



Mangrove Employer Services, Inc.

Independent Service Auditor's Report on Controls
Placed in Operation and Tests of
Operating Effectiveness for the Period

January 1, 2010 – December 31, 2010

SAS70 TYPE II



70
CPA



MANGROVE EMPLOYER SERVICES, INC.

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITOR’S REPORT.....	3
II. INFORMATION PROVIDED BY MANGROVE EMPLOYER SERVICES, INC.	6
DESCRIPTION OF RELEVANT CONTROLS PROVIDED BY MANGROVE EMPLOYER SERVICES, INC.	7
Products and Services Overview.....	7
RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, MONITORING, AND INFORMATION AND COMMUNICATION.....	10
Control Environment.....	10
Risk Assessment	15
Monitoring	15
Information Systems and Communication.....	16
Control Activities.....	29
User Control Considerations.....	37
III. INFORMATION PROVIDED BY SAS 70 CPA.....	39
CONTROL OBJECTIVES, RELATED CONTROLS, AND TESTS OF OPERATING EFFECTIVENESS	40
Control Objective 1 – Organization and Administration	40
Control Objective 2 – Human Resources Security	42
Control Objective 3 – Physical Access	44
Control Objective 4 – Environment Security.....	47
Control Objective 5 – Backup and Recovery.....	49
Control Objective 6 – Computer Operations	51
Control Objective 7 – Logical Access	52
Control Objective 8 – Data Communications	54
Control Objective 9 – Disaster Recovery.....	55
Control Objective 10 – Secure Storage, Media, and Document Destruction.....	56
Control Objective 11 – Application Development and Change Management.....	57
Control Objective 12 – Benefit Plan Administration.....	59
Control Objective 13 – Payroll Implementation	61
Control Objective 14 – Payroll Processing	63
Control Objective 15 – Tax Reconciliation	65

I. INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

Richard Cangemi
Mangrove Employer Services, Inc.
1501 South Church Avenue
Tampa, FL 33629

We have examined the accompanying description of controls related to the Information Technology, payroll, and benefits administration transactions environment of Mangrove Employer Services, Inc. (Mangrove) for users of these services. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of Mangrove's controls that may be relevant to a user organization's internal controls as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of Mangrove's controls, and (3) such controls had been placed in operation as of December 31, 2010. The control objectives were specified by the management of Mangrove. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

The scope of this SAS 70 Service Auditor's Report engagement is restricted only to Mangrove Employer Services, Inc. and does not extend to cover the payroll operations of its service bureau customers, for which Mangrove Employer Services, Inc. is only a subservice organization.

In our opinion, the accompanying description of the aforementioned controls presents fairly, in all material respects, the relevant aspects of Mangrove's controls that had been placed in operation as of December 31, 2010. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the user control considerations contemplated in the design of Mangrove's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific control activities, listed in Section III, to obtain evidence about their effectiveness in meeting the related control objectives during the period from January 1, 2010, to December 31, 2010. The specific controls and the nature, timing, extent, and results of the tests are listed in Section III. This information has been provided to user organizations of Mangrove and to their auditors to be taken into consideration, along with information about internal controls at user organizations, when making assessments of control risk for user organizations. In our opinion, the controls that were tested as described in Section III were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Section III were achieved during the period from January 1, 2010 to December 31, 2010.

The relative effectiveness and significance of specific controls at Mangrove and their effect on assessments of control risk at user organizations are dependent on their interaction with the controls and other facts present at individual user organizations. We have performed no procedures to evaluate the effectiveness of control activities at individual user organizations.

The description of controls at Mangrove is as of December 31, 2010 and information about tests of the operating effectiveness of specified control activities covers the period from January 1, 2010 to December

31, 2010. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at Mangrove is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions based on our findings to future periods is subject to the risk that changes made to the system or controls, or the failure to make needed changes to the system or controls, or changes required because of the passage of time may alter the validity of such conclusions.

This report is intended solely for the use of management of Mangrove, its user organizations, and the independent auditors of its user organizations.

SAS 70 CPA

SAS 70 CPA
2997-A Alternate 19
Palm Harbor, FL 34647

April 19, 2011

II. INFORMATION PROVIDED BY MANGROVE EMPLOYER SERVICES, INC.

DESCRIPTION OF RELEVANT CONTROLS PROVIDED BY MANGROVE EMPLOYER SERVICES, INC.

Overview of Operations

Founded in 1994 as Mangrove Software, Mangrove Employer Services, Inc. (Mangrove) has been characterized by consistent growth and a high level of financial and managerial stability. Mangrove has grown from a single project and one client in 1994 to over 1,000 successful implementations and over 10,000 organizations utilizing its payroll and software solutions today.

As stated in the Service Auditor's Letter, the scope of this SAS 70 Service Auditor's Report engagement is restricted only to Mangrove Employer Services, Inc. and does not extend to cover the payroll operations of its service bureau customers, for which Mangrove Employer Services, Inc. is only a subservice organization.

In February of 2007, Mangrove Software acquired BenefitOne of America. In doing so, it made a significant strategic investment and forged into the Benefits Administration business. BenefitOne was located in the same geographic location and shared many philosophical strategies as Mangrove. In addition, BenefitOne had been in the COBRA business since it was enacted in the mid 1980's and had grown to be a national provider of COBRA, HIPAA, Retiree and Leave of Absence billing, as well as Flexible Spending Accounts (FSA) services with full debit card administration. This acquisition was central to renaming the collective organizations to Mangrove Employer Services, Inc. Mangrove now has the ability to provide a much broader range of services to employers to assist in managing their employees.

In the fall of 2007, Mangrove made another strategic acquisition by acquiring Access1Source-Nevada Payroll Processing Operations located in Las Vegas, Nevada.

In July 2009, Mangrove expanded its payroll operations again by acquiring Access 1Source-Utah Payroll Processing Operations based in American Fork, UT.

These acquisitions expanded Mangrove's ability to provide Human Resource Management, Payroll Processing, and Benefits Administration Services to for-profit clients, non-profit clients, and service bureau organizations. Mangrove's capabilities range from experienced, time-tested software development to multi-project integration activities designed to improve an employer's ability to manage their employee population. Mangrove has created innovative, personalized solutions for even the most complex benefit plans.

Mangrove physically conducts operations out of Tampa, Florida and Las Vegas, Nevada. All IT and data processing assets are located in Tampa. All benefits administration operations occur in Tampa. All payroll service bureau operations are conducted from Las Vegas.

Products and Services Overview

Mangrove provides payroll software services to dozens of payroll Service Bureau Organizations (SBO) and 300 Application Service Providers (ASP). Mangrove's proprietary Workforce Empowerment™ payroll software platform provides payroll, Human Resource Management System (HRMS), benefits management, and recruitment management services in an online, Web-based environment. User organizations are connected to Mangrove via the Internet that provides online, real time access to the Workforce Empowerment™ payroll software platform. Mangrove markets its Workforce Empowerment™ payroll software platform to Payroll Service Bureau Organizations which provide payroll services to other client companies as well as Software as a Service (SaaS) fulfillment customers. In the SaaS market, Mangrove provides payroll services directly to the end user customer. In the Service Bureau Organization market, the

end user can elect to have its data and software hosted by Mangrove on Mangrove's servers. Alternately, Mangrove also licenses its software to be installed locally on client's hardware.

Benefits Administration

Mangrove's full-service benefits administration solutions help streamline Human Resource departments. Mangrove clients can take advantage of personalized offerings for COBRA, Flexible Spending Accounts (FSA), Health Savings Accounts (HSA), Health Reimbursement Arrangements (HRA) with debit card administration, Leave of Absence (LOA) billing, and Retiree billing.

Mangrove's customized solutions maintain strict compliance and utilize cutting-edge technology to provide virtually paperless administration. Mangrove takes administrative and compliance responsibilities seriously and has done so since COBRA was enacted in 1985.

Mangrove provides support for:

- ***COBRA Administration*** – Mangrove's COBRA business has been in place since COBRA was enacted in the mid-1980's. The compliance procedures are used by all size employers across the country today. The customized solutions maintain strict compliance with COBRA regulations while utilization of technology allows them to provide the client and COBRA-qualified beneficiaries more flexibility and choices as they interact with Mangrove.
- ***Retiree Billing and LOA Billing*** – Mangrove provides service for Retirees and Employees on Leave for premium billing.
- ***HIPAA and Certificates of Coverage*** – Mangrove's applications automate the process of completing the HIPAA certification process.
- ***FSA and Debit Card*** – Mangrove offers a fully automated service model approach to Flexible Spending Accounts administration under Section 125 Plans. Mangrove offers 'auto-adjudication' through the debit card which also can also be 'stacked' to allow for the addition of HSA dollars or HRA dollars.

Time Keeping

Mangrove's automated Time and Attendance solution is designed to meet the labor management needs of organizations of all sizes. The Time Keeping solution is completely Web-based and fully integrated with Mangrove's Workforce Empowerment Suite.

Mangrove's Timekeeping Solution offers the following benefits:

Ease of Use – There is no software to install. Users can view, edit, and run reports using a Web browser. Mangrove's Web-based server automatically does all the collecting, calculating, processing, and reporting necessary.

Savings and Affordability – Mangrove's automated timekeeping system is designed for the small to mid-size business with a focus on saving time and money. Mangrove offers brand-name equipment as well as including upgrades and daily email reports.

Convenience – The Internet-enabled time clock allows clients to monitor employees across an organization from their personal computers.

Payroll

Mangrove provides a platform to process payroll, print checks, print reports, create and send ACH files, and report taxes, all without limits on companies, employees, earnings, deductions, taxes, or net pay distributions. Users can employ multiple time entry methods, from time clock integration to online timesheets, and manage automatic sweeps and escrow payments. Additionally, Mangrove offers private branding, comprehensive back office tools, and an á la carte menu of services.

Payroll Features include:

- Payroll processing for an unlimited number of employees and per state transactions
- Third-party AP check generation for garnishments, tax levies, union dues, labor allocations, and more
- Multiple organizational tiers for sophisticated job costing and general ledger capabilities
- Ability to easily process multiple pay frequencies
- General ledger interface to increase data accuracy and reduce redundant data entry
- User definable roles with multi-level security options
- Handles FLSA, overtime, and state minimum wage compliance requirements
- Automatically receive updated tax codes for federal, state, and municipal requirements
- Send tax payments automatically via standard ACH processing
- Enter employee time worked via Mangrove's Web timesheet or import timecard information data from third-party time collection systems
- Access to over 600 standard reports with the ability for users to quickly develop custom reports

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, MONITORING, AND INFORMATION AND COMMUNICATION

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The control environment has a pervasive influence on the way business activities are structured, objectives are established, and risks are assessed. It also influences control activities, information and communication systems, and monitoring procedures. The control environment is influenced by an entity's history and managerial culture. Effectively controlled entities strive to have competent people, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive corporate direction. These entities establish appropriate controls which foster shared values and teamwork in pursuit of the organization's objectives.

Control environment elements include the following, and the extent to which each element is addressed at Mangrove is described below:

- Management Controls, Philosophy, and Operating Style
- Integrity and Ethical Values
- Organizational Structure
- Assignment of Authority and Responsibility
- Standard Operating Controls
- Audit
- Risk Management
- Monitoring

Management Controls, Philosophy, and Operating Style

Management is responsible for directing and controlling operations, establishing, communicating, monitoring control policies and procedures, as well as setting the tone for the organization. Importance is placed on accuracy and integrity, maintaining written and updated procedures, security and privacy, and establishing and maintaining sound internal controls over all functional aspects of operations.

Management's philosophy and operating style affect the way the entity is managed, including the kinds of business risks accepted. Mangrove places a great deal of importance on working to help ensure that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in the daily operations. Management and specific teams are structured to help ensure the highest level of integrity and efficiency in customer support and servicing.

Organizational values, ethics, and behavior standards are communicated through formal job descriptions and through regular team meetings and staff interactions. Personnel operate under Mangrove's policies and procedures, including confidentiality agreements and security policies. Periodic training is conducted to communicate regulations and the importance of privacy and security. Management is committed to being aware of regulatory and economic changes that affect lines of business and continually monitoring the customer base for trends, changes, and anomalies.

Competence should reflect the knowledge and skills needed to accomplish tasks that define an individual's job. Through consideration of an entity's objectives and the strategies and plans for achievement of those objectives, management must determine how well these tasks need to be accomplished. Management has

identified the competence levels for particular jobs and translated those levels into requisite knowledge and skills.

Integrity and Ethical Values

Maintaining a climate which demands integrity and ethical values is critical to the establishment and maintenance of an effectively controlled organization. The effectiveness of internal controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Mangrove has programs and policies designed to promote and ensure integrity and ethical values in their environment.

Mangrove desires to maintain a safe, pleasant, and cooperative working environment and expects employees to have high standards of performance, integrity, productivity, and professionalism. Mangrove has developed professional conduct policies which set forth policies of particular importance to all employees relating to ethics, values, and conduct. All employees are expected to know, acknowledge, and adhere to these standards, as well as to generally accepted norms of conduct and courtesy at all times. While managers are responsible for understanding, communicating, and enforcing Company policies, this does not override or diminish an employee's individual responsibility to be aware of and adhere to these policies. Violations of these policies or other forms of misconduct may lead to disciplinary or corrective action up to and including dismissal.

Standards of Conduct

The Company has implemented standards of conduct to guide all employee and contractor behavior. Management monitors behavior closely, and exceptions to these standards lead to immediate corrective action as defined by Human Resources (HR) policies and procedures. Additionally, all employees must sign confidentiality agreements prior to employment. Any employee found to have violated Mangrove's ethics policy may be subject to disciplinary action, up to and including termination of employment.

Commitment to Competence

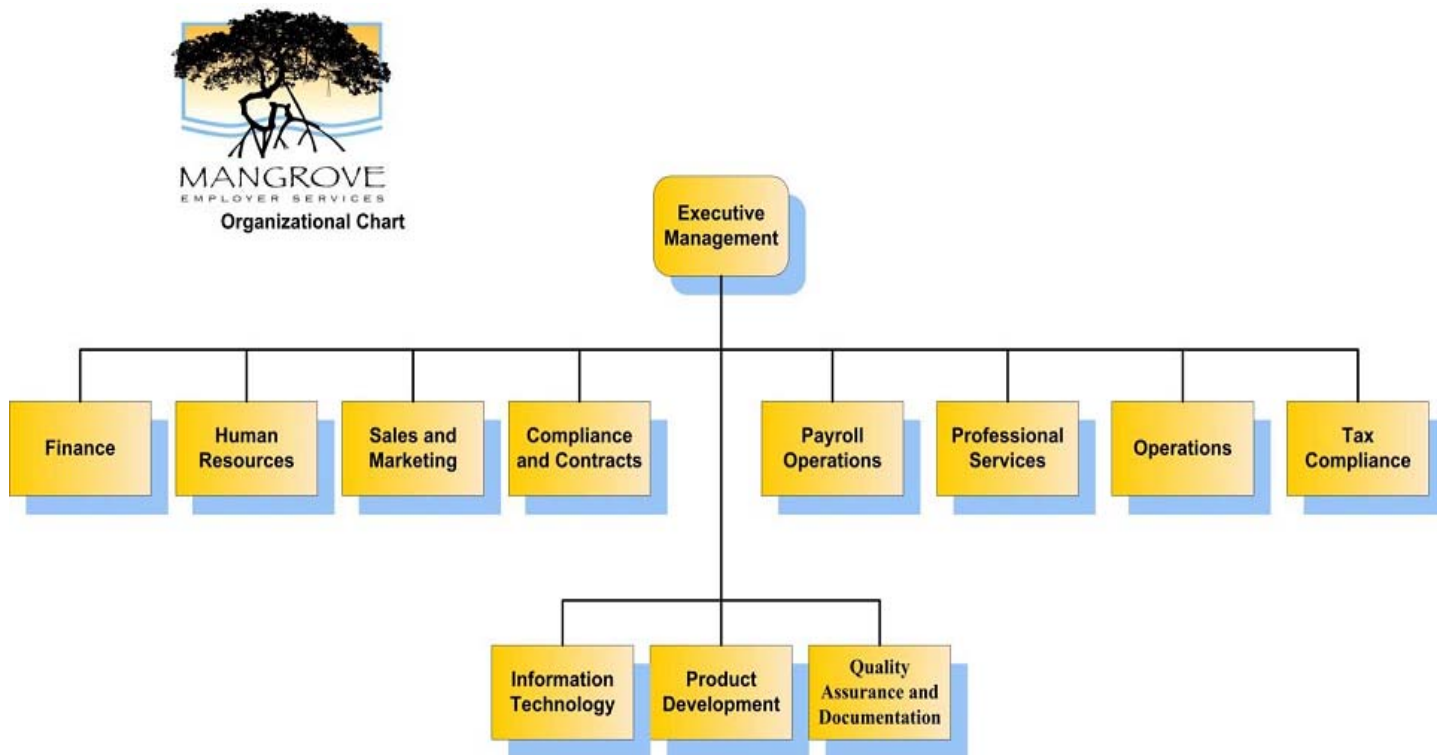
The Company has formal job descriptions which define roles and responsibilities, as well as the experience and background required to perform jobs in a professional and competent fashion. The Company analyzes the knowledge and skills needed to perform job duties and responsibilities and hires for that skill set and job requirement. Management monitors employee and contractor performance and formally evaluates it on a periodic basis to determine that standards are met or exceeded.

Organizational Structure

An entity's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Significant aspects of establishing a relevant organizational structure include defining key areas of authority and responsibility, as well as establishing appropriate lines of reporting. Significant cross-training between management positions and staff positions exists to help ensure smooth operations and maintenance of controls during staff or management absence.

Roles and Responsibilities

The following organization chart depicts the Mangrove corporate structure.



Mangrove is organized into the following departments: Executive Management, Finance, Human Resources, Sales and Marketing, Compliance and Contracts, Payroll Operations, Professional Services, Operations, Tax Compliance, Information Technology, Product Development, Quality Assurance and Documentation.

Assignment of Authority and Responsibility

The control environment is greatly influenced by the extent to which individuals recognize that they will be held accountable. This holds true for everyone who has ultimate responsibility for activities within an entity, including the internal control system. This includes assignment of authority and responsibility for operating activities, establishment of reporting relationships, and authorization protocols. Mangrove management encourages individuals and teams to use initiative in addressing issues and resolving problems. Policies describing appropriate business practices, knowledge and experience of key personnel, and available resources are provided to employees in order to assist them in carrying out their duties.

The Company is led by a team of senior executives that assign authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments. Such assignments commonly relate to achieving corporate objectives, oversight of operating functions, and any compliance with applicable regulatory requirements. Open dialogue and individual initiative is encouraged as a fundamental part of the Company's goal to deliver client service.

Executive Management – This department is responsible for developing and establishing organizational goals, strategic vision, organizational direction, client strategy, client acquisition, market positioning, and company growth.

Finance – This department is responsible for managing accounting functions and preparation of reports and statistics detailing financial results as well as establishing and maintaining accounting practices to ensure accurate and reliable data necessary for business operations is generated and safeguarded. This department oversees accounts receivable, accounts payable, payroll, financial reporting, and budget.

Human Resources – This department is responsible for providing a quality workforce by aiding all departments in the selection and retention of qualified employees as well as providing a safe and comfortable work environment for all company employees. Human Resources is responsible for all personnel functions including:

- Employee hiring procedures that include background and credit checks
- Employee benefits administration
- Payroll auditing, reporting, and processing
- Compliance with external and internal regulatory and policy requirements
- All recordkeeping as it relates to Human Resources
- Creation and interpretation of personnel policies and procedures
- Implementation and ongoing responsibility for employee orientation, education, and employee competency training programs
- Maintenance of a system of employee performance evaluations
- The recruitment process which includes employee qualifications, testing, and selection

Sales and Marketing – This department is responsible for planning, organizing, and implementing sales programs for Mangrove. Sales and Marketing oversees key accounts, coordinates sales budgets, forecasts, and monitors industry product and pricing trends. The marketing coordinator strategizes to meet organizational objectives, implements marketing plan changes, as well as evaluates customer research using customer satisfaction audits, market conditions, and competitor data.

Compliance and Contracts – This department is responsible for advising management of current and developing compliance for future issues/trends and making recommendations concerning compliance with relevant regulatory requirements. Compliance and Contracts is responsible for communicating with clients regarding regulatory issues related to all products Mangrove administers. Other responsibilities include overseeing the preparation of new contracts, renewals, and pricing guidelines.

Payroll Operations – This department is responsible for Mangrove’s Web-Based Payroll Services providing comprehensive payroll processing, human resource management, and self-service solutions.

Professional Services – This department is responsible for the management of all custom work requests that come into Mangrove via email, fax, phone, or the Customer Relationship Management (CRM) tool. This department collaborates with customers to define the scope of each project. Once the scope is defined, an Engagement Letter which assigns all fees to complete the project is presented to the customer. Once the Engagement Letter is executed by the customer, this group manages all efforts to complete the project by the agreed upon deadlines for both parties.

Operations – This department is responsible for all initial customer support, client application customization, integration services, enrollment, education, and training. Operations oversees software implementation, installation, and configuration based on business requirements in the customer’s environment. This includes custom training design, training delivery, project mentoring, technical support, and onsite troubleshooting.

Tax Compliance – This department is responsible for providing control and oversight of all client-related tax filing functions, including but not limited to new client setup and ongoing deposits and filings for quarter and year-end. This department communicates with clients regarding payroll and tax issues. Tax Compliance also communicates with IRS, federal, state, and city agencies regarding client tax issues.

Information Technology – This department is responsible for data center infrastructure support, network security, disaster recovery readiness, client-server applications, cable/fiber installation, desktop support, and helpdesk operations. IT oversees installation of new servers, troubleshoots/repairs all hardware-related issues, and maintains and analyzes all networking equipment. A main function of this group is data center administration which includes design, implementation, expansion, electrical load balancing, and 24x7x365 operational support.

Product Development – This department is responsible for writing original and modifying existing software programs to provide new application functionality and fix inappropriate application behavior. This group documents technical changes. Product Development interacts with senior staff and customers to develop extended knowledge of the software changes requested as well as to test the results of the work performed for conformance to assignment expectations. The development process covers all disciplines of project management, software development, and software quality assurance.

Quality Assurance and Documentation – This department oversees a system of procedures, checks, audits, and corrective actions to ensure that all design, monitoring, performance, research, sampling, and technical reporting activities are of the highest achievable quality. This department also determines whether products or services meet or exceed customer expectations. Mangrove utilizes the Six Sigma methodology approach to measuring transactional effectiveness on a daily basis. The metrics are derived the same day.

Standard Operating Controls

Mangrove management sends guidance to employees regarding expected levels of integrity, ethical behavior, and competence. Such practices relate to hiring, orientation, training, evaluation, counseling, promotion, compensation, and remedial actions.

Mangrove has formal hiring practices that are designed to help ensure that new employees are qualified for their job responsibilities. All applicants pass through an interview process which assesses their qualifications related to the expected responsibility level of the individual. Mangrove conducts preemployment reference checks from information provided on the employment application. Human Resources conducts pre-hire background investigations relating to past employment history, credit history, and criminal activity.

Mangrove invests significant resources in employee development by providing on-the-job training and other learning opportunities. New employees participate in an internal orientation program which acquaints them with the Mangrove organization, its affiliated companies, functions, values, products, and selected policies. Thereafter, development activities include providing more challenging assignments, job rotation, and seminars. Additionally, employees are provided with measurable objectives and are subject to periodic performance reviews to help ensure competence. Managers give each of their employees at least one formal written performance appraisal per year.

Human Resource Policies and Procedures

HR policies and practices are documented in the Associate handbook. The policies and procedures are designed to allow management to recruit, develop, and retain sufficiently competent personnel to achieve the Company's business and control objectives. These objectives include controls and policies for hiring,

training, evaluating, promoting, and compensating employees. All prospective employees complete a comprehensive and detailed employment application, and employment is contingent on rigorous interviewing (and testing if applicable), successful reference checks, and background checks. These screening procedures allow the Company to avoid hiring candidates of poor moral character. Employee retention is a high priority, and management clearly establishes and communicates promotion criteria. Management conducts employee performance evaluations on a systematic basis and relates them to the Company's goals.

Training

Mangrove is committed to training as an essential part of the success of each employee. Training is provided to employees to help them gain the product knowledge and professional skills necessary to maintain the Mangrove standard of service excellence. Ongoing training is conducted in many other areas as well.

Training staff consists of middle and senior management skilled in training techniques, as well as the technical aspects of the subject matter they are instructing.

Audit

Mangrove performs periodic audits of procedures and holds scheduled compliance meetings with staff to review current and new procedures.

Risk Assessment

Mangrove management meets on a regular basis to discuss risks associated with current and future business opportunities. Items addressed in these meetings pertain to the current risk of the daily business along with potential risks associated with new business opportunities. A review of the business plan is also performed in these meetings.

Mangrove has a cross functional risk assessment process that utilizes management, as well as staff, to identify risks that could affect Mangrove's ability to meet its contractual obligations. Risk assessment efforts include analyses of threats, probabilities of occurrence, potential business impacts, and associated mitigation plans. Risk mitigation strategies include prevention and elimination through the implementation of internal controls and transference through commercial general and umbrella policies. Management maintains risk plans and updates them at least annually.

Team leaders are required to identify significant risks related to their areas of responsibility and implement measures to mitigate those risks. The management team, including the Chief Executive Officer, Chief Operating Officer, and the Chief Technology Officer, meets regularly to identify any risks and develop corrective steps to minimize the impact of these risks. The Company employs numerous methods to assess and manage risk including policies, procedures, team structure, recurring meetings, and automated error detection controls. The Company strives to identify and prevent risks at an early stage through policy and procedure adherence in addition to mitigating relevant risks as discovered either through team structure, meetings, or notifications.

Monitoring

Mangrove Executive Management meets on a regular basis to review the operational and financial performance of the Company. Reports are distributed detailing the information discussed.

Management monitors internal controls as part of normal business operations. Mangrove uses a series of management reports and processes to monitor the results of the various business processes. The management team regularly reviews the reports, and all exceptions to normal processing activities are logged, reported, and resolved.

The Company uses software to track user and customer requests which are maintained in a system and tracked until completion. Management performs regular reviews of tasks assigned to their departments. Tasks that are not addressed in a timely manner are manually escalated and resolved.

Information Systems and Communication

Network Overview

All production processing systems are located in the data center in the Tampa facility with components of the backup system located in the Las Vegas, NV location. Mangrove engineers maintain all production systems as well as provide remote administration to satellite offices. The data center houses the Mangrove SaaS operations as well as the majority of the company's corporate operations. In both locations, the offices have primary and redundant data connectivity. All incoming and outgoing traffic passes through a firewall. The firewall is managed by Mangrove engineers.

Mangrove has standardized on Dell and SuperMicro hardware for its server platforms and purchases next-day, onsite support warranties on all of its hardware. All servers have single to quad Central Processing Units (CPUs), dual Network Interface Cards (NICs), and have been configured with a Redundant Array of Independent Disks (RAID) Level 5. Mangrove has implemented a Storage Area Network (SAN) which is configured with RAID 5 and RAID 10. Load balancing is provided by an enterprise system on a fiber backbone. Mangrove owns or leases all of the equipment used in the production environment located at the Mangrove facilities.

Network Communications Overview

Redundant circuits are utilized for the production network through contracted Internet Service Providers (ISP). All patch panels, smart jacks, and network connectivity infrastructure are contained in the secured server room and are grounded. Access to the server room is restricted by the use of proximity locks which are administered by select authorized personnel. The data center remains locked at all times.

Redundant firewalls and network security devices are used to manage and monitor the Internet connections and point-to-point circuits. For its telecommunications infrastructure, Mangrove utilizes an IP telephone system configured to be independent of the data infrastructure to provide enhanced quality of service and security.

Mangrove engineers perform all of the tasks relating to maintaining the Company's production environment. The anti-virus system, operating system patches and upgrades, WAN communications and configuration, data backup, and hardware installation and repairs are all managed by Mangrove's engineers.

Network Perimeter Security

The following are complementary perimeter devices used by Mangrove in its production environment to defend Internet accessible systems:

- Firewalls
- Routers and Switches
- VPN (Virtual Private Network)
- NAT (Network Address Translation)
- DMZ (Demilitarized Zone)

Firewalls

The Company's production operations are protected from the Internet through the use of firewalls. The firewall implementation provides instantaneous failover, application-aware firewall services with identity-based access control, and DoS attack protection. The devices are utilized to provide network access to administrators as well as controlled access to select Web-based applications and network resources. The firewall appliance scans all incoming and outgoing traffic continuously and includes proactive monitoring with traffic reports, policy compliance, and suspicious activity alerts.

Routers and Switches

Routers and switches are essential components of the network and control much of the data center communications. The devices are utilized to divide the network into segments and control traffic flow from one segment to another. Segmenting the network in this manner adds additional levels of security and performance due to the application of traffic flow rules configured on each of the devices. The routers and switches are located in secure, locked rooms at Mangrove's facilities to prevent tampering. Logical access to the devices is protected by unique user names and passwords, and can only be utilized by authorized personnel. Additionally, Mangrove utilizes network monitoring tools to proactively monitor its network for outages.

Virtual Private Network (VPN)

A VPN is used to provide secure, encrypted communication between a network and a remote host or other remote networks over the public Internet. VPNs allow the establishment of an encrypted tunnel that protects the flow of network traffic from eavesdroppers.

A VPN is a private encrypted network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses virtual connections routed through the Internet from the company's private network to the remote site or employee. Virtual Private Networking is used to allow remote users to access Mangrove's internal network. Users authenticate with the VPN concentrator and then authenticate with the Windows domain to gain access to the network resources. Three levels of access rights are implemented based on the type of users accessing the network. Strong VPN authentication and encryption protocols are in use.

Network Address Translation (NAT)

Intruders gain access to networks by scanning for known IP addresses on the Internet. If the addresses are visible from the Internet, the intruder can start probing for the type of machine and vulnerabilities. This can lead to data loss, data corruption, and business interruption.

Mangrove uses the technique of NAT on the main Internet router to provide hidden Internet addresses to internal Mangrove computers. This effectively mitigates the possibility of external sources finding the addresses of internal Mangrove computers.

Demilitarized Zone (DMZ)

Mangrove is segregated into two logical networks, separating the DMZ network from the internal Mangrove network. Network computers exposed to the Internet can subject the entire network to intruder attacks. This can lead to compromised data, viruses, and other types of malicious acts that could damage the company's credibility and operations.

A DMZ has been established to isolate some production systems from the Internet and to restrict their access to/from other areas of the production environment. The DMZ design is reviewed periodically at management meetings.

Headquarters Physical Access

Mangrove owns the entire building located in Tampa, FL which it occupies for the majority of its business divisions. In order to gain access to the internal building, visitors must abide by the Mangrove Physical Security Policy.

Clients, vendors, and all other visitors including former employees:

- Must be escorted by a Mangrove employee at all times while on the premises
- Clients who visit the office for training are issued a proximity card that allows them access to the training room, restrooms, and break room.
- Vendors and contractors are given proximity cards programmed to allow them access only to areas they need to access.
- All proximity cards are returned to the HR Manager and can be reprogrammed or deactivated.

Employee Security access (Proximity Card):

Physical access to application server hardware and all related systems is controlled via a proximity card system plus a security alarm keypad. The proximity card access rights system can only be modified by the HR Manager. The proximity card system is secured in a controlled access area to protect unauthorized access or tampering. Only specific IT staff are granted access to the secured areas housing the aforementioned hardware and systems.

Physical Assets Safeguard

Procedures are in place to ensure the protection of physical assets. Payroll Operations is secured from unauthorized personnel and visitors through a proximity card reader system installed on all entrances. Access cards are issued through the onsite Human Resources Manager. New employees are provided cards programmed according to their responsibilities. Entry access is restricted by hours as well as by area. Users are instructed to report lost cards timely, and these can be cancelled immediately. The security system is monitored 24 hours per day. Logs are maintained of every card attempting clearance in the building.

Data Center

Located in Tampa, FL, Mangrove's data center environment provides security and redundancy for all critical systems with onsite and remote monitoring.

Features of the data center include:

- RAID (Level 5 or 10) on critical file systems
- Redundant disk controllers
- Dual power supplies on critical application servers
- Clustered application servers
- Load balancing
- Patch management
- Data backup and storage
- System monitoring – activity, performance, CPU utilization, and storage
- Environmental monitoring
- UPS power for data center
- Backup generator
- Dedicated, redundant air conditioning units

Environmental Controls

Backup Power

The facility utilizes a redundant source of UPS power. In the event of an electrical failure, the battery-powered electrical supply system provides approximately 30 minutes of power. In the event of extended power outages, a backup generator is located onsite and is dedicated to the data center. An automatic transfer switch controls the power load when switching between commercial and auxiliary power.

Data Center Cooling

The temperature of the facility is controlled by a Computer Room Air Conditioning (CRAC) unit. The CRAC unit has redundancy built in. Additionally, a redundant HVAC system is utilized in the event of a failure to the CRAC unit. The server cabinets in the data center are designed with optimal air flow in mind.

The CRAC unit monitors temperature and humidity. Periodic visual inspections are performed by data center staff to ensure the unit is operating within parameters.

Data Center Fire Detection and Suppression

The CRAC unit onsite has its own detection monitor that produces audible alerts. The local administrators are the main component of the fire prevention system that detects heat, smoke, and alerts without triggering the sprinklers. The sprinkler system in the data center is configured with high temperature heads which activate under a higher temperature than the sprinkler heads in other areas of the facility. As an additional layer of protection, an emergency shut off switch is located near the data center door which is used to cut the power in the event of an emergency. Fire detection and suppression features include:

- Fire alarm with offsite after hours alarm monitoring
- Smoke detector with offsite after hours alarm monitoring
- Handheld Halon fire suppression extinguishers
- Sprinkler system

Data Backup and Restore

Mangrove has implemented various backup methods as part of its production operations. Mangrove has a multi-layered strategy for protecting critical data files to meet business requirements. This strategy includes using hard disc storage, off-site replication, and tape archiving. Specified backup jobs are administered and run using automated backup utilities with alert notifications on success or failure. Tape backup media is rotated on a regular schedule and stored in a protected offsite location.

Off-Site Data Replication

Production database data stores are replicated off-site every three hours. The system has been configured for block-level replication whereby snapshots of changed binary blocks of data are transferred to the Las Vegas location for storage on the remote SAN array. The system has been configured to store the last 16 snapshots providing a comprehensive restore set.

Backup Policy

The backup policy includes computers within Mangrove which are expected to have their data backed up. The IT Manager is responsible for performing regular backups of company data and the production environment. The IT Manager has developed a procedure for testing backups and the ability to restore data from backups on a routine basis.

Data Backed Up

Data to be backed up includes the following information:

- Production data stores
- User data stored on network drives
- System state data
- The registry

Systems to be backed up include but are not limited to:

- Production and backup mainframe applications
- File servers
- Mail servers
- Production Web servers
- Domain controllers
- Test environment servers

Restoration

Customers or staff that need files restored must submit a request to IT. Requests must include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

Computer Operations

The majority of workstation operating system software is Microsoft Windows XP Professional. Microsoft Active Directory has been implemented to provide administrative security boundaries for Mangrove engineers, clients, and staff. All workstations are members of the Mangrove domain and have policies enforced that restrict user rights to authorized business needs.

Hardware, Servers, and Systems Monitoring

Hardware

The Mangrove production network utilizes multiple Dell and SuperMicro servers segregated from the Internet and DMZ by a dedicated firewall. Access to the Dell and SuperMicro servers is controlled via IP-specific firewall rule sets. Mangrove owns all of the equipment utilized in its production environment and has employed fault tolerance on these systems.

Servers

Most servers have redundant power supplies and a RAID 5 or 10 SCSI hard disk array to allow hot swapping of hard drives in the event of a single hard drive failure. Windows operating systems are used on all servers. A SAN is used as the primary source of data storage providing exceptional fault tolerance by using RAID levels 5 and 10. Multiple windows servers are used for database processing and hosting operations.

Systems Monitoring

Mangrove's Information Technology team regularly monitors the customer hosted network for capacity, performance, and hardware failure. Overall database health and capacity planning are also monitored daily to ensure the system will meet the needs of Mangrove's clients. Information Technology monitors security access violations, including server logs and reports.

Monitoring policies and procedures are utilized for addressing issues relating to outages of critical services or other issues needing immediate action. These procedures vary based on the severity level of the problem.

The Mangrove engineers use several monitoring tools to identify and provide alerts to the following conditions:

- A managed system has exceeded a predefined performance or load threshold.
- A managed system has suffered an error condition.
- A managed system has detected a hardware element that is expected to fail in the near future.
- A managed system is no longer in communication with the monitoring infrastructure.
- A managed system has entered a condition previously specified by the Mangrove engineers as operating outside of a threshold.

Software and Hardware Maintenance

All employee workstation computers have a minimum standard hardware and software configuration. Employees are not allowed to install any software on Mangrove-owned computers. All company documents are stored on a file server for nightly backup.

Mangrove IT maintains several replacement computers that can replace workstations in need of repair or maintenance, thereby disrupting the employee's workday as little as possible. A hardware replacement contract is in place to minimize downtime due to component failure.

Virus Protection

Mangrove ensures that all computer devices (including servers, desktops, laptops, etc.) connected to the network have proper virus protection software, current virus definition libraries, and the most recent operating system and security patches installed. Mangrove verifies that all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating. In the event of a virus threat, the antivirus system will attempt to delete or quarantine the infected file. If the virus cannot be deleted or quarantined, the infected machine will be disconnected from the network and cleaned manually. All virus incidents generate an email notification indicating the action taken.

Patch Deployment

Mangrove takes a proactive approach to patch management. Mangrove engineers regularly monitor various message boards and mailing lists where advanced notification of bug and related patches is often disclosed prior to public announcement by the vendor. This allows Mangrove to plan well ahead for upcoming patches.

Mangrove engineers consider each patch carefully and independently to determine if it is necessary to deploy it within the production environment. In many cases, the vulnerability being addressed by the patch has been mitigated through any number of other countermeasures already in place such as firewalls, the intrusion prevention system, or an aspect of their hardening process. In these cases, patches may be deferred until they are included in a future service pack. If Mangrove engineers decide that the patch is necessary and should be deployed, the patch is tested. Once the patch has been thoroughly tested, it is approved for deployment in the production environment.

Due to the redundant nature of the Mangrove environment, it is usually possible for engineers to remove individual processing servers from rotation, patch them, and return them to rotation without ever impacting the availability of the customer's site. Patches to the firewalls can be applied similarly.

Incident Response

The Company has a formal Incident Response Policy whereby responsibilities regarding notification and action taken are clearly defined. Security incidents are handled by various members of IT management and IT engineers. The IT Manager is responsible for keeping management apprised of an incident's status through resolution.

Information Security

At Mangrove, security is critical to the physical network, facility, computer operating systems, and application programs. Each area offers its own set of security issues and risks. An Information Security Policy is necessary to serve statutory goals pertaining to government organizations, healthcare organizations, financial organizations, and other industries. These goals include:

- Ensure continuity of operations
- Protect the safety and integrity of confidential information
- Prevent unauthorized access to confidential information

- Ensure proper use of communications areas
- Assign responsibility for efficient and economical management of confidential records
- Protect company data

Mangrove implements a comprehensive security program that offers a high level of protection commensurate with the value of the assets. The information security program provides reasonable protection against unauthorized access, disclosure, modification, or destruction, as well as to assure the availability, integrity, usability, authenticity, and confidentiality of information. This applies to all systems that manage or store data.

Confidentiality and Privacy

All members of the Company are obligated to respect and in many cases to protect confidential data. There are, however, technical and legal limitations on the ability to protect confidentiality. For legal purposes, electronic communications are no different from paper documents. Electronic communications are, however, more likely to leave a trail of inadvertent copies and more likely to be seen in the course of routine maintenance of computer systems.

Mangrove's policies permit limited personal use of computer resources. The company has the ability to monitor the content of personal Web pages, email, or other online communications. The company reserves the right to examine computer records or monitor activities of individual computer users (a) to protect the integrity or security of the computing resources or protect the company from liability, (b) to investigate unusual or excessive activity, (c) to investigate apparent violations of law or company policy, and (d) as otherwise required by law or exigent circumstances. In limited circumstances, the company may be legally compelled to disclose information relating to business or personal use of the computer network to governmental authorities or in the context of litigation and other third parties.

Access

No one may access confidential records unless specifically authorized to do so. Even authorized individuals may use confidential records only for authorized purposes. The company expects a respect of privacy of others and their accounts, no access to data of others without permission, and no use of another's password or access of files under false identity.

Technology assets are housed in appropriately secure physical locations. Technology assets include servers and personal computers that contain systems with controlled access and network components (cabling, electronics, etc.). Passwords help protect against misuse by seeking to restrict use of network systems to authorized users. Each authorized user (specific individual) is assigned a unique password that is to be protected by that individual and not shared with others, is difficult to crack, is changed on a regular basis, and is deleted when no longer authorized.

Mangrove's Information Security program defines access rights and privileges and protects assets and data from loss or inappropriate disclosure by specifying acceptable use guidelines for users, operations staff, and management. The Information Security program provides guidelines for external connections, for data communications, for connecting devices to a network, and for adding new software to systems. As part of the program, the responsibility and accountability for its implementation has been established.

Accountability

Staff are responsible for ensuring that others do not use their system privileges. In particular, users must take great care in protecting their user names and passwords from eavesdropping or careless misplacement.

Passwords are never to be loaned. Individual users will be held responsible for any security violations associated with their user names.

Management is responsible for reviewing audit logs and identifying potential security violations. The IT Manager is responsible for establishing the security and access control mechanisms (such as user names, passwords, logging, etc.), and may be held accountable for any security breaches that arise from improper configuration of these mechanisms.

Authentication

Authentication, data encryption, or point-to-point communication has been implemented for all systems that send or receive sensitive data or when it is critical that both parties know with whom they are communicating. The decision of whether or not to encrypt data should be made by the IT Manager.

Availability

Mission critical systems are expected to be available at all times. Backup of data will be well documented and tested. Backups of mission critical data must be maintained to guard against the impact of disasters.

Information takes many forms. It may be stored on computers, transmitted across networks, printed, written, and spoken in conversations. Information technology systems are vital assets to all industries. These information assets are essential to the daily operation of these institutions and agencies and may affect each organization or entity that provides or relies on their services.

Systems (hardware and software) designed primarily to store confidential records (such as financial and customer information) require enhanced security protections and are controlled (strategic) systems to which access is closely monitored. Networks provide connection to records, information, and other networks and require security protections. The use of Mangrove's assets in any manner other than for the purpose for which they were intended represents a misallocation of resources and possibly a violation of law.

Responsibility for guaranteeing appropriate security for data, systems, and networks is assigned to the IT Manager. The IT Manager responsible for designing, implementing, and maintaining security protection, but senior management retains responsibility for ensuring compliance with this policy. In addition to management, the individual user is responsible for the information technology equipment and resources under his or her control.

Information systems policies and procedures are outlined in Company policy documentation. These policies document acceptable use of systems (including email and Internet access) and data (including protection from viruses and data privacy). Monitoring procedures are followed to review data and information produced by security controls for the purpose of detecting violations of the security policy. Recovery procedures are followed to restore security following detection of failures.

Logical Access

Logical access to Mangrove's systems, applications, and data is limited to properly authorized individuals, and user rights are kept to a minimum needed to perform job-related functions. Mangrove engineers administer network and server passwords. The IT Manager is responsible for maintaining data integrity and for determining end-user access rights. All access granted to systems, applications, and data is password protected using role-based security. Auditing is implemented on all systems, where possible, to track a variety of events including but not limited to security access violations, application, and database access.

Network Password Security

Local network password rules are established according to the Mangrove Security Policy. The following parameters have been systematically configured requiring passwords to be a minimum length of characters and composed of a combination of alpha and numeric characters to comply with complex password requirements as established by management and implemented by the Windows operating system. Individual user accounts for each customer are setup with a unique user ID.

User Administration

Mangrove's policies require users to be specifically authorized to access information and system resources. Mangrove administrators are responsible for security administration functions including assigning/deleting administrative users to Mangrove resources. Upon termination from Mangrove, employee access is removed from Active Directory and all associated Mangrove sites and pages.

New Hires

An approved request form is required for a new user or a change to existing user access. The IT Manager is the security administrator and is responsible for ensuring adherence to the IT Policy which addresses logical access control procedures. Unique user IDs and passwords are assigned to each individual user at the network level.

Network and application access is controlled by the IT Manager and engineers. Mangrove company servers and email services cannot be accessed without appropriate network access. The IT Manager ensures that proper levels of access within applications are assigned and maintained.

Terminated/Transferred Users

When an employee resigns or is terminated from Mangrove, the supervisor is responsible for informing IT to restrict the employee's access. IT disables a user's access rights from each applicable system upon first communication (verbal or written) of a resignation or termination.

At the time of termination, a checklist is completed for the terminating employee. Disabling the network user account is integral to the exit process and is a staged process designed to keep email accounts open to retain data while disabling the terminated user's access immediately.

The IT Manager terminates the employee in all systems and double checks access lists to ensure integrity. After 60 days, the terminated employee's email account is removed from the Exchange server by IT. After 90 days, the user identity is deleted from the network. This process provides necessary security while minimizing any disruption in the ability of client companies contacting Mangrove during the termination transition.

Account Review

System security access levels are reviewed semi-annually by the IT Manager, delegate, and supervisors to ensure individual access rights are appropriate based on job responsibilities. As responsibilities change for a user, the associated security role is also changed to reflect the user's new job responsibilities.

Database Security

The database software maintains a client database which is only accessible through the software application and is protected from unauthorized access. User names in the database are created by the IT department. Passwords are changed periodically as required by management. Management determines the level of system access for each individual based on assigned responsibilities.

IT controls access to the Mangrove database as follows:

- For employee access, IT grants a level of access pursuant to a request from a department manager.
- For client employee access, the IT Manager grants a level of access to each employee approved for such access by the client. In addition to the above controls, the IT Manager oversees the development of Web site interfaces, databases, and reports customized to client specifications.

Data Communications

Secured Web Pages and Authentication Certificates

Mangrove uses Secure Sockets Layer (SSL) over Hyper Text Transfer Protocol (HTTP) for its client hosted connections. This ensures authentication and encrypted communications for security-sensitive information such as user log-in and account information. While not a separate protocol, HTTPS refers to the combination of a normal HTTP interaction over an encrypted Secure SSL or Transport Layer Security (TLS) transport mechanism and indicates that HTTP is to be used, but with a different default Transmission Control Protocol (TCP) port and an additional encryption/authentication layer between the HTTP and TCP.

Disaster Recovery Preparedness

The Company maintains a formal Disaster Recovery Plan (DRP) in the event of an emergency or natural disaster. The company's DRP covers the following critical functions in the event of a business interruption:

- Crisis Team Membership
- Plan activation
- Designation and activation of the disaster recovery site
- Departmental action items
- Notification and coordination with key vendors and customers
- Recovery operations
- Training and awareness

The DRP is intended to be a living document which is reviewed and updated annually. The Mangrove management team ensures that the plan undergoes a formal review to confirm the incorporation of all changes since the prior review. These revisions will be distributed to all authorized personnel.

Testing the Disaster Recovery Plan is an essential element of preparedness. Partial tests of individual components and recovery plans are carried out on a regular basis.

Application Development and Change Management

Software Development Life Cycle (SDLC)

The SDLC that Mangrove uses for larger projects is most closely aligned with the ‘Agile’ approach. A project is divided into time boxes or fixed periods in which development is done. These time boxes are called iterations. The iteration length is usually fixed between two to eight weeks, although small projects can have an iteration length in days or even hours. Testers and architects also create tasks as part of the iteration plan. These roles are involved in ensuring that the solution is well architected and tested. They work in conjunction with the developers, business analysts, and project managers to ensure the defined process meets initial requirements.

Finally, there are reviews of system functionality after key iterations with the customer. There are many vehicles for these reviews from actual working systems to storyboards with screen captures in cases where it is impossible to simulate the deployment environment in the area where the review is held.

Quality Assurance (QA)

The Mangrove quality team consists of a technical team of developers and analysts that provide a range of services that support a development project. In order to provide high quality services, the IT team must adhere to processes, procedures, and standards. QA is a process used to monitor and evaluate the adherence to processes, procedures, and standards to determine software quality. It involves reviewing and auditing the products and activities to verify that they comply with the applicable procedures and standards, and assuring the appropriate visibility for the results of the reviews and audits.

All development activity is required to include QA activities as an integral part of processes used for the development and delivery of software. Quality Assurance will work to foster constructive communication, provide feedback to detect and prevent development problems, control risks, discuss alternative solutions, and ensure quality is built into all application development.

The QA function will be a separate entity and will maintain independence from project management by possessing a direct reporting function to senior management. This structure will protect the QA team’s independence and objectivity.

Documentation

All required documents for a project will follow the appropriate standards concerning content and format. When industry standards are not available, the QA team, along with input from the project team, must develop the standards or adapt documents developed by other groups to use as standards within the project. The information used from other group’s documents will be used to ensure compatibility between other networks existing within the organization. Standards will be identified and followed for all required project documentation.

The development activities are to be implemented according to customer requirements. The required documentation is necessary to ensure development activities are planned, monitored, and controlled and will be used to verify the adequacy of the actual processes and procedures used to develop and/or deliver software.

Audit Process

The QA team, along with Senior Management, is responsible for conducting product, service, and process audits. The purpose of these audits is to identify deviations in process performance, identify noncompliance items that cannot be resolved at the technical support or project management level, to validate process improvement/corrective action achievements, and to provide relevant reports to all management levels.

A product audit is an examination of work products to assess compliance with specifications, standards, customer requirements, or other criteria. Product audits are used to verify that the product was evaluated before it was delivered to the customer, that it was evaluated against applicable standards, procedures, or other requirements, that deviations are identified, documented, and tracked to closure, and to verify corrections.

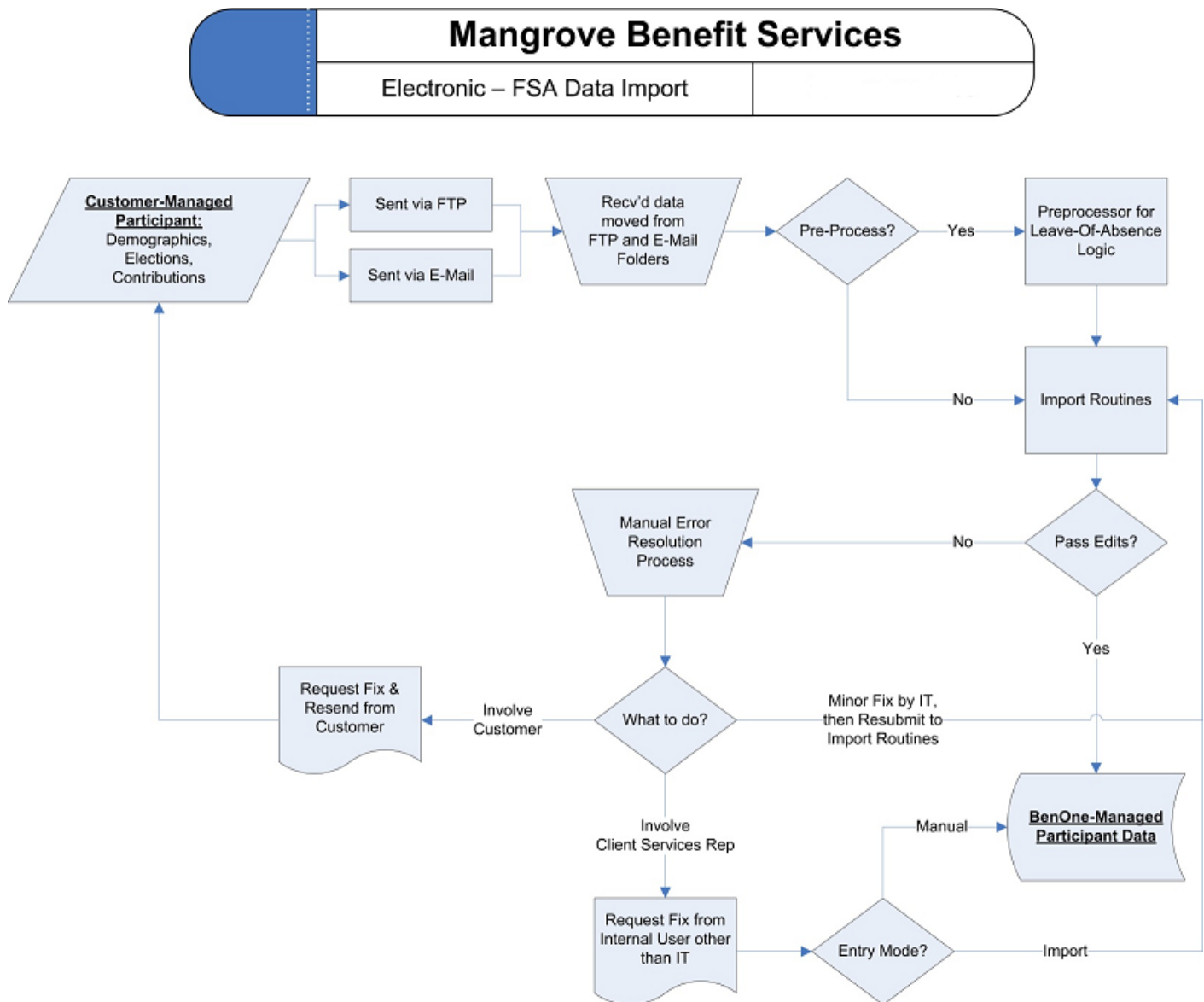
A process audit is a systematic and independent examination to determine whether quality activities and related results comply with planned arrangements, and whether these arrangements are implemented effectively and are suitable to achieve objectives.

Noncompliance Reporting Procedures

- Problems are resolved with the direct producer or the appropriate task leader, when possible.
- Problems that cannot be resolved with the technical team or task leader are elevated to the project manager.
- Problems that have been referred to the project manager are reviewed weekly until they are resolved. Items that cannot be resolved by the project manager within six weeks are elevated to the technical monitor for resolution.

Control Activities

FSA Data Import Process



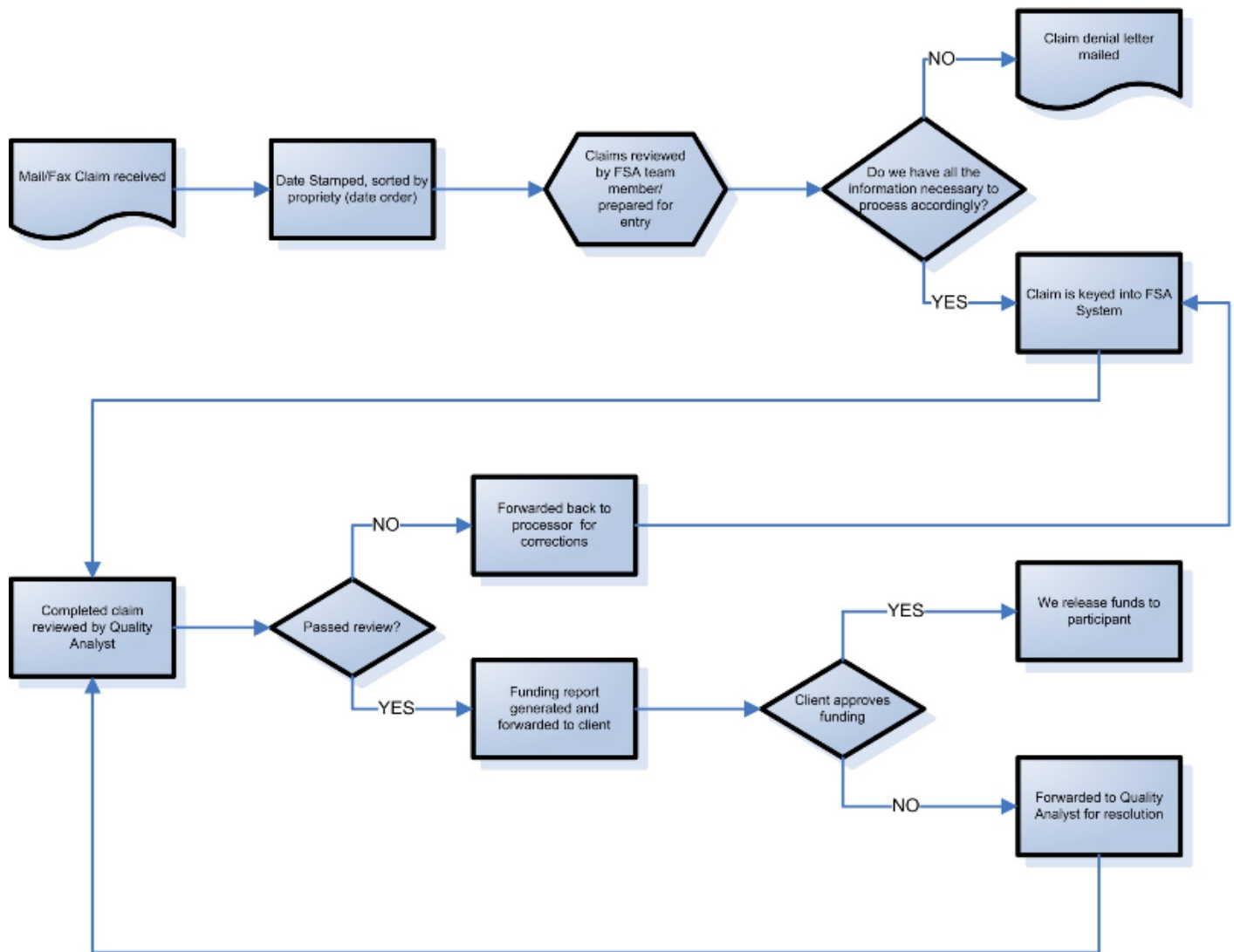
Participant elections are received via paper, fax, or by an electronic file. Participant contributions are received and posted based on the client's choice of the following methods:

1. The auto posting method, which is to post contributions each pay period based on participant elections received when enrolled, or
2. The actual posting method, which is for the client to send Mangrove an electronic file with the actual payroll deductions withheld for importing and posting to the FSA system.

All electronic files received are processed by a Business Analyst.

Mangrove Benefit Services

FSA Process Flow



FSA Claim Reimbursement Process

All Flexible Spending Account claims are received via fax, email, electronic file, online, or mail. The File Clerk sorts and date stamps the claims. If the claim form is submitted online, the participant may scan and submit receipts electronically. The system then automatically attaches the scanned receipts to the claim form. The participant also has the option to fax in the receipts, and then a manual process is used to attach receipts received by fax to the claim form submitted online.

All claims received are filed in a folder labeled 'waiting to be processed' and sorted by client in order of the scheduled reimbursement day.

All FSA claims are processed daily. The Claim Processor will pull the claims to review for required information per IRS regulations which includes:

- Completed and signed claim form
- Description of services provided
- Provider name
- Claimant name
- Date of service provided
- Attached receipts from third-party provider

The Claim Processor also judges the claims to verify that:

- The service or product provided is eligible for reimbursement
- The date of service falls within the participant's covered period

If the claim submitted is complete, the eligible and non-eligible claims are keyed into the FSA system. After they are entered, the claim forms are placed in an audit folder. If the claim was entered as denied, the participant will be sent a denial letter. Denial letters are generated every Friday and mailed to participants. The FSA system automatically catches ineligible claims based on date of service, plan year, and end of run out period.

The FSA system searches for duplicate claims with the same:

- Date of service
- Provider name
- Dollar amount

If any of the above is the same, it is flagged as a possible duplicate. The Claims Processor will need to verify whether it is a duplicate claim or not.

Claims marked as denied by the FSA system or the Claims Processor are flagged for review and then all claims are audited by a Quality Analyst. After the Quality Analyst reviews claims entered, a check register showing the participant name, type of FSA, and amount to be reimbursed is sent to the client to request that they fund their bank account accordingly. A separate check register for direct deposit is sent to clients for approval. Once a client approves the check register and their account is funded, they will authorize payment to participants via email to be made via check or via Electronic Funds Transfer (EFT).

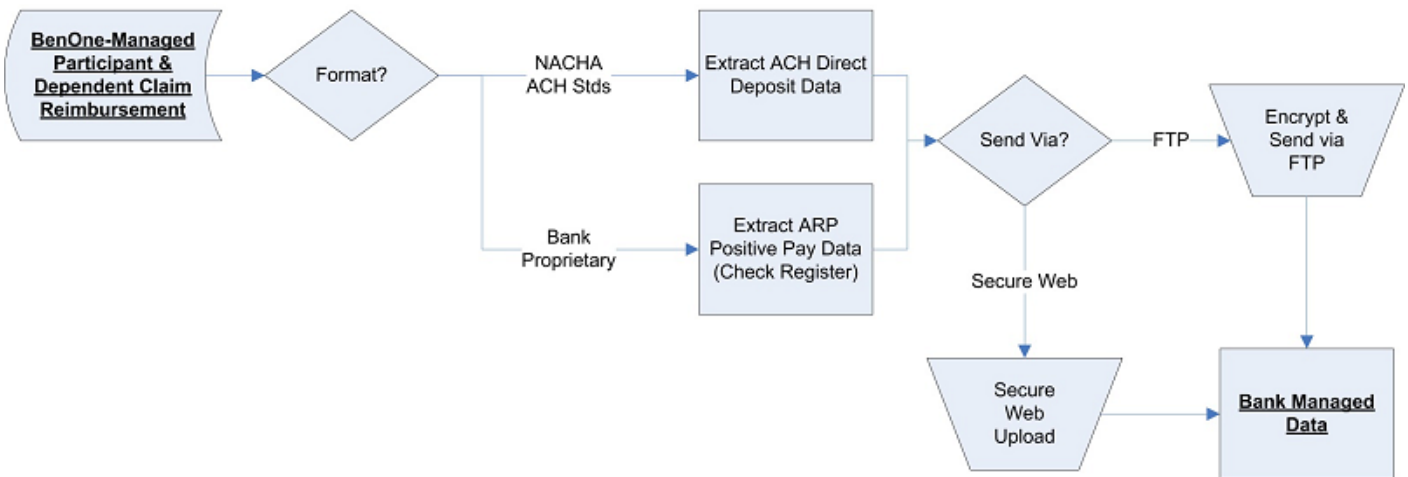
Participants also have access to their FSA funds via the Benny Card, an employee benefit debit card. Participants swipe the debit card at their medical care provider's office at the time of visit, at the pharmacy, or other approved health care and dependent care merchants, and the claims are substantiated automatically per the auto substantiation parameters set up for the employer group per IRS regulations. The funds are then withdrawn from the participant FSA account to reimburse the employer for the debit card expense. All debit card claims are substantiated by Evolution Benefits, the provider of the Benny Card and administrator of the Benny Central processing application. If the debit card swipe cannot be auto substantiated, Evolution Benefits notifies Mangrove, and they in turn notify the participant that they must submit copies of their receipts or additional information for validation.

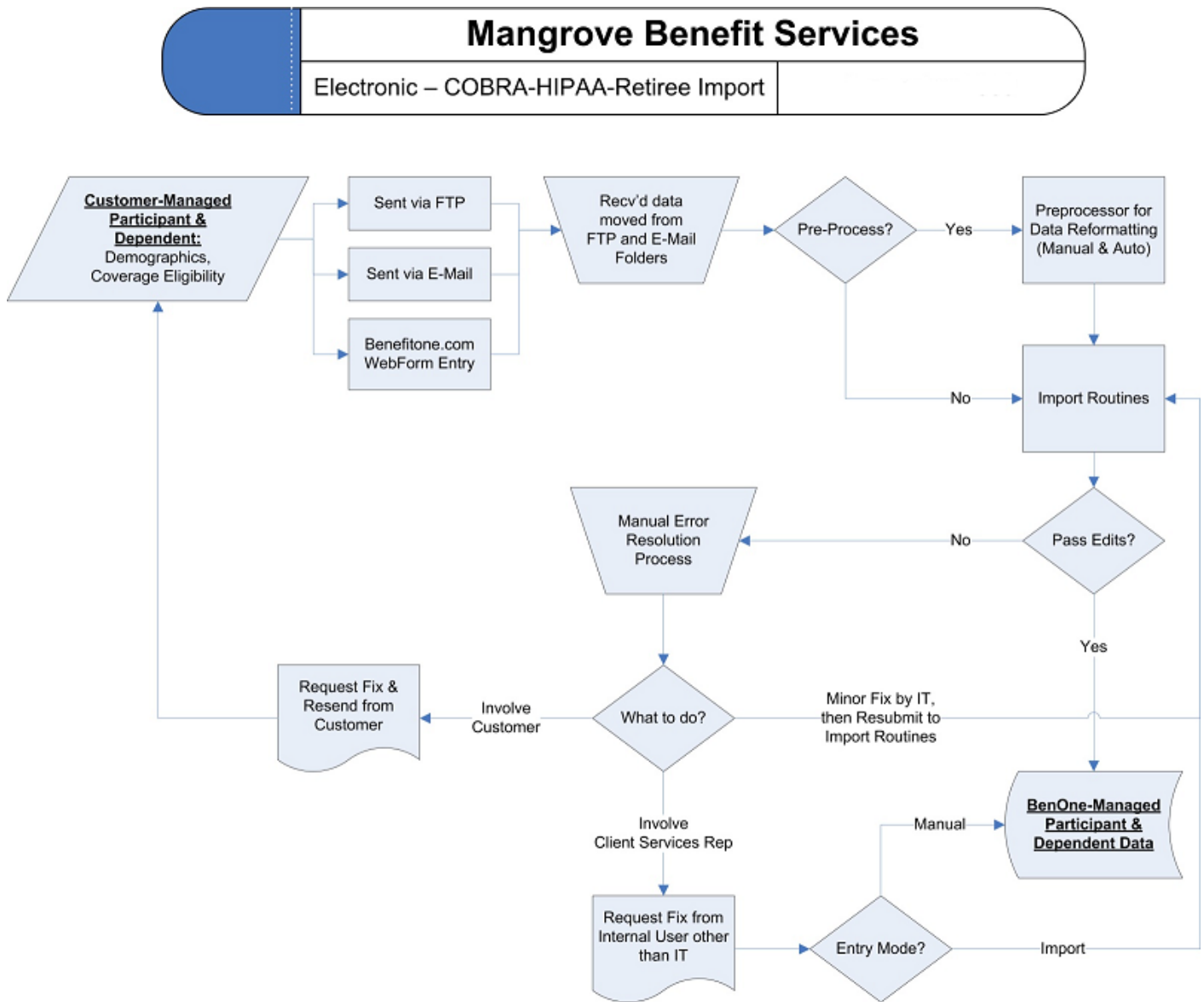
Evolution Benefits receives and processes any electronic Explanation of Benefits (EOB) rollover files from insurance carriers and sends an FSA Claim import file to Mangrove. Participants can view their contributions, claims, and reimbursements online.

All participant funds are drawn on the client’s bank account. Checks are printed by the Finance department with an authorized client electronic signature and mailed to participants.

Direct deposit is handled by Finance through Intercept Organization, a third-party processor of electronic funds transfers (EFT) through the Automated Clearing House (ACH). Access to the Intercept system is limited to Finance.

FSA Claim Reimbursement



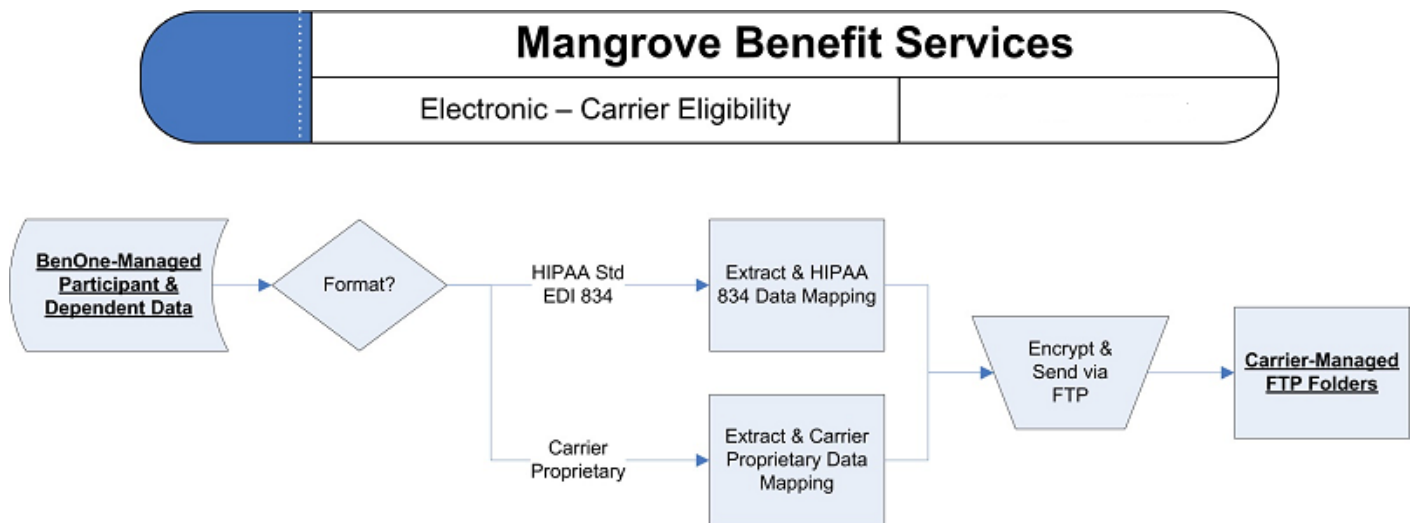


Mangrove provides a full range of COBRA administrative services from tracking eligible employees and sending the initial notices upon the employee’s election of covered benefits to processing Qualified Events and notifying carriers of reinstatements, changes, and terminations of COBRA continuation coverage.

Qualifying Events can be received by Mangrove via fax, email, mail, online, or by electronic file. Electronic files are imported by IT. The Processing Unit enters all COBRA Qualifying Events received by paper. Once entered, the COBRA system automatically generates the required notices which are run every night.

Every night, an automated process is run to process all adds, changes, and deletes which require COBRA notices. The mail room checks this process every morning, and prints, collates, and mails all COBRA notices. The Processing Unit enters elections of COBRA continuation coverage. The Processing Unit then matches all COBRA election forms received and entered to the carrier reinstatement notice to verify that all elections are entered and sent to the carrier.

Carrier Eligibility Process



IT generates and sends via Secure FTP all carrier electronic files for reinstatement, adds, changes, and termination of COBRA continuation coverage.

Finance receives all COBRA premium payments. All checks are mailed to a post office box and picked up daily by Finance. Checks are entered manually by Finance and scanned and electronically deposited into the COBRA Group Agent Account daily. Payments accompanied by a payment coupon ensure the posting of premiums to the correct participant. If no coupon is attached to the check, there are processes in place to verify the identity of the participant for whom the payment was received.

Participants can also make COBRA premium payments via ACH. Mangrove uses ACH Direct services to collect ACH payments of COBRA premiums. Each participant completes an ACH collect authorization form. ACH Direct wires premium payments collected directly to the COBRA Group Agent account daily.

Participants can also make COBRA premium payments with online bill pay, where their bank will send a check on their behalf to Mangrove. Finance manually enters and scans and electronically deposits these payments into the COBRA Group Agent Account daily.

Exceptions for being able to post premiums, e.g. payment exceeds money due, payment cannot be applied, etc. are handled by Operations. Once resolved, Finance posts the premium payment.

Upon termination of COBRA, the participant is mailed a termination notice with reason for termination of COBRA continuation coverage and a HIPAA certificate of credible coverage. The Insurance Carrier is also sent a termination notice to cancel coverage.

COBRA Premium Payments to Employers or Insurance Carriers are printed and mailed by Finance. A Payment Detail report is sent along with payment which details the total money received, deposited, and distributed per participant. Finance also processes refund payments to COBRA participants.

The COBRA Group Agent Account is reconciled monthly. A monthly premium distribution reconciliation of total monies received and total monies distributed is performed by Finance.

Retiree Billing Processing

Retiree Billing parameters are determined by the client. A client specification sheet is collected that outlines the client's requirements.

Upon receipt of election of retiree benefits, the processing unit enters the election, and retirees are sent coupons for premium payments due. The processing unit will notify the insurance carrier of elections, adds, changes, and terminations to retiree coverage. Retiree billing premium payments are received, posted, then scanned and electronically deposited by Finance.

Payroll Processing

The Payroll Processor ensures jobs are scheduled and processed in accordance with established procedures. Activity reports are printed for the next week every Friday and distributed to all employees. This document provides the Processors with a checklist to utilize to ensure all scheduled payrolls and activities are processed and completed according to the schedule.

Payroll data is received by clients in three ways:

- Time Clock Import
- Hand Keyed by Processor
- Customer Online Data Entry

Processors review the received data to ensure it is received from authorized sources.

Time Clock Import – Clients notify the Processors that the file is ready to be imported. The import file log is checked for errors. If errors exist, the Processor contacts the client to have them corrected. Once the payroll is processed, the client is contacted to review. If no changes are required, the client gives permission to close and post the payroll. No payroll is closed without approval from the client.

Manual Input – Clients fax or email their payroll to Mangrove. The Processor will confirm the sending fax number with the fax number of record. The Processor will contact the client if the Processor questions the source or validity of the information provided. If a change in client contact occurs, client management must provide written approval of the new contact and, if needed, specify the security limitations or access for the new contact. This allows for the proper flow of information between the Processors and clients. Processors input the payroll data received from fax or email by the clients and check the data entry against what was sent by the client. Once payroll is completed, the client is contacted to review. If no changes are required, the client gives permission to close and post the payroll. No payroll is closed without approval from the client.

Client-entered Payroll – Clients enter their payroll and notify the Processor that their payroll is ready for review. The Processor reviews the payroll for errors. If there are none, the client closes and posts the payroll. The print flags are set to either allow the client to print the checks or when the payroll is closed for the Processor to print, package, and ship the checks. Mangrove does not verify the validity or the accuracy of the payroll data. Mangrove only processes the data as entered by the client.

All payroll funds are drawn on the client's bank account. Clients are sent a check register, and all accounts are funded by client via wire transfer two days prior to pay day to ensure that the funds are present and clear. Checks are printed and mailed by Payroll Operations. Once payroll is complete, it is marked off the activity sheet and sent to shipping. Packages are then prepared for shipment and placed out for pickup.

ACH Processing

Automated Clearing House (ACH) files are created at the end of each day after all payroll processing is complete. Direct deposit is handled by Finance through Intercept Organization, a third-party processor of electronic funds transfers (EFT) through the ACH. Access to the Intercept system is limited to Finance.

The ACH files will collect and disburse billing, taxes, direct deposit, and trust account funds resulting from payroll processes. Procedures are in place for the creation, transmission, and verification of ACH files. Mangrove contracts with Intercept Organization to perform the warehousing and transmission of ACH entries subject to the National Automated Clearing House Association (NACHA) rules.

Direct deposit is processed two days prior to payday. The file is transmitted to Intercept with two parts: (1) funding from the customer to Intercept, and (2) one day later funding from Intercept to the Individual Employees.

Tax Filing

Mangrove has a full-service Tax Compliance department that generates agency-approved federal, state, and local tax returns and payments. Procedures have been established to ensure that the appropriate tax filings are complete, accurate, and timely. Payments for federal, state, and local taxes are remitted electronically for all agencies supporting electronic funds transfer. The staff also routinely balances the daily tax liabilities for the companies that were processed. Checks and balances are in place to ensure that all filings are completed for all clients.

Tax impound funds are held in escrow in the tax trust account. The tax trust account is maintained and reconciled by Finance. For clients that choose to be full service tax clients, funds are escrowed for taxes withheld and employer taxes collected each pay period are remitted as they become due. Several methods are used to verify and reconcile the tax trust account. Transactions are downloaded daily from the bank, and the reconciliation is completed. Finance compares the monthly tax deposits made on behalf of clients to the tax impounds during the month to confirm the correct amounts from each client were collected and paid.

Checklists are prepared by tax code and the client to ensure that all monthly, quarterly, and annual tax returns are filed, even if no payments were made. Quarterly returns are processed after rigorous data integrity testing and balancing procedures are completed. Annual processing and verification procedures produce annual tax reports as required by government agencies at the federal, state, and local level. These reports include employer and employee forms W-2, employer forms W-3, 940, and 941. In addition, files are generated that contain employer W-2 and W-3 information for transmission to the Social Security Administration for subsequent processing.

Communication

Mangrove uses a variety of methods for communication to ensure that significant events and issues are conveyed in a timely manner and that staff understand their role and responsibility over service and controls. These methods include the following: new hire training, ongoing training, policy and process updates, periodic departmental meetings summarizing events and changes, use of email and paging to communicate time sensitive information, instant messaging, and the documentation and storage of historical data in internal repositories for business and support activities. The Company maintains systems that manage the flow of information and facilitate communication with its customers.

Information Flow from Senior Management to Operations Staff

Mangrove has implemented various methods of communication to help ensure that employees understand their individual roles and responsibilities over processing and controls and communicate significant events in a timely manner. Employee manuals are provided upon hire which communicates all relevant policies and procedures concerning employee conduct. Security of the physical premises and logical security of systems is reinforced by training and through awareness programs. The communication system between senior management and operations staff includes the use of the office email system, written memos when appropriate, and weekly meetings. Periodic department meetings between each manager and their staff are held to discuss new Company policies and procedures and other business issues. Staff and training meetings are utilized to inform staff of new policy and technology updates. Communication is encouraged at all levels to promote the operating efficiency of Mangrove.

Control Objectives and Related Controls

Mangrove's control objectives and related control activities are included in Section III of this report to eliminate the redundancy that would result from listing them here in Section II and repeating them in Section III. Although the control objectives and related control activities are included in Section III, they are, nevertheless, an integral part of Mangrove's description of controls.

User Control Considerations

The Company's applications are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report.

This section describes additional controls that should be in operation at user organizations to complement the controls at the Company. User auditors should consider whether the following controls have been placed in operation at the user organizations:

- Client review and approval is required as outlined in client service agreements for payroll to be processed.
- Controls to provide reasonable assurance that changes to processing options (parameters) are appropriately authorized, approved, and implemented.
- Controls to provide reasonable assurance those transactions are appropriately authorized, complete, and accurate.
- Controls to provide reasonable assurance that erroneous input data are corrected and resubmitted.
- Controls to provide reasonable assurance that output reports are reviewed by appropriate individuals for completeness and accuracy.
- Controls to inform Mangrove of any regulatory issues that may affect the services provided by Mangrove.
- Controls to understand and comply with their contractual obligations with Mangrove,
- Controls to notify Mangrove when changes are made to technical, billing, or administrative contact information in a timely manner.
- Controls to comply with the operating instructions of Mangrove's products and applications.
- Controls for the supervision, management, and control of the use of Mangrove applications by its personnel.
- Controls for system sign-on controls and procedures for the selection and printing of available reports at their respective locations.

- Controls for implementing formal security controls that include, but are not limited to, password creation and maintenance, review of user profiles, terminal timeouts, limited sign-on attempts, and reviewing security reports on a periodic basis.
- Controls to ensure the confidentiality of any user IDs and passwords assigned.
- Controls to immediately notify Mangrove of any actual or suspected information security breaches, including compromised user accounts.
- Controls to maintain their own systems of recordkeeping unless this service has been contracted from Mangrove.
- Controls to verify that any changes to application security requested by the user organization and performed by Mangrove personnel were accurately performed.
- Controls to dictate the use of encryption.
- Controls for approving the telecommunications infrastructure between itself and Mangrove.
- Controls for monitoring activity on accounts belonging to employees and directors of the user organizations and Mangrove employees.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Processing of transactions for clients by Mangrove covers only a portion of the overall internal control structure of each client. The Mangrove products and services were not designed to be the only control component in the internal control environment. Additional control procedures are required to be implemented at the client level. It is not feasible for all of the control objectives relating to the processing of transactions to be completely achieved by Mangrove. Therefore, each client's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

III. INFORMATION PROVIDED BY SAS 70 CPA

CONTROL OBJECTIVES, RELATED CONTROLS, AND TESTS OF OPERATING EFFECTIVENESS

Control Objective 1 – Organization and Administration

CO1- Controls provide reasonable assurance that management provides oversight, segregation of duties, and guides consistent implementation of security practices.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C1.1	Mangrove has a Security Policy and procedures manual that describes the Mangrove security posture and practices.	Inspected the current Information Security Policy to determine that the policy described the Mangrove security posture and practices.	No Relevant Exceptions Noted.
C1.2	Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel and are updated on a periodic basis.	Inspected the organizational chart to determine that documentation was in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel and was updated on a periodic basis.	No Relevant Exceptions Noted.
C1.3	The roles and responsibilities of the Mangrove staff providing information technology services are segregated into separate and distinct positions within the organization.	Reviewed the organization chart to determine that the information technology services roles and responsibilities were clearly defined and followed. Conducted corroborative inquiry of management to determine that Mangrove staff providing information technology services were segregated into separate and distinct positions within the organization.	No Relevant Exceptions Noted.
C1.4	Management's philosophy and operating style is documented and communicated to employees via the associate handbook.	Inspected the associate handbook to determine that management's philosophy and operating style were documented and communicated to employees.	No Relevant Exceptions Noted.

Control Objective 1 - Organization and Administration (Continued)

CO1- Controls provide reasonable assurance that management provides oversight, segregation of duties, and guides consistent implementation of security practices.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C1.5	Organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.	Inspected organizational policy statements and codes of conduct to determine that organizational policies communicated entity values and behavioral standards to personnel.	No Relevant Exceptions Noted.
C1.6	Corporate policies are reviewed annually, updated, and approved by management to remain current.	Inspected the policy review schedule to determine that corporate policies had been reviewed, updated, and approved by management within the previous twelve months.	No Relevant Exceptions Noted.
C1.7	Management communicates individual staff responsibilities through formal job descriptions.	Inspected a sample of job descriptions to determine that management communicated individual staff responsibilities through formal job descriptions.	No Relevant Exceptions Noted.
C1.8	Management maintains insurance liability policies to mitigate losses and transfer certain identified risks.	Inspected the current insurance liability policies to determine that management maintained insurance liability policies to mitigate losses and transfer certain identified risks.	No Relevant Exceptions Noted.
C1.9	Management meetings are held on a regular basis to discuss operational issues.	Conducted corroborative inquiry of management to determine that management meetings were held on a regular basis to discuss operational issues.	No Relevant Exceptions Noted.

Control Objective 2 – Human Resources Security

CO2 – Control activities provide reasonable assurance to ensure that employees, contractors, understand their responsibilities, are suitable for the roles they are considered for, and exit the organization or change employment in an orderly manner.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C2.1	Management has documented its human resources policies and practices related to hiring, orientation, evaluating, counseling, promoting, compensating, and remedial actions.	Inspected Mangrove human resources policies to determine that management documented its human resource policies and practices related to hiring, orientation, evaluating, counseling, promoting, compensating, and remedial actions.	No Relevant Exceptions Noted.
C2.2	Management assesses each job candidate to ascertain whether the candidate possesses the requisite level of competence to fill the job position.	Conducted inquiry of HR Manager to determine that management assessed each job candidate to ascertain whether or not the candidate possessed the requisite level of competence to fill the position.	No Relevant Exceptions Noted.
C2.3	Management ensures employees are subjected to a background check during the hiring process. Employees are required to sign a background check release authorizing the checks.	Inspected a sample of signed background release authorization forms for employees hired during the period under review to determine that each employee authorized a background check during the hiring process.	No Relevant Exceptions Noted.
C2.4	Employees must sign a statement confirming acknowledgement of all policies and procedures in the associate handbook.	Inspected a selection of signed employee acknowledgement forms for employees hired during the period under review to determine that employees signed a statement confirming acknowledgement of all policies and procedures in the associate handbook.	No Relevant Exceptions Noted.

Control Objective 2 – Human Resources Security (Continued)

CO2 – Control activities provide reasonable assurance to ensure that employees, contractors, understand their responsibilities, are suitable for the roles they are considered for, and exit the organization or change employment in an orderly manner.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C2.5	Employees must sign a Non-Disclosure Agreement as acknowledgement not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected a sample of signed Non-Disclosure Agreements to determine that employees were required to sign the agreement not to disclose proprietary or confidential information, including client information, to unauthorized parties.	No Relevant Exceptions Noted.
C2.6	Employee evaluations are performed on a regular basis against individual objectives derived from the organization’s goals, established standards, and specific job responsibilities.	Conducted inquiry of HR Manager to determine that employee evaluations were performed on a regular basis against individual objectives derived from the organization’s goals, established standards, and specific job responsibilities.	No Relevant Exceptions Noted.
C2.7	Termination checklists are utilized to ensure that an individual's physical access privileges are revoked on the date of termination.	Inspected the termination checklists for a sample of employees terminated during the period under review to determine that termination checklists were utilized to ensure that an individual's physical access privileges were revoked on the date of termination.	No Relevant Exceptions Noted.

Control Objective 3 – Physical Access

CO3 – Control activities provide reasonable assurance that physical access to assets and resources are restricted to authorized personnel only.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C3.1	<p>Physical entry to Mangrove’s Tampa facility is controlled through two access points: the main entrance and the rear entrance, with two side entrances not utilized. The building is kept locked, and access is provided to select authorized users by use of a proximity card system. The two side entrances are blocked, not utilized, and kept locked at all times.</p> <p>For Mangrove Las Vegas, the building is locked at all times beyond the lobby. Access beyond the lobby is restricted to authorized personnel via locked doors.</p>	<p>Observed the entrances to the Tampa facility and conducted corroborative inquiry of Mangrove Tampa management to determine that the building was kept locked at all times and that access was provided to select authorized users by use of a proximity card system.</p> <p>Observed the entrances to the Las Vegas facility and conducted corroborative inquiry of Mangrove Las Vegas management to determine that the building was locked at all times beyond the lobby and restricted to select authorized personnel via locked doors.</p>	<p>No Relevant Exceptions Noted.</p> <p>No Relevant Exceptions Noted.</p>
C3.2	<p>The Tampa and Las Vegas facilities have a security and fire alarm system that is monitored 24x7x365.</p>	<p>Inspected the most recent security monitoring contracts to determine third-party monitoring was in place 24x7x365 for both Tampa and Las Vegas facilities.</p>	<p>No Relevant Exceptions Noted.</p>
C3.3	<p>A badge access system is utilized at Mangrove’s Tampa facility to limit access to and within the facilities.</p>	<p>Inspected the zone definitions for the badge access system to determine that a badge access system was utilized at Mangrove’s Tampa facility to limit access to and within the facilities.</p>	<p>No Relevant Exceptions Noted.</p>
C3.4	<p>Badge access cards reported as lost or stolen are reported to security personnel.</p>	<p>Conducted inquiry of management to determine that badge access cards reported as lost or stolen were reported to security personnel.</p>	<p>No Relevant Exceptions Noted.</p>

Control Objective 3 – Physical Access (Continued)

CO3 – Control activities provide reasonable assurance that physical access to assets and resources are restricted to authorized personnel.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C3.5	For the Tampa facility, the IT department reviews the active badge report periodically to identify any active badges that should be deactivated due to termination, change in job function, or inactivity.	Inspected a current active badge report and conducted corroborative inquiry of IT management to determine that the report was reviewed periodically by IT management to identify any active badges that should be deactivated due to termination, change in job function, or inactivity.	No Relevant Exceptions Noted.
C3.6	For the Las Vegas facility, the building has separate alarm zones separating the lobby from the rest of the building, mechanical locks, and numeric key pads for critical areas. Alarm codes are restricted to select authorized personnel.	Observed the Las Vegas facility’s security measures to determine that the building had separate alarm zones separating the lobby from the rest of the building, mechanical locks, and numeric key pads for critical areas. Conducted corroborative inquiry of management to determine that alarm codes were restricted to select authorized personnel.	No Relevant Exceptions Noted. No Relevant Exceptions Noted.
C3.7	Management restricts the ability to create, modify, or delete user badge access privileges to the facility.	Inspected the badge access system administrator listing and conducted corroborative inquiry of management to determine that management restricted the ability to create, modify, or delete user badge access privileges to the facility.	No Relevant Exceptions Noted.
C3.8	Management secures badge access cards and physical keys, which are restricted to select authorized personnel.	Observed the badge access cards and physical keys in the locked file cabinets to determine that management secured badge access cards and physical keys, which were restricted to select authorized personnel.	No Relevant Exceptions Noted.

Control Objective 3 – Physical Access (Continued)

CO3 – Control activities provide reasonable assurance that physical access to assets and resources are restricted to authorized personnel.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C3.9	<p>For Mangrove’s Tampa facility, physical access to the data center is controlled by a badge access system.</p> <p>For Mangrove’s Las Vegas facility, physical access to the data center is controlled by a numeric keypad electromechanical lock.</p>	<p>Observed the Tampa facility to determine that physical access to the data center was controlled by a badge access system.</p> <p>Observed the Las Vegas facility to determine that physical access to the data center was controlled by a numeric keypad electromechanical lock.</p>	<p>No Relevant Exceptions Noted.</p> <p>No Relevant Exceptions Noted.</p>
C3.10	<p>For Mangrove’s Tampa facility, the walls surrounding the data center extend above the drop ceiling tiles all the way to the physical ceiling.</p>	<p>Observed the Tampa data center to determine that the walls surrounding the data center extended above the drop ceiling tiles all the way to the physical ceiling.</p>	<p>No Relevant Exceptions Noted.</p>

Control Objective 4 – Environment Security

CO4 – Control activities provide reasonable assurance that information technology infrastructure is secured from certain environmental threats.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C4.1	The Tampa facility is equipped with a heat sensor-activated water sprinkler system.	Observed the Tampa facility to determine that the facility was equipped with a heat sensor-activated water sprinkler system.	No Relevant Exceptions Noted.
C4.2	The Tampa and Las Vegas facilities are protected by a fire alarm system.	Observed the Tampa and Las Vegas facilities and conducted corroborative inquiry of onsite management to determine that the facilities were protected by a fire alarm system.	No Relevant Exceptions Noted.
C4.3	Fire extinguishers are in place throughout the facilities and are inspected annually.	Inspected fire extinguishers located throughout both facilities to determine that they were in place and inspected within the previous twelve months.	No Relevant Exceptions Noted.
C4.4	Mangrove maintains business interruption and fire insurance.	Inspected insurance documentation to determine that Mangrove maintained business interruption and fire insurance.	No Relevant Exceptions Noted.
C4.5	The Tampa data center has been configured with hot and cold aisles to maximize cooler airflow to the front of systems.	Observed the hot and cold aisle configuration in the Tampa data center to determine that it was configured with hot and cold aisles to maximize cooler airflow to the front of systems.	No Relevant Exceptions Noted.
C4.6	Both facilities are equipped with a monitoring device that produces an audible alert if the data center air temperature or smoke levels exceed predetermined thresholds.	Observed the presence of the monitoring devices to determine that the facilities were equipped with monitoring devices that produced an audible alert if the data center air temperature or smoke levels exceed predetermined thresholds.	No Relevant Exceptions Noted.

Control Objective 4 – Environment Security (Continued)

CO4 – Control activities provide reasonable assurance that information technology infrastructure is secured from certain environmental threats.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C4.7	The data centers are equipped with primary and redundant Air Conditioning (AC) units.	Observed the data center facilities to determine that they were equipped with primary and redundant AC units.	No Relevant Exceptions Noted.
C4.8	An Uninterruptible Power Supply (UPS) system is in place at both facilities to provide alternate power in the event of a momentary interruption in commercial power.	Observed the UPS systems at both facilities to determine that a UPS was in place provide alternate power in the event of a momentary interruption in commercial power.	No Relevant Exceptions Noted.
C4.9	The Tampa facility utilizes a backup generator to provide power in the event of an extended power loss.	Observed the backup generator at the Tampa facility to determine that an electric power generator was in place to provide power in the event of an extended power loss.	No Relevant Exceptions Noted.
C4.10	The Tampa data center is equipped with raised flooring which is grounded and wired to the main building ground strap.	Observed the Tampa data center to determine that it was equipped with raised flooring which was grounded and wired to the main building ground strap.	No Relevant Exceptions Noted.
C4.11	The Tampa data center is equipped with water sensors under the data center floor.	Observed the Tampa data center to determine that it was equipped with water sensors under the data center floor.	No Relevant Exceptions Noted.

Control Objective 5 – Backup and Recovery

C05 – Control activities provide reasonable assurance that timely system backups, including daily backups of critical files, offsite backup storage, and regular offsite rotation of backup files occur.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C5.1	Critical data, application code, application server operating systems, network operating systems, and customer data is backed up on a regular basis.	Reviewed backup policies, backup applications, and conducted corroborative inquiry of management to determine that critical data, application code, application server operating systems, network operating systems, and customer data was backed up on a regular basis.	No Relevant Exceptions Noted.
C5.2	Automated backup systems are utilized to perform scheduled system backups of target data.	Inspected the configuration of the backup system to determine that an automated backup system was utilized to perform scheduled system backups.	No Relevant Exceptions Noted.
C5.3	Incremental backups of application components and databases are performed on a daily basis, and full backups are performed weekly.	Inspected a selection of backup job completion results to determine that incremental backups of application components and databases were performed on a daily basis, and full backups were performed weekly.	No Relevant Exceptions Noted.
C5.4	Personnel monitor the success or failure of backups on a daily basis and are notified of backup job status via backup log entries and email notifications.	Inspected a sample of backup job summary and email notification history reports and conducted corroborative inquiry of management to determine that Mangrove personnel monitored the success or failure of backups on a daily basis and were notified of backup job status via backup log entries and email notifications.	No Relevant Exceptions Noted.

Control Objective 5 – Backup and Recovery (Continued)

C05 – Control activities provide reasonable assurance that timely system backups, including daily backups of critical files, offsite backup storage, and regular offsite rotation of backup files occur.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C5.5	Restores from backup media are performed as a component of normal business operations to verify that system components can be recovered from backup media.	Inspected a sample of restore job results and conducted corroborative inquiry of management to determine that restores from backup media were performed as a component of normal business operations to verify that system components could be recovered from backup media.	No Relevant Exceptions Noted.
C5.6	An inventory of backup media is maintained.	Inspected a sample backup inventory report to determine that an inventory of backup media was maintained.	No Relevant Exceptions Noted.
C5.7	Backup media is physically secured while onsite in a secured area for shipment to/from offsite storage.	Observed the storage location of the backup media to determine that backup media was physically secured while onsite in a secured area for shipment to/from offsite storage.	No Relevant Exceptions Noted.
C5.8	Backup media is transported to a secure offsite location on a regular schedule.	Inspected the third-party agreement to determine that backup media was transported to a secure offsite location on a regular schedule.	No Relevant Exceptions Noted.
C5.9	Management restricts the ability to retrieve tapes from the offsite storage location to select authorized personnel.	Conducted inquiry of management regarding the backup tapes to determine that the ability to retrieve tapes was restricted to select authorized personnel.	No Relevant Exceptions Noted.

Control Objective 6 – Computer Operations

CO6 – Control activities provide reasonable assurance that systems are maintained in a manner that helps ensure system availability.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C6.1	The organization has an Incident Response Policy in place to provide guidance for responding to and reporting security breaches.	Inspected the Incident Response Policy to determine that documentation was in place for responding to and reporting security breaches.	No Relevant Exceptions Noted.
C6.2	Antivirus software is installed on production systems and managed systems.	Inspected the antivirus configuration and conducted corroborative inquiry of management to determine that antivirus software was utilized on production and systems.	No Relevant Exceptions Noted.
C6.3	Antivirus software is configured to automatically update servers and personal computers on a daily basis.	Inspected antivirus software configurations to determine that antivirus software was configured to automatically update servers and personal computers on a daily basis.	No Relevant Exceptions Noted.
C6.4	System downtime and operations issues are maintained and monitored by management to ensure that system downtime does not exceed acceptable levels.	Inspected a selection of monitoring logs to determine that system downtime and operations issues were maintained and monitored by management to ensure that system downtime did not exceed acceptable levels.	No Relevant Exceptions Noted.
C6.5	Documented procedures exist to respond to application, server, and network outages.	Conducted inquiry of management to determine that procedures were in place to respond to application, server, and network outages.	No Relevant Exceptions Noted.

Control Objective 7 – Logical Access

C07 – Control activities provide reasonable assurance that network logical security settings prevent unauthorized access to the network, limit access to network resources based on business need, and provide management with an audit trail of certain events that occur within the network.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C7.1	Network users are authenticated via a network ID and password before being granted access to network domains.	Inspected the network operating system configurations to determine that network users were authenticated via a network ID and password before being granted access to network domains.	No Relevant Exceptions Noted.
C7.2	Network passwords must conform to minimum complexity as established by management.	Inspected network operating system configurations and conducted corroborative inquiry of management to determine that network passwords conformed to minimum complexity requirement as established by management.	No Relevant Exceptions Noted.
C7.3	Management restricts access to data and application files maintained on the network based on job responsibility.	Conducted corroborative inquiry of management to determine that management restricted access to data and application files maintained on the network based on job responsibility.	No Relevant Exceptions Noted.
C7.4	Network domain administrator rights are restricted to select authorized personnel.	Inspected the network domain administrator group and conducted corroborative inquiry of management to determine that network domain administrator rights were restricted to select authorized personnel.	No Relevant Exceptions Noted.
C7.5	Network management personnel deactivate network accounts assigned to terminated employees upon notification of the employee termination.	Inspected the current domain user account listing and the terminated employee listing to determine that network management personnel deactivated network accounts assigned to terminated employees as a component of the termination process.	No Relevant Exceptions Noted.

Control Objective 7 – Logical Access (Continued)

C07 – Control activities provide reasonable assurance that network logical security settings prevent unauthorized access to the network, limit access to network resources based on business need, and provide management with an audit trail of certain events that occur within the network.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C7.6	Network audit settings are configured to log specific events on the network domains and are reviewed by network management personnel on a daily basis.	Inspected the network domain audit policy configuration and conducted corroborative inquiry of management to determine that network audit settings were configured to log specific events on the network domains and were reviewed by network management personnel on a daily basis.	No Relevant Exceptions Noted.

Control Objective 8 – Data Communications

CO8 – Control activities provide reasonable assurance that the security infrastructure and practices secure against unauthorized access to the company’s internal network, and threats from connections to external networks are limited.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C8.1	A firewall is in place to control network traffic and prevent unauthorized traffic from passing between the internal and external networks.	Inspected the firewall configuration to determine that a firewall was in place to control network traffic and prevent unauthorized traffic from passing between the internal and external networks.	No Relevant Exceptions Noted.
C8.2	A redundant firewall is configured for high availability to minimize downtime.	Inspected the firewall configurations to determine a redundant firewall was operational and configured for high availability.	No Relevant Exceptions Noted.
C8.3	High-level alerts are emailed to administrators for analysis and follow-up is performed to correct problems.	Inspected a sample of email alerts and conducted corroborative inquiry of management to determine that high-level alerts were emailed to administrators for analysis and follow-up was performed to correct problems.	No Relevant Exceptions Noted.
C8.4	All data communications issues are logged and administered through the use of a Network Monitoring system.	Inspected screenshots of the various network monitoring tools and alerts to determine that all data communications issues were logged and administered through the use of a Network Monitoring system.	No Relevant Exceptions Noted.
C8.5	Management restricts the ability to administer the firewall systems to select authorized personnel.	Conducted inquiry of management to determine that management restricted the ability to administer the firewall systems to select authorized personnel.	No Relevant Exceptions Noted.
C8.6	Secure wireless access points exist on the Mangrove corporate network.	Inspected WAP configurations to determine the Company used a secured level of encryption.	No Relevant Exceptions Noted.

Control Objective 9 – Disaster Recovery

CO9 – Control activities provide reasonable assurance that policies and procedures are in place to minimize disruption of processing activities and services to user organizations in the event of a business interruption or natural disaster.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C9.1	Formal documented disaster recovery plans (DRP) are in place to facilitate disaster recovery operations.	Inspected the DRP to determine that formal documented disaster recovery plans were in place to facilitate disaster recovery operations.	No Relevant Exceptions Noted.
C9.2	Certain aspects of the disaster recovery plan are tested on an annual basis.	Inspected a sample of data restores as a component of the DRP to determine certain aspects of the DRP were tested during the period under review.	No Relevant Exceptions Noted.
C9.3	The disaster recovery plans are reviewed on a periodic basis and revised as necessary.	Inspected the DRP version information to determine they were revised within previous 12 months.	No Relevant Exceptions Noted.

Control Objective 10 – Secure Storage, Media, and Document Destruction

CO10 – Controls provide reasonable assurance that procedures are in place and followed for the secure storage and destruction of sensitive data and documents.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C10.1	A secure storage area and shredding system is in place to manage sensitive documents.	Observed the secure storage area and shredding systems to determine that the secure storage area and shredding system was in place.	No Relevant Exceptions Noted.
C10.2	A third-party document management vendor shreds sensitive documentation onsite.	Inspected a sample of recent invoices to determine that a third-party document management vendor shredded sensitive documentation onsite.	No Relevant Exceptions Noted.

Control Objective 11 – Application Development and Change Management

CO11 – Control activities provide reasonable assurance that changes to production, application, system, and programs are properly authorized, tested approved, implemented, and documented.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C11.1	Mangrove application program code is designed and documented in accordance with written standards and procedures established by management.	Inspected the software development workflow to determine that Mangrove application program code was designed and documented in accordance with written standards and procedures established by management.	No Relevant Exceptions Noted.
C11.2	The tracking system logs application change requests from users and internal parties.	Inspected a sample of tracking system logs to determine that the tracking system logs application change requests from users and internal parties.	No Relevant Exceptions Noted.
C11.3	A documented change request is submitted for development and maintenance requests related to applications.	Inspected a sample of change requests to determine that a documented change request was submitted for all development and maintenance requests related to the applications.	No Relevant Exceptions Noted.
C11.4	Modifications and enhancements to existing programs are subjected to user and management review, approval, and testing prior to implementation into the production environment.	Inspected a sample of tickets to determine that modifications and enhancements to existing programs were subjected to user and management review, approval, and testing prior to implementation into the production environment.	No Relevant Exceptions Noted.
C11.5	Management restricts the ability to move code into the production environment to production control personnel.	Conducted inquiry of management to determine that management restricted the ability to move code into the production environment to production control personnel.	No Relevant Exceptions Noted.

Control Objective 11 – Application Development and Change Management (Continued)

CO11 – Control activities provide reasonable assurance that changes to production, application, system, and programs are properly authorized, tested approved, implemented, and documented.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C11.6	QA testing is performed for development and maintenance activities.	Inspected a sample of tickets to determine that QA testing was performed for development and maintenance activities.	No Relevant Exceptions Noted.
C11.7	Logically separated environments are utilized to support the development, QA, client test, and production environments.	Inspected the separate environments to determine that the development, QA, client test, and production environments were logically separated.	No Relevant Exceptions Noted.
C11.8	Version control software is utilized to control access to source code.	Inspected the version control software to determine that commercial version control software was utilized to control access to source code.	No Relevant Exceptions Noted.
C11.9	Management restricts access to the version control software to select authorized personnel.	Conducted inquiry of management to determine that management restricted access to the version control software to select authorized personnel.	No Relevant Exceptions Noted.
C11.10	An emergency change request must be submitted to Mangrove’s helpdesk to utilize the tracking system.	Inspected a sample of emergency change requests to determine that emergency change requests were submitted to Mangrove’s helpdesk.	No Relevant Exceptions Noted.

Control Objective 12 – Benefit Plan Administration

CO12– Controls provide reasonable assurance to ensure that employee benefit administration is accurate and complies with applicable laws and regulations.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C12.1	Formal processes outlining client implementation have been established and executed.	<p>Inspected client implementation process diagrams to determine that formal processes outlining client implementations were established.</p> <p>Inspected a sample of client Statement of Work forms to determine that formal processes outlining client implementations were executed.</p>	<p>No Relevant Exceptions Noted.</p> <p>No Relevant Exceptions Noted.</p>
C12.2	Formal processes outlining the tracking and reconciliation of participant contributions to their employee benefit plans have been established and implemented.	Inspected the process diagram and conducted corroborative inquiry of management to determine that formal processes were in place for posting and reconciling participant contributions as well as for providing clients with an exception report.	No Relevant Exceptions Noted.
C12.3	There are formal processes in place outlining claim adjudication and processing.	Inspected claim adjudication and processing diagrams and conducted corroborative inquiry of management to determine that formal processes were in place outlining the procedures.	No Relevant Exceptions Noted.
C12.4	There are formal procedures in place for receipt of COBRA premium payments from participants.	Observed the receipt processing procedures and conducted corroborative inquiry of management to determine that formal procedures were in place for receipt of COBRA premium payments from participants.	No Relevant Exceptions Noted.

Control Objective 12 – Benefit Plan Administration (Continued)

CO12– Controls provide reasonable assurance to ensure that employee benefit administration is accurate and complies with applicable laws and regulations.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C12.5	Reconciliations are performed for bank accounts and COBRA premium distributions made.	Inspected a sample of reconciliations to determine that reconciliations were performed for bank accounts and COBRA premium distributions made.	No Relevant Exceptions Noted.
C12.6	FSA claims are reviewed for required information prior to entry into the BEMAS system.	Observed staff process and review claims to determine that FSA claims were reviewed for required information prior to entry into the BEMAS system.	No Relevant Exceptions Noted.
C12.7	FSA claims are batched daily and transmitted via SFTP to Benny Central for claims adjudication.	Observed transmission and receipt of a sample batch job sent to Benny Central for adjudication to determine that the transmission was sent via SFTP.	No Relevant Exceptions Noted.
C12.8	An automatic process is used to print checks for approved claims and denial letters for denied claims and the mailings are verified for accuracy by claims staff prior to delivery.	<p>Inspected the automated software configuration to determine that the software will automatically generate a check or denial letter if the claim was approved or denied.</p> <p>Observed staff review the checks and letters to determine that the mailings were verified for accuracy by claims staff prior to delivery.</p>	<p>No Relevant Exceptions Noted.</p> <p>No Relevant Exceptions Noted.</p>

Control Objective 13 – Payroll Implementation

CO13 – Controls provide reasonable assurance that new clients are setup and converted completely and accurately.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C13.1	Mangrove utilizes standard new client checklists to gather required payroll information for the client.	Inspected a sample of standard new client checklists to determine that Mangrove utilized standard new client checklists to gather required payroll information for the client.	No Relevant Exceptions Noted.
C13.2	All clients sign a client service agreement with Mangrove.	Inspected a sample of signed statements of work to determine that all clients signed a client service agreement with Mangrove.	No Relevant Exceptions Noted.
C13.3	<p>The Implementation Team reviews all company information and employee demographics in the payroll software for accuracy and completeness prior to the first payroll run.</p> <p>A Payroll Tax Manager will perform a review of the tax setup, banking setups, ACH file set up, and payroll calendar set up prior to the first run.</p>	<p>Conducted corroborative inquiry of management to determine that the Implementation Team reviewed all company information and employee demographics in the payroll software for accuracy and completeness prior to the first payroll run.</p> <p>Observed a Payroll Tax manager performing verification on a sample of payroll jobs to ensure the accuracy of information used to build the job.</p>	<p>No Relevant Exceptions Noted.</p> <p>No Relevant Exceptions Noted.</p>
C13.4	The Implementation Team performs a balancing process for quarter-to-date wages, year-to-date wages, and tax liabilities of takeover clients prior to the first payroll run.	Conducted corroborative inquiry of the Implementation Team and payroll personnel to determine that the payroll personnel performed a balancing process for quarter-to-date wages, year-to-date wages, and tax liabilities of takeover clients prior to the first payroll run.	No Relevant Exceptions Noted.

Control Objective 13 – Payroll Implementation (Continued)

CO13 – Controls provide reasonable assurance that new clients are setup and converted completely and accurately.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C13.5	Tax filing frequency, account numbers, and year-to-date wages and tax liabilities are reviewed by the Tax Compliance department prior to the first payroll run.	Inspected a sample of tax reviews to determine that tax filing frequency, account numbers, year-to-date wages, and tax liabilities were reviewed by the Tax Compliance department for accuracy prior to the first payroll run.	No Relevant Exceptions Noted.
C13.6	The Implementation Team performs a final quality review of all new clients before the first payroll run.	Inspected a sample of quality reviews to determine that the Implementation Team performed a final quality review of all new clients prior to the first payroll run.	No Relevant Exceptions Noted.
C13.7	A new client’s first two payroll runs are performed and reviewed by the Implementation Team members prior to processing.	Inquired of Finance department management of payroll runs and verification procedures to determine that the Payroll personnel reviewed the first two payroll runs for a new client for accuracy and completeness.	No Relevant Exceptions Noted.

Control Objective 14 – Payroll Processing

CO14 – Controls provide reasonable assurance that processing is scheduled and performed appropriately and deviations from the schedule are identified and resolved.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C14.1	Annually, the payroll processing schedule is published via eMangrove for client review and comment.	Observed the update procedures and publication of annual payroll calendar via eMangrove to determine that the payroll processing schedule was published for client review and comment within the previous twelve months.	No Relevant Exceptions Noted.
C14.2	Activity Reports list each client’s payroll, taxes, and other reports that are to be processed and the date to be processed for the week.	Conducted inquiry of management to determine that weekly processing activities were scheduled for the week’s payroll runs.	No Relevant Exceptions Noted.
C14.3	Payroll is not processed unless approval is received from the client based on agreed procedures authorization method specified in the client contract.	Conducted inquiry of management to determine that payrolls were not processed unless approval was received from the client based on agreed procedures authorization method specified in the client contract.	No Relevant Exceptions Noted.
C14.4	Payroll activity is reviewed by the Payroll Manager and processors throughout the day to verify all scheduled payrolls have been processed and packaged for delivery.	Conducted inquiry of the Payroll Manager to determine that daily payroll review procedures were performed by management and payroll processors to identify any payroll not processed according to the schedule.	No Relevant Exceptions Noted.
C14.5	Payroll check batches are verified when the batch has been printed by comparing printed check counts to the amount of printed checks on the Payroll Register Processing Report.	Conducted inquiry of management to determine that payroll check batches were verified when the batch has been printed by comparing printed check counts to the amount of printed checks on the Payroll Register Processing Report.	No Relevant Exceptions Noted.

Control Objective 14 – Payroll Processing (Continued)

CO14 – Controls provide reasonable assurance that processing is scheduled and performed appropriately and deviations from the schedule are identified and resolved.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C14.6	The 512 report is used to reconcile taxes for the payroll run. This report is used to verify that the proper tax payments are made.	Observed payroll tax verification procedures to determine that a 512 report was utilized for tax total and payment amount verification.	No Relevant Exceptions Noted.
C14.7	ACH files are created in eMangrove, verified, and submitted to the bank for processing.	Observed ACH file creation and verification procedures for a sample of transmitted files to determine that ACH files were created in eMangrove, verified, and submitted to the bank for processing.	No Relevant Exceptions Noted.

Control Objective 15 – Tax Reconciliation

CO15– Controls provide reasonable assurance that appropriate federal, state, and local tax filings are complete, accurate, and timely.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C15.1	The Tax Compliance department runs the Payroll Activity Report daily. This report is sorted by tax type and identifies clients with tax deposits due for a selected date range. Discrepancies appearing on this report are immediately researched and corrected.	Inspected a sample of reports and conducted corroborative inquiry of management to determine that the Tax Compliance department verifies the Tax Deposit by Due Date report daily for accuracy and completeness.	No Relevant Exceptions Noted.
C15.2	The Tax Compliance department utilizes a Payroll Tax Contribution and Wage Summary Report to reconcile the quarter-to-date and year-to date tax returns with the gross wages and taxable wages for all clients per the payroll reports prior to submittal of returns to tax agencies.	Inspected a sample of reconciliation of quarter-to-date and year-to date tax returns with gross wages and taxable wages to determine that the Tax Compliance department utilized a Payroll Tax Contribution and Wage Summary Report to reconcile the quarter-to-date and year-to date tax returns with the gross wages and taxable wages for all clients per the payroll reports prior to submittal of returns to tax agencies.	No Relevant Exceptions Noted.
C15.3	Quarterly, the Tax Compliance department performs a series of audits on all new clients as well as a sample of existing clients to review the taxable wages, tax liabilities, and related tax deposits.	Observed auditing procedures and conducted corroborative inquiry of management to determine that the Tax Compliance department performed a series of audits on all new clients as well as a sample of existing clients to review the taxable wages, tax liabilities, and related tax deposits for completeness and accuracy.	No Relevant Exceptions Noted.
C15.4	A daily date range report is utilized to ensure that all semi-weekly, monthly, quarterly, and annual tax returns are filed.	Conducted inquiry of management to determine that a daily date range report was utilized to ensure that all semi-weekly, monthly, quarterly, and annual tax returns were filed.	No Relevant Exceptions Noted.

Control Objective 15 – Tax Reconciliation (Continued)

CO15– Controls provide reasonable assurance that appropriate federal, state, and local tax filings are complete, accurate, and timely.

	Controls Specified by Mangrove	Testing Performed by SAS 70 CPA	Results of Tests
C15.5	Weekly, the Tax Compliance department reviews the monthly tax deposits made on behalf of clients to the tax impounds during the month to confirm that the correct amounts from each client were collected and paid.	Observed the weekly procedures of the Tax Compliance department and conducted corroborative inquiry of management to determine that the Tax Compliance department reviewed the monthly tax deposits made on behalf of clients to the tax impounds during the month to confirm the correct amounts from each client were collected and paid.	No Relevant Exceptions Noted.