees on an internal site.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document was made available to employees on an internal site.	No exceptions noted.
P4.1.5	Employees are required to read and acknowledge their understanding of the internal privacy policy within 30 days of hire and annually thereafter.	For a selection of current employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that employees read and acknowledged the internal privacy policy annually.	No exceptions noted.
		For a selection of new hire employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that new hire employees read and acknowledged the internal privacy policy within 30 days of their hire date.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P4.1.6	Access to OutSolve systems (network, OutSolve Plan Management System, and client web portal) is restricted through the use of defined application and database user roles, which require a unique username and password. In addition, user access rights are assigned based on job responsibilities.	Inspected supporting documentation to determine that separate user groups were setup in the Active Directory and separate roles existed in the Plan Management System and client web portal.	No exceptions noted.
		For a selection of new hires, inspected user access permissions to determine that new hire user access rights for the OutSolve network were assigned based on job responsibilities.	No exceptions noted.
P4.1.7	Quarterly reviews of network users for appropriateness are performed by the Chief Technology Officer and the Chief Administrative Officer to determine controls over user access are operating as expected.	For a selection of quarters, inspected the meeting invitation and network user listing to determine that the third party IT support vendor provided a network user listing for review on a quarterly basis to the Chief Technology Officer and the Chief Administrative Officer and the provided network user listing included identification of network user accounts for discussion during quarterly meetings attended by the Chief Technology Officer, the Chief Administrative Officer, and the third party IT support vendor.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P4.2: The entity retains personal information consistent with the entity's objectives related to privacy.			
P4.2.1	OutSolve has developed a Document and Data Retention policy to establish documentation retention and disposal requirements to meet confidentiality commitments and system requirements.	Inspected the Document and Data Retention policy to determine that the policy addressed documentation retention and disposal requirements.	No exceptions noted.
P4.2.2	Significant network files and programs, the client portal, and web server are backed up on a daily basis. Backups are encrypted during the backup process. Backups remain encrypted while being replicated to OutSolve's co-location facility.	Inspected backup configurations to determine that backups of significant network files and programs, the client portal, and web server were configured to be performed on a daily basis.	No exceptions noted.
		Inspected backup configurations to determine that backups were configured to be encrypted at the time of back up and while being replicated to OutSolve's co-location facility.	No exceptions noted.
P4.2.3	A quarterly test restoration of a sample data set is performed to verify that backup data is recoverable.	On a sample basis, inspected quarterly email notifications from the IT support vendor to determine that test restorations of sampled backed up data sets were completed and communicated to OutSolve. In addition, inspected supporting documentation to determine that restorations of sampled backed up data sets were successful.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P4.2.4	Personally Identifiable Information Handling Procedures policy document defines the procedures for processing data deletion requests.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document defined the procedures for processing data deletion requests.	No exceptions noted.
P4.2.5	The internal privacy policy defines the privacy objectives as well as the roles and responsibilities of internal personnel. The internal privacy policy is available to employees on an internal site.	Inspected OutSolve's internal privacy policy to determine that the internal privacy policy defined the privacy objectives as well as the roles and responsibilities of internal personnel. Also, inspected the intranet to determine that the internal privacy policy was made available to employees on an internal site.	No exceptions noted.
P4.2.6	The basis for consent on behalf of data subjects is described in the posted external privacy policy.	Inspected OutSolve's privacy policy on the OutSolve external website to determine that the basis for consent on behalf of data subjects was described in the posted external privacy policy.	No exceptions noted.
P4.3: The entity securely disposes of personal information to meet the entity's objectives related to privacy.			
P4.3.1	Personally Identifiable Information Handling Procedures policy document defines the procedures for processing data deletion requests.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document defined the procedures for processing data deletion requests.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P4.3.2	The internal privacy policy defines the privacy objectives as well as the roles and responsibilities of internal personnel. The internal privacy policy is available to employees on an internal site.	Inspected OutSolve's internal privacy policy to determine that the internal privacy policy defined the privacy objectives as well as the roles and responsibilities of internal personnel. Also, inspected the intranet to determine that the internal privacy policy was made available to employees on an internal site.	No exceptions noted.
P4.3.3	The Personally Identifiable Information Handling Procedures policy document is available to employees on an internal site.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document was made available to employees on an internal site.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P4.3.4	Data deletion requests are logged and tracked to resolution by the OutSolve management.	There were no data deletion request raised during the audit period. As such, the control did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no data deletion request raised during the period, corroborative inquiry with multiple members of management and inspection of Data Disposal Request Log was performed. No indication of data review request during the period was noted.
P4.3.5	OutSolve disposes of confidential information according to its data retention policy.	Inspected the 'Document and Data Retention' clause in Information Security Policies and Procedures document to determine that OutSolve disposed of confidential information according to its data retention policy.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P5.1: The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.			
P5.1.1	The Personally Identifiable Information Handling Procedures policy document defines the procedures for processing data review requests.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document defined the procedures for processing data review requests.	No exceptions noted.
P5.1.2	The internal privacy policy defines the privacy objectives as well as the roles and responsibilities of internal personnel. The internal privacy policy is available to employees on an internal site.	Inspected OutSolve's internal privacy policy to determine that the internal privacy policy defined the privacy objectives as well as the roles and responsibilities of internal personnel. Also, inspected the intranet to determine that the internal privacy policy was made available to employees on an internal site.	No exceptions noted.
P5.1.3	The Personally Identifiable Information Handling Procedures policy document is available to employees on an internal site.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document was made available to employees on an internal site.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P5.1.4	The Personally Identifiable Information Handling Procedures policy document defines the procedures for processing data subject requests for data inventories.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document defined the procedures for processing data subject requests for data inventories.	No exceptions noted.
P5.1.5	Data inventory requests are logged and tracked to resolution by the OutSolve management.	There were no data inventory request raised during the audit period. As such, the control did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no data inventory request raised during the period, corroborative inquiry with multiple members of management and inspection of Privacy Data Request Log was performed. No indication of data review request during the period was noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P5.2: The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.			
P5.2.1	The internal privacy policy defines the privacy objectives as well as the roles and responsibilities of internal personnel. The internal privacy policy is available to employees on an internal site.	Inspected OutSolve's internal privacy policy to determine that the internal privacy policy defined the privacy objectives as well as the roles and responsibilities of internal personnel. Also, inspected the intranet to determine that the internal privacy policy was made available to employees on an internal site.	No exceptions noted.
P5.2.2	Employees are required to read and acknowledge their understanding of the internal privacy policy within 30 days of hire and annually thereafter.	For a selection of current employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that employees read and acknowledged the internal privacy policy annually.	No exceptions noted.
		For a selection of new hire employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that new hire employees read and acknowledged the internal privacy policy within 30 days of their hire date.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P5.2.3	The external privacy policy includes contact information allowing data subject to contact OutSolve directly.	Inspected OutSolve's privacy policy on the OutSolve external website to determine that the external privacy policy included contact information allowing data subject to contact OutSolve directly.	No exceptions noted.
P5.2.4	The Personally Identifiable Information Handling Procedures policy document defines the procedures for processing data correction requests.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document defined the procedures for processing data correction requests.	No exceptions noted.
P5.2.5	The Personally Identifiable Information Handling Procedures policy document is available to employees on an internal site.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document was made available to employees on an internal site.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P5.2.6	Data correction requests are logged and tracked to resolution by the OutSolve management.	There were no data correction request raised during the audit period. As such, the control did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no data correction request raised during the period, corroborative inquiry with multiple members of management and inspection of Privacy Data Request Log was performed. No indication of data review request during the period was noted.
P6.1: The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.			
P6.1.1	The basis for consent on behalf of data subjects is described in the posted external privacy policy.	Inspected OutSolve's privacy policy on the OutSolve external website to determine that the basis for consent on behalf of data subjects was described in the posted external privacy policy.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P6.1.2	Requests for PII disclosure from authorized third-parties are documented, approved by management and communicated to affected data subjects prior to disclosure. Consent of the data subjects is obtained if required.	There were no requests for PII disclosure from authorized third-parties raised during the audit period. As such, the control did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no requests for PII disclosure from authorized third-parties raised during the period, corroborative inquiry with multiple members of management and inspection of Privacy Data Request Log was performed. No indication of data review request during the period was noted.
P6.1.3	Data subjects are informed of their choices regarding data collection and the consequences of each choice, through the posted external privacy policy.	Inspected OutSolve's privacy policy on the OutSolve external website to determine that the data subjects were informed of their choices regarding data collection and the consequences of each choice, through the posted external privacy policy.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P6.2: The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.			
P6.2.1	The Personally Identifiable Information Handling Procedures policy document defines the procedures for processing data subject requests for data inventories.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document defined the procedures for processing data subject requests for data inventories.	No exceptions noted.
P6.2.2	Data inventory requests are logged and tracked to resolution by the OutSolve management.	There were no data inventory request raised during the audit period. As such, the control did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no data inventory request raised during the period, corroborative inquiry with multiple members of management and inspection of Privacy Data Request Log was performed. No indication of data review request during the period was noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P6.2.3	The Personally Identifiable Information Handling Procedures policy document is available to employees on an internal site.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document was made available to employees on an internal site.	No exceptions noted.
P6.2.4	The internal privacy policy defines the privacy objectives as well as the roles and responsibilities of internal personnel. The internal privacy policy is available to employees on an internal site.	Inspected OutSolve's internal privacy policy to determine that the internal privacy policy defined the privacy objectives as well as the roles and responsibilities of internal personnel. Also, inspected the intranet to determine that the internal privacy policy was made available to employees on an internal site.	No exceptions noted.
P6.3: The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.			
P6.3.1	OutSolve has developed formal disaster recovery and incident response plans. These plans are reviewed by management annually, and updated as necessary, to accurately reflect current processes and procedures in place to address company commitments and requirements.	Inspected the disaster recovery and incident response plans to determine that they have been developed and were reviewed by management at least annually.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P6.3.2	Incidents are documented and communicated to management and external users in accordance with the Incident Response Plan and are tracked until resolved.	There were no incidents raised during the audit period. As such, the control did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no incidents raised during the period, corroborative inquiry with multiple members of management and inspection of Incident Log was performed. No indication of incidents during the period was noted.
P6.3.3	External users are provided with contact information on OutSolve's website to report any failures, incidents, concerns, and other complaints to OutSolve management.	Inspected OutSolve's external privacy policy on the OutSolve external website to determine that the external users were provided with contact information on OutSolve's website to report any failures, incidents, concerns, and other complaints to OutSolve management.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P6.4: The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.			
P6.4.1	Privacy commitments, including commitments related to data breach notification, are included in agreements with third-parties with access or potential access to personal information.	For a selection of third-parties with access to personal information, inspected the vendor contracts to determine that the privacy commitments, including commitments related to data breach notification, were included in agreements with third-parties with access or potential access to personal information.	No exceptions noted.
P6.4.2	OutSolve has contractual provisions in place to require third-parties to notify OutSolve of actual or suspected unauthorized access to personal information provided by OutSolve.	For a selection of third-parties with access to personal information, inspected the vendor contracts to determine that the OutSolve had contractual provisions in place to require third-parties to notify OutSolve of actual or suspected unauthorized access to personal information provided by OutSolve.	No exceptions noted.
P6.4.3	OutSolve has a documented Third Party Management policy and process to evaluate third party organizations prior to contracting with them for services and periodically thereafter to determine their achievement of contracted responsibilities, including standards of conduct that align with OutSolve's organizational expectations.	Inspected the Third Party Management policy to determine that it addresses the third party organization evaluations performed prior to contracting for services and periodically thereafter.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no new vendors for the period. Therefore, the portion of the control related to the performance of a vendor review prior to contracting with new vendors did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no new vendors during the period, performed corroborative inquiry with multiple members of management. No instances were reported.
P6.4.4	OutSolve has contracts or other provisions in place with key third party organizations to document their responsibilities and requirements, including standards of conduct that align with OutSolve's organizational expectations. As part of ongoing monitoring and communications, OutSolve will provide necessary feedback to third party organizations if their personnel and/or service offerings are not meeting contractual requirements and expectations. Changes in services, commitments, or requirements require an appropriate addendum to the existing contract or a new contract to be executed.	There were no new instances of new key third party organizations contracted during the examination period to determine existence and inclusion of documented responsibilities and requirements. Therefore, no substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period that a new third party organization was contracted to perform services, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no instances during the exam period in which a third party organization needed to be contacted regarding contractual requirements and expectations not being met. Therefore, no further substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which a third party organization needed to be contacted regarding contractual requirements and expectations not being met, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no instances during the exam period in which an existing third party organization's services, commitments, or requirements changed. Therefore, no further substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which a third party organization's services, commitments, or requirements changed, performed corroborative inquiry with multiple members of management. No instances were reported.
		Inspected the vendor contract for a selection of key third party organizations to determine that OutSolve has contracts or other provisions in place with key third party organizations to document their responsibilities and requirements.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P6.5: The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.			
P6.5.1	Privacy commitments, including commitments related to data breach notification, are included in agreements with third-parties with access or potential access to personal information.	For a selection of third-parties with access to personal information, inspected the vendor contracts to determine that the privacy commitments, including commitments related to data breach notification, were included in agreements with third-parties with access or potential access to personal information.	No exceptions noted.
P6.5.2	OutSolve has contractual provisions in place to require third-parties to notify OutSolve of actual or suspected unauthorized access to personal information provided by OutSolve.	For a selection of third-parties with access to personal information, inspected the vendor contracts to determine that the OutSolve had contractual provisions in place to require third-parties to notify OutSolve of actual or suspected unauthorized access to personal information provided by OutSolve.	No exceptions noted.
P6.5.3	OutSolve has a documented Third Party Management policy and process to evaluate third party organizations prior to contracting with them for services and periodically thereafter to determine their achievement of contracted responsibilities, including standards of conduct that align with OutSolve's organizational expectations.	Inspected the Third Party Management policy to determine that it addresses the third party organization evaluations performed prior to contracting for services and periodically thereafter.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no new vendors for the period. Therefore, the portion of the control related to the performance of a vendor review prior to contracting with new vendors did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no new vendors during the period, performed corroborative inquiry with multiple members of management. No instances were reported.
P6.5.4	OutSolve has contracts or other provisions in place with key third party organizations to document their responsibilities and requirements, including standards of conduct that align with OutSolve's organizational expectations. As part of ongoing monitoring and communications, OutSolve will provide necessary feedback to third party organizations if their personnel and/or service offerings are not meeting contractual requirements and expectations. Changes in services, commitments, or requirements require an appropriate addendum to the existing contract or a new contract to be executed.	There were no new instances of new key third party organizations contracted during the examination period to determine existence and inclusion of documented responsibilities and requirements. Therefore, no substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period that a new third party organization was contracted to perform services, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no instances during the exam period in which a third party organization needed to be contacted regarding contractual requirements and expectations not being met. Therefore, no further substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which a third party organization needed to be contacted regarding contractual requirements and expectations not being met, performed corroborative inquiry with multiple members of management. No instances were reported.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
		There were no instances during the exam period in which an existing third party organization's services, commitments, or requirements changed. Therefore, no further substantive testing was performed.	Non-operational. To substantiate management's statement that there were no instances during the exam period in which a third party organization's services, commitments, or requirements changed, performed corroborative inquiry with multiple members of management. No instances were reported.
		Inspected the vendor contract for a selection of key third party organizations to determine that OutSolve has contracts or other provisions in place with key third party organizations to document their responsibilities and requirements.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P6.6: The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.			
P6.6.1	OutSolve has developed formal disaster recovery and incident response plans. These plans are reviewed by management annually, and updated as necessary, to accurately reflect current processes and procedures in place to address company commitments and requirements.	Inspected the disaster recovery and incident response plans to determine that they have been developed and were reviewed by management at least annually.	No exceptions noted.
P6.6.2	Incidents are documented and communicated to management and external users in accordance with the Incident Response Plan and are tracked until resolved.	There were no incidents raised during the audit period. As such, the control did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no incidents raised during the period, corroborative inquiry with multiple members of management and inspection of Incident Log was performed. No indication of incidents during the period was noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P6.6.3	OutSolve has contractual provisions in place to require third-parties to notify OutSolve of actual or suspected unauthorized access to personal information provided by OutSolve.	For a selection of third-parties with access to personal information, inspected the vendor contracts to determine that the OutSolve had contractual provisions in place to require third-parties to notify OutSolve of actual or suspected unauthorized access to personal information provided by OutSolve.	No exceptions noted.
P6.7: The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.			
P6.7.1	The Personally Identifiable Information Handling Procedures policy document defines the procedures for processing data subject requests for data inventories.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document defined the procedures for processing data subject requests for data inventories.	No exceptions noted.
P6.7.2	The internal privacy policy defines the privacy objectives as well as the roles and responsibilities of internal personnel. The internal privacy policy is available to employees on an internal site.	Inspected OutSolve's internal privacy policy to determine that the internal privacy policy defined the privacy objectives as well as the roles and responsibilities of internal personnel. Also, inspected the intranet to determine that the internal privacy policy was made available to employees on an internal site.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P6.7.3	The Personally Identifiable Information Handling Procedures policy document is available to employees on an internal site.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document was made available to employees on an internal site.	No exceptions noted.
P6.7.4	Data inventory requests are logged and tracked to resolution by the OutSolve management.	There were no data inventory request raised during the audit period. As such, the control did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no data inventory request raised during the period, corroborative inquiry with multiple members of management and inspection of Privacy Data Request Log was performed. No indication of data review request during the period was noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P7.1: The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.			
P7.1.1	The internal privacy policy defines the privacy objectives as well as the roles and responsibilities of internal personnel. The internal privacy policy is available to employees on an internal site.	Inspected OutSolve's internal privacy policy to determine that the internal privacy policy defined the privacy objectives as well as the roles and responsibilities of internal personnel. Also, inspected the intranet to determine that the internal privacy policy was made available to employees on an internal site.	No exceptions noted.
P7.1.2	The Personally Identifiable Information Handling Procedures policy document is available to employees on an internal site.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document was made available to employees on an internal site.	No exceptions noted.
P7.1.3	Employees are required to read and acknowledge their understanding of the internal privacy policy within 30 days of hire and annually thereafter.	For a selection of current employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that employees read and acknowledged the internal privacy policy annually.	No exceptions noted.
		For a selection of new hire employees, inspected the signed OutSolve Data Security Standards Acknowledgment and Agreement to determine that new hire employees read and acknowledged the internal privacy policy within 30 days of their hire date.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P7.1.4	OutSolve requests client data utilizing the Requested Data Elements form. OutSolve requires clients to submit requested data in the appropriate electronic format to meet data processing timeliness objectives and increase the likelihood of data accuracy and completeness.	Inspected the Requested Data Elements form to determine existence and to gain an understanding of the data submission specifications.	No exceptions noted.
		Inspected instructions provided to a customer to determine that a customer was requested to utilize the Requested Data Elements form to provide requested data in the appropriate electronic format.	No exceptions noted.
P7.1.5	At the time client data is uploaded to the OutSolve Plan Management System and after data processing and report generation, data validation is performed by the system to reasonably ensure client provided data is complete and accurate. Upon completion of the data validation process, an error log is generated for review by an OutSolve employee. Identified errors are researched and corrected.	For a selection of completed client reports, inspected the error log generated after the completion of data validation to determine that data validation is performed by the system.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P8.1: The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.			
P8.1.1	The external privacy policy includes contact information allowing data subject to contact OutSolve directly.	Inspected OutSolve's privacy policy on the OutSolve external website to determine that the external privacy policy included contact information allowing data subject to contact OutSolve directly.	No exceptions noted.
P8.1.2	External users are provided with contact information on OutSolve's website to report any failures, incidents, concerns, and other complaints to OutSolve management.	Inspected OutSolve's external privacy policy on the OutSolve external website to determine that the external users were provided with contact information on OutSolve's website to report any failures, incidents, concerns, and other complaints to OutSolve management.	No exceptions noted.
P8.1.3	The Personally Identifiable Information Handling Procedures policy document defines the procedures for processing data correction requests.	Inspected the Personally Identifiable Information Handling Procedures policy to determine that the Personally Identifiable Information Handling Procedures policy document defined the procedures for processing data correction requests.	No exceptions noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P8.1.4	Data review requests are logged and tracked to resolution by the OutSolve management.	There were no data review request raised during the audit period. As such, the control did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no data review request raised during the period, corroborative inquiry with multiple members of management and inspection of Privacy Data Request Log was performed. No indication of data review request during the period was noted.

Control Number	OutSolve LLC's Controls	Independent Service Auditor's Test	Results
P8.1.5	Data correction requests are logged and tracked to resolution by the OutSolve management.	There were no data correction request raised during the audit period. As such, the control did not operate and tests of operating effectiveness were not performed.	Non-operational. To substantiate management's statement that there were no data correction request raised during the period, corroborative inquiry with multiple members of management and inspection of Privacy Data Request Log was performed. No indication of data review request during the period was noted.

SECTION FIVE

Other Information Provided by OutSolve, LLC That Is Not Covered by the Independent Service Auditor's Report

SECTION FIVE – OTHER INFORMATION PROVIDED BY OUTSOLVE, LLC THAT IS NOT COVERED BY THE INDEPENDENT SERVICE AUDITOR'S REPORT

The information in this section describing OutSolve, LLC's (OutSolve) development of a new cloud-based production system is presented by OutSolve to provide additional information and is not a part of OutSolve's description of controls that may be relevant to user organizations' internal control. Such information has not been subjected to the procedures applied in the examination of the description of the Plan Management System and, accordingly, the auditor expresses no opinion on it.

New Production System

In October 2023, OutSolve engaged a third-party vendor, West Monroe Partners, to design and develop a new cloud-based production system that will be in Microsoft Azure. The design and development of the new production system was ongoing during the current year examination period April 1, 2024 through March 31, 2025. The new production system was excluded from the scope of the current year SOC 2 examination and management's system description. As of the report date (May 14, 2025), client data was not hosted within the new production system.