GENERAL CONTROLS SUPPORTING THE APPLICATION SERVICE PROVIDER OPERATIONS

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

For the Period of July 1, 2006, to January 31, 2007

REALTIME COMPUTER CORPORATION

INDEPENDENT SERVICE AUDITOR'S REPORT FOR THE GENERAL CONTROLS SUPPORTING THE APPLICATION SERVICE PROVIDER OPERATIONS

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Realtime Computer Corporation:

We have examined the accompanying description of the general controls supporting the application service provider operations of Realtime Computer Corporation (Realtime). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of Realtime's controls that may be relevant to a user organization's internal control 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 Realtime's controls; and (3) such controls had been placed in operation as of January 31, 2007. The control objectives were specified by the management of Realtime. 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.

In our opinion, the accompanying description of the aforementioned general controls supporting the application service provider operations presents fairly, in all material respects, the relevant aspects of Realtime's controls that had been placed in operation as of January 31, 2007. 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 controls contemplated in the design of Realtime'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 controls, which are presented in Section 3 (the Testing Matrices) of this report, to obtain evidence about their effectiveness in meeting the related control objectives described in the Testing Matrices, during the period from July 1, 2006, to January 31, 2007. The specific controls and the nature, timing, extent, and results of the tests are listed in the Testing Matrices. This information has been provided to user organizations of Realtime and to their auditors to be taken into consideration, along with information about the internal control at user organizations, when making assessments of control risk for user organizations. In our opinion, the controls that were tested, as described in the Testing Matrices, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in the Testing Matrices were achieved during the period from July 1, 2006, to January 31, 2007. However, the scope of our engagement did not include tests to determine whether control objectives not listed in the Testing Matrices were achieved; accordingly, we express no opinion on the achievement of control objectives not included in the Testing Matrices.

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

The description of controls at Realtime is as of January 31, 2007, and information about tests of the operating effectiveness of specific controls covers the period from July 1, 2006, to January 31, 2007. 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 Realtime 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, or the failure to make needed changes, may alter the validity of such conclusions.

This report is intended solely for use by the management of Realtime, Bob Evans Farms, Inc. (Mimi's), and the independent auditors of Bob Evans Farms, Inc. (Mimi's).

[SIGNATURE TO BE ADDED IN FINAL VERSION OF REPORT]

January 31, 2007

SECTION 2

DESCRIPTION OF CONTROLS PLACED IN OPERATION

OVERVIEW OF OPERATIONS

Company Background

Realtime started in 1945 doing basic accounting services, or "write up work". When the early computers were introduced, Realtime used them to produce financial statements, and eventually payroll. At this time Realtime served a variety of businesses and was considered a "service bureau".

During its history, Realtime used the full spectrum of hardware systems including IBM, Honeywell, and HP. In the last 20 years, Realtime has specialized in the hospitality industry. Within the hospitality industry, Realtime specializes in "mid market" restaurant and hotel chains. Realtime targets companies with 50 locations in a variety of states, and has $100 to $300 million in annual revenue.

Description of Services Provided

Realtime provides customers with the ability to process their Accounts Payable, Accounts Receivable, Inventory, Sales Analysis, General Ledger, Financial Statements, and Payroll utilizing Realtime systems. Reatime will design and customize large financial applications for national restaurant and hotel chain customers. Realtime provides its customers with an "enterprise outsourcing" solution, which means all the programs and data, reside at Realtime.

A customer connects to Realtime via a secure encrypted Internet connection and has all of the stores or properties connected to Realtime. Realtime acts like the customer's computer department providing both the centralized hardware and software necessary to process the financial accounting information.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Realtime's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of Realtime's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well by example. Specific control activities that Realtime has implemented in this area are described below.

- Organizational policy statements are documented to communicate entity values and behavioral standards to personnel.
- The employee policy and procedures handbook contains organizational policy statements and codes of conduct to which employees are required to adhere.
- Policies and procedures require that employees sign an acknowledgment form indicating that they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- Employees must sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

Realtime's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Realtime's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Department managers are responsible for training and development to qualify personnel for their functional responsibilities.

Management's Philosophy and Operating Style

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

Organizational Structure and Assignment of Authority and Responsibility

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

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

Human Resource Policies and Practices

Realtime's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Specific control activities that Realtime has implemented in this area are described below.

- Management has established pre-hire screening procedures which are performed for programmers.
- Management has established a formal hiring checklist to guide personnel with the new hire process.
- Management performs evaluations for each employee on a periodic basis.
- Management has established a formal employee termination checklist to guide personnel with the termination process.

RISK ASSESSMENT

Realtime has placed into operation a risk assessment process to identify and manage risks that could affect the organization's ability to provide reliable transaction processing for user organizations. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address those risks. Risks that are considered during management's formal and informal risk assessment activities may include consideration of the following events:

- Changes in operating environment
- New personnel
- New or revamped information systems
- Rapid growth
- New technology
- New business models, products, or activities
- Corporate restructurings
- Expanded operations
- New accounting pronouncements
- Regulatory requirements

Management's recognition of risks that could affect the organization's ability to provide reliable transaction processing for its user organizations is generally implicit, rather than explicit. Management's involvement in the daily operations allows them to detect and mitigate risk related to transaction processing through direct personal involvement with employees and outside parties, thus reducing the need for formalized and structured risk assessment processes.

CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES

Realtime's control objectives and related control activities are included in Section 3 (the Testing Matrices) of this report to eliminate the redundancy that would result from listing them in this section and repeating them in the Testing Matrices. Although the control objectives and related control activities are included in the Testing Matrices, they are, nevertheless, an integral part of Realtime's description of controls.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

MONITORING

Management monitors controls to consider whether they are operating as intended and that the controls are modified appropriately for changes in conditions. Realtime management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policy and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

The Realtime management team conducts quality assurance monitoring on a regular basis and additional training is provided based upon the results of monitoring procedures. Monitoring activities are used to initiate corrective action through firm meetings, department meetings, client conference calls, and informal notifications.

Management's close involvement in the application service provider operations helps to identify significant variances from expectations regarding internal controls. Upper management immediately evaluates the specific facts and circumstances related to any suspected control breakdowns. A decision for addressing any control weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Realtime personnel.

INFORMATION AND COMMUNICATION SYSTEMS

Information Systems

Custom developed applications are utilized to support the application service provider operations. Realtime services are provided by a single Hewlett Packard server, which has redundant power supplies, redundant disks, redundant disk interface cards, redundant memory, redundant processors, redundant cooling fans, redundant tape backup systems, and built-in battery backup. There is also a 100KVA diesel generator, which activates automatically if there is a power outage lasting more than a few seconds.

Communication Systems

Upper management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to an appropriate higher level within Realtime. Realtime management believes that open communication channels help ensure that exceptions are reported and acted on. For that reason, formal communication tools such as organizational charts, employee handbooks, training classes and job descriptions are in place. Management's communication activities are made electronically, verbally, and through the actions of management.

Services are provided through the Internet. To guarantee availability, four different Internet connections are available, each using different pathways through the Internet. In addition to the inherent redundancy provided by multiple Internet pathways, additional redundancy is provided by the use of redundant power systems on the Cisco routers which connect Realtime to the Internet.

Each Internet pathway is able to use three different security mechanisms: SSH, SSL, and IPSec. SSL is used for encrypting web pages. SSH is used for encrypting file transfers. IPSec is used for securing connections to corporate LANs. All three techniques use a minimum of 128-bit encryption.

COMPLEMENTARY CONTROLS AT USER ORGANIZATIONS

Realtime's services are designed with the assumption that certain controls will be implemented by user organizations. Such controls are called complementary user organization controls. It is not feasible for all of the control objectives related to Realtime's services to be solely achieved by Realtime's control procedures. Accordingly, user organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Realtime.

The following complementary user organization controls should be implemented by user organizations to provide additional assurance that the control objectives described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user organizations' locations, user organizations' auditors should exercise judgment in selecting and reviewing these complementary user organization controls.

Complementary User Organization Controls:

1. User organizations are responsible for ensuring that account passwords are unique, not shared, and not easy to guess.
2. User organizations are responsible for ensuring that user accounts and passwords are assigned to only authorized individuals.
3. User organizations are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with Realtime's systems.
4. User organizations are responsible for immediately notifying Realtime of any actual or suspected information security breaches, including compromised user accounts.
5. User organizations are responsible for maintaining their own system(s) of record.
6. User organizations are responsible for determining whether Realtime's security infrastructure is appropriate for its needs and for notifying the service organization of any requested modifications.
7. User organizations are responsible for viewing Realtime websites using an Internet browser capable of decrypting standardized encryption methods.
8. User organizations are responsible for verifying, auditing and reconciling data that is sent to Realtime to confirm that the data is complete and accurate.
9. User organizations are responsible for understanding and complying with their contractual obligations to Realtime.
10. User organizations are responsible for defining the communications method utilized to connect to Realtime's systems (e.g., direct connections, over public networks, etc.).
11. User organizations are responsible for developing their own disaster recovery and business continuity plans that address their inability to access or utilize Realtime's services.
12. User organizations are responsible for testing new and/or modified applications before providing approval for implementation into the production environment.
13. User organizations are responsible for their own security and firewalls on user-controlled networks.
14. User organizations are responsible for determining and maintaining which applications and which modules of the application each user has access to.
15. User organizations are responsible for notifying Realtime in writing of any requested programming modifications.
16. User organizations are responsible for notifying Realtime in writing of the addition, modification, or termination of user accounts.
17. User organizations are responsible for notifying Realtime of changes made to technical or administrative contact information in a timely manner.
18. User organizations are responsible for ensuring the supervision, management, and control of the use of Realtime services by their personnel.
19. User organizations are responsible for ensuring that data is submitted to Realtime in a timely manner.

SECTION 3

TESTING MATRICES

MATRIX 1 **CONTROL ENVIRONMENT**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an integral part of the organization and influence the control consciousness of its personnel.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Integrity and Ethical Values		
1.1	Organizational policy statements are documented to communicate entity values and behavioral standards to personnel.	Inspected the employee handbook to determine that organizational policy statements were documented and communicated entity values and behavioral standards to personnel.	No relevant exceptions noted.
1.2	The employee policy and procedures handbook contains organizational policy statements and codes of conduct to which employees are required to adhere.	Inspected the employee handbook to determine that the handbook contained organizational policy statements and codes of conduct to which employees were required to adhere.	No relevant exceptions noted.
1.3	Policies and procedures require that employees sign an acknowledgment form indicating that they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.	Inquired of the office manager regarding the employee handbook to determine that policies and procedures required that employees sign an acknowledgment form indicating that they had been given access to the employee manual and understood their responsibility for adhering to the policies and procedures contained within the manual.	No relevant exceptions noted.
		Inspected the employee handbook acknowledgment form to determine that the acknowledgement form was included as a part of the employee handbook.	No relevant exceptions noted.

MATRIX 1 **CONTROL ENVIRONMENT**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an integral part of the organization and influence the control consciousness of its personnel.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.4	Employees must sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inquired of the office manager regarding confidentiality statements to determine that employees must sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	No relevant exceptions noted.
		Inspected the confidentiality agreement to determine that the confidentiality statement required employees to agree not to disclose proprietary or confidential information, including client information, to unauthorized parties.	No relevant exceptions noted.
1.5	Background checks are performed for employees as a component of the hiring process.	Inquired of the office manager regarding background checks to determine that background checks were performed for employees as a component of the hiring process.	No relevant exceptions noted.
		Inspected a background checklist to determine that background checks were performed as a component of the hiring checklist.	No relevant exceptions noted.

MATRIX 1 **CONTROL ENVIRONMENT**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an integral part of the organization and influence the control consciousness of its personnel.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Commitment to Competence		
1.6	Department managers are responsible for training and development to qualify personnel for their functional responsibilities.	Inquired of the vice president regarding training initiatives to determine that department managers were responsible for training and development to qualify personnel for their functional responsibilities.	No relevant exceptions noted.
	Management's Philosophy and Operating Style		
1.7	Management is periodically briefed on industry changes affecting services provided.	Inspected a nonstatistical sample of industry publications to determine that management was periodically briefed on industry changes affecting services provided.	No relevant exceptions noted.
1.8	Management meetings are held on a periodic basis to discuss operational issues.	Inquired of the president regarding the nature and extent of management meetings to determine that management meetings were held on a periodic basis to discuss operational issues.	No relevant exceptions noted.
		Inspected a nonstatistical sample of management meeting documents to determine that management meetings were held on a periodic basis to discuss operational issues.	No relevant exceptions noted.

MATRIX 1 **CONTROL ENVIRONMENT**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an integral part of the organization and influence the control consciousness of its personnel.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Organizational Structure and Assignment of Authority and Responsibility		
1.9	An organizational chart is in place to communicate key areas of authority, responsibility and lines of reporting to personnel. These charts are communicated to employees and updated as needed.	Inquired of the office manager regarding organizational charts to determine that an organizational chart was in place to communicate key areas of authority, responsibility and lines of reporting to personnel and that these charts were communicated to employees and updated as needed.	No relevant exceptions noted.
		Inspected the current organizational chart to determine that organizational charts were in place to communicate key areas of authority, responsibility and lines of reporting to personnel.	No relevant exceptions noted.
	Human Resource Policies and Practices		
1.10	Management has established pre-hire screening procedures which are performed for programmers.	Inquired of the office manager regarding pre-hire screening procedures to determine that management had established pre-hire screening procedures which were performed for programmers.	No relevant exceptions noted.
		Inspected the pre-hire screening tests to determine that management had established pre-hire screening procedures for programmers.	No relevant exceptions noted.

MATRIX 1 **CONTROL ENVIRONMENT**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an integral part of the organization and influence the control consciousness of its personnel.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.11	Management has established a formal hiring checklist to guide personnel with the new hire process.	Inquired of the office manager regarding the use of hiring checklists to determine that management had established a formal hiring checklist to guide personnel with the new hire process.	No relevant exceptions noted.
		Inspected the new hire checklist to determine that management had established a formal hiring checklist to guide personnel with the new hire process.	No relevant exceptions noted.
1.12	Management performs evaluations for each employee on a periodic basis.	Inquired of the president regarding employee evaluations to determine that management performed evaluations for each employee on a periodic basis.	No relevant exceptions noted.
		Inspected the employee evaluations for a nonstatistical sample of employees to determine that management performed evaluations for each employee on a periodic basis.	No relevant exceptions noted.
1.13	Management has established a formal employee termination checklist to guide personnel with the termination process.	Inquired of the office manager regarding termination procedures to determine that management had established a formal employee termination checklist to guide personnel with the termination process.	No relevant exceptions noted.
		Inspected the termination checklist to determine that management had established a formal employee termination checklist to guide personnel with the termination process.	No relevant exceptions noted.

MATRIX 2 **PHYSICAL SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Multi -Tenant Office Facility		
2.1	The office complex requires the use of a key card to enter the front entrance after normal business hours.	Observed the office complex front entrance to determine that the office complex required the use of a key card to enter the front entrance after normal business hours.	No relevant exceptions noted.
2.2	Management will notify office complex security personnel when an employee has been terminated to de-activate the key card.	Inquired of the office manager regarding termination procedures to determine that management notified office complex security personnel when an employee had been terminated to de-activate the key card.	No relevant exceptions noted.
		Inspected the office complex key card listing and the listing of employees terminated during the review period to determine that terminated employees were not assigned an active key card.	No relevant exceptions noted.
2.3	Digital surveillance security cameras record activities at the office complex entrances and other areas within the office complex.	Observed the security cameras for the office complex to determine that digital surveillance security cameras recorded activities at the office complex entrances and other areas within the office complex.	No relevant exceptions noted.

MATRIX 2 **PHYSICAL SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.4	The office complex maintains a back-up recording of images obtained by the digital surveillance security cameras for at least 30 days.	Observed images and settings of the office complex digital surveillance security cameras to determine that the office complex maintained a back-up recording of images obtained by the security cameras for at least 30 days.	No relevant exceptions noted.
2.5	Security guards are present during evening hours at the office complex.	Observed the security guards monitoring the office complex during the evening hours to determine that security guards were present during evening hours at the office complex.	No relevant exceptions noted.
		Inspected the building management security guard evening schedule documentation to determine that security guards were present during evening hours at the office complex.	No relevant exceptions noted.
	Realtime Office Facility		
2.6	An alarm security system is in place that utilizes motion detectors to detect unauthorized access attempts within the office facility during non-business hours.	Inquired of the vice president to determine that an alarm security system was in place that utilized motion detectors to detect unauthorized access attempts within the office facility during non-business hours.	No relevant exceptions noted.
		Observed the entry to the facility to determine that an alarm security system was in place that utilized motion detectors to detect unauthorized access attempts within the office facility during non-business hours.	No relevant exceptions noted.

MATRIX 2 **PHYSICAL SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.7	A digital surveillance security camera records activities at the office facility entrance during non-business hours.	Observed the digital surveillance security camera to determine that a digital surveillance camera recorded activities at the office facility entrance during non-business hours.	No relevant exceptions noted.
		Inspected the recorded digital images to determine that a digital surveillance camera recorded activities at the office facility entrance during non-business hours.	The test of the control activity, performed in January 2007, disclosed that the digital surveillance security camera did not record activities at the office facility entrance during non-business hours. Subsequent testing of the control activity, performed in January 2007, disclosed that the digital surveillance camera was recording activities at the office facility entrance during non-business hours.
2.8	The Realtime facility is monitored 24 hours a day by a third party security alarm monitoring company which notifies management by cell phone, paging or landline phone if a breach occurs.	Inspected the alarm monitoring contract to determine that the Realtime facility was monitored 24 hours a day by a third party security alarm monitoring company which notified management by cell phone, paging or landline phone if a breach occurs.	No relevant exceptions noted.

MATRIX 2 **PHYSICAL SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.9	Management restricts access to the office facility to the following personnel: • President • Vice president • Office manager • Shipping manager • Programmers (4) • Consultant	Inspected the physical key assignment listing that included the employee name and job title to determine that management restricted access to the office facility to the following personnel: • President • Vice president • Office manager • Shipping manager • Programmers (4) • Consultant	No relevant exceptions noted.
	<u>Server Room</u>		
2.10	The server room is monitored 24 hours a day by a third party security alarm monitoring company which notifies management by cell phone, paging, or landline phone if a breach occurs.	Inspected the alarm monitoring contract to determine that the server room was monitored 24 hours a day by a security alarm monitoring company which notified management by cell phone, paging, or landline phone if a breach occurs.	No relevant exceptions noted.
2.11	The server room is equipped with a two-factor security access system requiring the knowledge of an access alarm code and a physical key for entry.	Observed the entry into the server room to determine that the server room was equipped with a two-factor access security system requiring the knowledge of an access alarm code and a physical key for entry.	No relevant exceptions noted.

MATRIX 2 **PHYSICAL SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.12	Management restricts access to the server room to the following personnel: • President • Vice president • Office manager • Shipping manager • Programmer	Inquired of the vice president regarding access to server room to determine that management restricted access to the server room to the following personnel: • President • Vice president • Office manager • Shipping manager • Programmer	No relevant exceptions noted.
		Inspected the server room physical key assignment listing that included the employee name and job title to determine that management restricted access to the server room to the following personnel: • President • Vice president • Office manager • Shipping manager • Programmer	No relevant exceptions noted.

MATRIX 2 **PHYSICAL SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.13	The access alarm door codes for the server room security alarm system are changed on a periodic basis.	Inquired of the vice president regarding server room security alarm code changes to determine that the access alarm door codes for the server room security alarm system were changed on a periodic basis.	No relevant exceptions noted.
2.14	Third party contractors must be escorted by an authorized Realtime employee when in the server room facility.	Inquired of the vice president regarding third party contractors' access to the server room to determine that third party contractors were escorted by an authorized Realtime employee when in the server room facility.	No relevant exceptions noted.
		Observed access by third party contractors to the server room to determine that third party contractors were escorted by an authorized Realtime employee when in the server room facility.	No relevant exceptions noted.

MATRIX 2 **PHYSICAL SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.15	Management obtains the physical keys for the office and server room facility as a component of the employee termination process.	Inquired of the office manager regarding the employee termination process to determine that management obtained the physical keys for the office and server room facility as a component of the employee termination process.	No relevant exceptions noted.
		Inspected the office and server room physical key listings for a nonstatistical sample of employees terminated during the review period to determine that the sampled terminated employees were not in possession of the physical keys.	No relevant exceptions noted.
2.16	Glass breakage sensors are installed on the server room glass walls and are connected to the security alarm system.	Observed the glass breakage sensors to determine that the glass breakage sensors were installed on the server room glass walls and were connected to the security alarm system.	No relevant exceptions noted.
		Inspected the security alarm system monitoring contract to determine that the glass breakage sensors were connected to the security alarm system.	No relevant exceptions noted.
2.17	Motion sensors are installed in the ceiling tiles over the server room to prevent unauthorized access to the server room and are connected to the security alarm system.	Observed the motion sensors above the server room to determine that the motion sensors were installed in the ceiling tiles over the server room.	No relevant exceptions noted.
		Inspected the security alarm system monitoring contract to determine that the motion sensors were connected to the security alarm system.	No relevant exceptions noted.

MATRIX 3 **ENVIRONMENTAL SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Server Room		
3.1	The facility is protected by fire detection and suppression controls that include the following: • Fire alarms • Smoke detectors • Water sprinklers • Hand-held fire extinguishers	Inquired of the vice president regarding the facility fire detection and suppression controls to determine that the facility was protected by fire detection and suppression controls that included the following: • Fire alarms • Smoke detectors • Water sprinklers • Hand-held fire extinguishers	No relevant exceptions noted.
		Observed the office facility fire detection and suppression controls to determine that the facility was protected by fire detection and suppression controls that included the following: • Fire alarms • Smoke detectors • Water sprinklers • Hand-held fire extinguishers	No relevant exceptions noted.
3.2	Third party specialists inspect and maintain the fire alarms, smoke detectors, and water sprinklers on an annual basis to ensure that the systems are functioning properly.	Inspected the fire protection equipment test report to determine that third party specialists inspected and maintained the fire alarms, smoke detectors, and water sprinklers within the 12 months preceding the end of the review period to ensure that the systems were functioning properly.	No relevant exceptions noted.

MATRIX 3 **ENVIRONMENTAL SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.3	Third party specialists inspect and maintain the hand-held fire extinguishers on an annual basis to ensure that the extinguishers are functioning properly.	Observed the third party inspection tags for a nonstatistical sample of fire extinguishers to determine that third party specialists inspected and maintained the hand-held fire extinguishers within the 12 months preceding the end of the review period to ensure that the extinguishers were functioning properly.	No relevant exceptions noted.
3.4	The server room is equipped with primary and redundant air conditioning units. The units keep certain infrastructure equipment at vendor recommended temperatures.	Observed the air conditioning thermostats to determine that the server room was equipped with primary and redundant air conditioning units and that the units kept certain infrastructure equipment at vendor recommended temperatures.	No relevant exceptions noted.
3.5	The air conditioning systems are inspected and maintained annually by third party specialists to ensure they are functioning as expected.	Inspected the service agreement for the air conditioning systems to determine that the air conditioning systems were inspected and maintained within the 12 months preceding the end of the review period by third party specialists to ensure they were functioning as expected.	No relevant exceptions noted.
3.6	Pager alert notifications are sent to management personnel when certain infrastructure equipment exceeds vendor recommended temperatures.	Inspected the thermometer device system configurations to determine that pager alert notifications were sent to management personnel when certain infrastructure equipment exceeded vendor recommended temperatures.	No relevant exceptions noted.

MATRIX 3 **ENVIRONMENTAL SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.7	Certain production equipment in the server room is supported by an uninterruptible power supply (UPS) system to provide temporary power in the event of an outage.	Observed the presence of the UPS systems to determine that the server room was supported by a UPS system to provide temporary power in the event of an outage.	No relevant exceptions noted.
3.8	Management maintains a 24 hours a day support and repair service agreement with third party specialists for the production server UPS system.	Inspected the hardware maintenance onsite support agreement to determine that management maintained a 24 hours a day support and repair service agreement with third party specialists for the production server UPS system.	No relevant exceptions noted.
3.9	A diesel fueled electric power generator is in place to provide power to the server room in the event of a power outage.	Observed the diesel fueled powered generator to determine that a diesel fueled electric power generator was in place to provide power to the server room in the event of a power outage.	No relevant exceptions noted.

MATRIX 3 **ENVIRONMENTAL SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.10	Third party specialists perform periodic preventative maintenance procedures on the diesel fueled electric power generator.	Inspected the preventive maintenance inspection form to determine that third party specialists performed preventative maintenance procedures within the 12 months preceding the end of the review period on the diesel fueled electric power generator.	No relevant exceptions noted.
3.11	Water detection devices are in place in the server room to prevent water damage in the event of a flood and/or water leak.	Observed the water detection devices to determine that water detection devices were in place in the server room to prevent water damage in the event of a flood and/or water leak.	No relevant exceptions noted.
3.12	Management has contracted with a third party provider to monitor the water detection device in the server room.	Inspected the third party service contract to determine that management contracted with a third party provider to monitor the water detection device in the server room.	No relevant exceptions noted.

MATRIX 4 **COMPUTER OPERATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance of timely system backups of critical files, off-site backup storage, and regular off-site rotation of backup files.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.1	Management maintains documented system backup policies and procedures that address the following: • Data backup • Recovery • Off-site storage and rotation	Inspected backup policy documentation to determine that management maintained documented system backup policies and procedures that addressed the following: • Data backup • Recovery • Off-site storage and rotation	No relevant exceptions noted.
4.2	Management utilizes an automated backup system to perform weekly, full system backups.	Inspected backup logs and shipping receipts for a nonstatistical sample of weeks during the review period to determine that management utilized an automated backup system to perform weekly, full system backups.	No relevant exceptions noted.
4.3	The backup system is configured to log daily backup events to the production monitoring report on a daily basis.	Inspected production monitoring reports for a nonstatistical sample of days during the review period to determine that the backup system was configured to log daily backup events to the production monitoring report on a daily basis.	No relevant exceptions noted.
4.4	Management reviews production monitoring reports on a daily basis.	Inquired of the vice president regarding production monitoring to determine that management reviewed production monitoring reports on a daily basis.	No relevant exceptions noted.
		Inspected production monitoring reports for a nonstatistical sample of days during the review period to determine that management reviewed production monitoring reports on a daily basis.	No relevant exceptions noted.

MATRIX 4 **COMPUTER OPERATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance of timely system backups of critical files, off-site backup storage, and regular off-site rotation of backup files.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.5	Management reviews system backup results on a daily basis.	Inspected backup logs for a nonstatistical sample of days during the review period to determine that management reviewed system backup results on a daily basis.	No relevant exceptions noted.
4.6	Management utilizes a third party media vaulting company for secure off-site storage of backup media.	Inspected the third party media vaulting service agreement to determine that management utilized a third party media vaulting company for secure off-site storage of backup media.	No relevant exceptions noted.
4.7	Information technology personnel rotate backup tape media off-site on a weekly basis.	Inspected shipping receipts for a nonstatistical sample of weeks during the review period to determine that information technology personnel rotated backup tape media off-site on a weekly basis.	No relevant exceptions noted.
4.8	Management restricts the ability to recall backup media from the third party media vaulting company to the following individuals: • President • Vice president • Office manager • Network support (2)	Inspected the authorized caller list to determine that management restricted the ability to recall backup media from the third party media vaulting company to the following individuals: • President • Vice president • Office manager • Network support (2)	No relevant exceptions noted.

MATRIX 4 **COMPUTER OPERATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance of timely system backups of critical files, off-site backup storage, and regular off-site rotation of backup files.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.9	Management utilizes a third party safe deposit box for secure off-site storage of backup media.	Inquired of the vice president regarding media storage to determine that management utilized a third party safe deposit box for secure off-site storage of backup media.	No relevant exceptions noted.
		Inspected the third party safe deposit box agreement to determine that management utilized a third party safe deposit box for secure off-site storage of backup media.	No relevant exceptions noted.
4.10	Management restricts the ability to recall backup media from the third party safe deposit box to the following individuals: • President • Vice president • Office manager • Network support	Inspected the authorized access list to determine that management restricted the ability to recall backup media from the third party safe deposit box to the following individuals: • President • Vice president • Office manager • Network support	No relevant exceptions noted.
4.11	Management performs backup data restores on a monthly basis.	Inspected restoration logs for a nonstatistical sample of months during the review period to determine that management performed backup data restores on a monthly basis.	No relevant exceptions noted.

MATRIX 5 **COMPUTER OPERATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that systems are maintained in a manner that helps ensure system availability.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.1	Management maintains documented computer operations policies and procedures that address the following: • Equipment outage • Production monitoring • Maintenance • Incident response • Server builds	Inspected computer operations policy documentation to determine that management maintained documented computer operations policies and procedures that addressed the following: • Equipment outage • Production monitoring • Maintenance • Incident response • Server builds	No relevant exceptions noted.
5.2	Information technology personnel utilize a ticket tracking system to manage system incidents, response and resolution.	Inspected the ticketing system configuration to determine that information technology personnel utilized a ticket tracking system to manage system incidents, response and resolution.	No relevant exceptions noted.

MATRIX 5 **COMPUTER OPERATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that systems are maintained in a manner that helps ensure system availability.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.3	Management maintains a production monitoring report which is reviewed on a daily basis for the following: • Backup/exports • Environmental thresholds • Disk space • Load capacity • Unfinished print jobs • Router settings • Modem settings • Integrity checks • Virus definitions • Security patch check	Inquired of the vice president regarding production monitoring to determine that management maintained a production monitoring report which was reviewed on a daily basis for the following: • Backup/exports • Environmental thresholds • Disk space • Load capacity • Unfinished print jobs • Router settings • Modem settings • Integrity checks • Virus definitions • Security patch check	No relevant exceptions noted.

MATRIX 5 **COMPUTER OPERATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that systems are maintained in a manner that helps ensure system availability.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.3 (cont.)		Inspected the daily production monitoring reports for a nonstatistical sample of days during the review period to determine that management maintained a production monitoring report which was reviewed on a daily basis for the following: • Backup/exports • Environmental thresholds • Disk space • Load capacity • Unfinished print jobs • Router settings • Modem settings • Integrity checks • Virus definitions • Security patch check	No relevant exceptions noted.

MATRIX 5 **COMPUTER OPERATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that systems are maintained in a manner that helps ensure system availability.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.4	Certain production systems are configured to send alert notifications when predefined thresholds are exceeded including but not limited to: • Disk space • Utilization • Infinite programming loops • Server failure • Connectivity	Observed a nonstatistical sample of system alerts to determine that certain production systems were configured to send alert notifications when predefined thresholds were exceeded including but not limited to: • Disk space • Utilization • Infinite programming loops • Server failure • Connectivity	No relevant exceptions noted.
		Inspected the alert configuration to determine that certain production systems were configured to send alert notifications when predefined thresholds were exceeded including but not limited to: • Disk space • Utilization • Infinite programming loops • Server failure • Connectivity	No relevant exceptions noted.
5.5	Management maintains warranty and service agreements for certain hardware and software components.	Inspected service contracts to determine that management maintained warranty and service agreements for certain hardware and software components.	No relevant exceptions noted.

MATRIX 5 **COMPUTER OPERATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that systems are maintained in a manner that helps ensure system availability.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Antivirus		
5.6	Antivirus software is configured to monitor traffic within the internal network, as well as communications with external networks, and detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus server settings to determine that antivirus software was configured to monitor traffic within the internal network, as well as communications with external networks, and detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	No relevant exceptions noted.
5.7	The antivirus software updates antivirus definitions on a real-time basis.	Inspected the antivirus software configuration to determine that the antivirus software updated antivirus definitions on a real-time basis.	No relevant exceptions noted.
5.8	The antivirus software is configured to scan the corporate system for virus signatures on a weekly basis.	Inspected the antivirus software configuration to determine that the antivirus software was configured to scan the corporate system for virus signatures on a weekly basis.	No relevant exceptions noted.

MATRIX 6 **APPLICATION CHANGE CONTROL**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that unauthorized changes are not made to production application systems.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Change Request Initiation and Control		
6.1	Management maintains documented change management procedures to guide personnel in requesting, approving, testing and documenting changes to production applications.	Inspected the application change control procedures to determine that management maintained documented change management procedures to guide personnel in requesting, approving, testing and documenting changes to production applications.	No relevant exceptions noted.
6.2	Management maintains documented programming standards to provide personnel with policies, guidelines and standards for designing and developing application code.	Inspected the programming practices and coding notes to determine that management maintained documented programming standards to provide personnel with policies, guidelines and standards for designing and developing application code.	No relevant exceptions noted.
6.3	Management utilizes a change management ticketing system to centrally maintain, manage and monitor development and maintenance activities.	Inquired of the vice president regarding the change management ticketing system to determine that management utilized a change management ticketing system to centrally maintain, manage and monitor development and maintenance activities.	No relevant exceptions noted.
		Inspected a nonstatistical sample of application changes implemented during the review period to determine that management utilized a change management ticketing system to centrally maintain, manage and monitor development and maintenance activities.	No relevant exceptions noted.

MATRIX 6 **APPLICATION CHANGE CONTROL**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that unauthorized changes are not made to production application systems.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Control of Changes		
6.4	Development and production environments are logically separated.	Inquired of the vice president regarding development and production environments to determine that development and production environments were logically separated.	No relevant exceptions noted.
		Inspected the production operating system disk listing and settings to determine that the development and production environments were logically separated.	No relevant exceptions noted.
6.5	Changes to source code results in the creation of a new version of the application code. If necessary, changes can be rolled back to prior versions of the application code.	Inquired of the vice president regarding version control to determine that changes to source code resulted in the creation of a new version of the application code and that changes could be rolled back to prior versions of the application code.	No relevant exceptions noted.
		Inspected a nonstatistical sample of application changes implemented during the review period to determine that changes to source code resulted in the creation of a new version of the application code and that changes could be rolled back to prior versions of the application code.	No relevant exceptions noted.

MATRIX 6 **APPLICATION CHANGE CONTROL**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that unauthorized changes are not made to production application systems.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.6	Management approves application changes prior to migrating the change to the production environment. Management approval is documented in the change management ticketing system.	Inquired of the vice president regarding the application change approval process to determine that management approved application changes prior to migrating the change to the production environment and that the approval was documented in the change management ticketing system.	No relevant exceptions noted.
		Inspected evidence of approval for a nonstatistical sample of application changes implemented during the review period to determine that management approval for changes to the production environment were documented in the change management ticketing system.	No relevant exceptions noted.
6.7	Management restricts the ability to migrate changes to the production environment to the following positions: • President • Vice president • Office manager	Inspected the production operating system security configuration to determine that management restricted the ability to migrate changes to the production environment to following positions: • President • Vice president • Office manager	No relevant exceptions noted.

MATRIX 6 **APPLICATION CHANGE CONTROL**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that unauthorized changes are not made to production application systems.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.8	Management utilizes a daily file integrity assessment tool to monitor instances of unauthorized changes to the production operating system and file configurations.	Inquired of the vice president regarding the daily file integrity assessment tool to determine that management utilized a file integrity assessment tool to monitor instances of unauthorized changes to the production operating system and file configurations.	No relevant exceptions noted.
		Inspected a nonstatistical sample of daily monitoring reports generated during the review period to determine that management utilized the daily file integrity assessment tool to monitor instances of unauthorized changes to the production operating system and file configurations.	No relevant exceptions noted.
	<u>Emergency Changes</u>		
6.9	Emergency change requests are required to be submitted utilizing the change management ticketing system.	Inquired of the vice president regarding emergency changes to determine that emergency change requests were required to be submitted utilizing the change management ticketing system.	No relevant exceptions noted.

MATRIX 7 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	General Administrative Controls		
7.1	Management maintains documented information privacy and security policies and procedures that address the following: • Information protection • Authentication • Access • Monitoring	Inspected policy documentation to determine that management maintained documented information privacy and security policies and procedures that addressed the following: • Information protection • Authentication • Access • Monitoring	No relevant exceptions noted.
7.2	Management revokes operating system access privileges assigned to terminated employees as a component of the employee termination process.	Inquired of the vice president regarding access revocation to determine that management revoked operating system access privileges assigned to terminated employees as a component of the employee termination process.	No relevant exceptions noted.
		Inspected access privileges for a nonstatistical sample of employees terminated during the review period to determine that management revoked operating system access privileges.	No relevant exceptions noted.
	UNIX Operating System (O/S) Authentication Controls		
7.3	The operating system requires users to authenticate via a user ID and password.	Inspected security configurations to determine that the operating system required users to authenticate via a user ID and password.	No relevant exceptions noted.

MATRIX 7 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.4	Operating system passwords are required to conform to minimum length requirements.	Inspected security configurations to determine that operating system passwords were required to conform to minimum length requirements.	No relevant exceptions noted.
7.5	Operating system passwords are required to adhere to certain complexity requirements.	Inspected security configurations to determine that operating system passwords were required to adhere to certain complexity requirements.	No relevant exceptions noted.
7.6	Operating system passwords are required to be changed according to a specified expiration interval.	Inspected security configurations to determine that operating system passwords were required to be changed according to a specified expiration interval.	The test of the control activity, performed in January 2007, disclosed that passwords were not required to be changed according to a specified expiration interval. Subsequent testing of the control activity, performed in January 2007, disclosed that passwords were required to be changed according to a specified interval.
7.7	The operating system is configured to automatically suspend accounts after a specified number of unsuccessful login attempts.	Inspected security configurations to determine that the operating system was configured to automatically suspend accounts after a specified number of unsuccessful login attempts.	No relevant exceptions noted.

MATRIX 7 **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	UNIX O/S Access Controls		
7.8	Management restricts administrative access privileges within the operating system to the following personnel: • President • Vice president	Inquired of the vice president regarding administrative access to determine that management restricted administrative access privileges within the operating system to the following personnel: • President • Vice president	No relevant exceptions noted.
		Inspected the administrative user access listing to determine that management restricted individual users from 'root' privileges.	No relevant exceptions noted.
	UNIX O/S Logging and Monitoring Controls		
7.9	The operating system is configured to capture and post certain events to the daily production monitoring report including, but not limited to: • System traffic activity • Administrator logins • Operating system configuration changes • Operating system file changes	Inspected production monitoring reports for a nonstatistical sample of days to determine that the operating system was configured to capture and post certain events to the daily production monitoring report including, but not limited to: • System traffic activity • Administrator logins • Operating system configuration changes • Operating system file changes	No relevant exceptions noted.

MATRIX 8 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	General Controls		
8.1	Management maintains documented data communications policies and procedures that address the following: • Router configuration • Firewall Configuration • VPN configuration • Encryption standards	Inspected data communications policy documentation to determine that management maintained documented data communications policies and procedures that addressed the following: • Router configuration • Firewall Configuration • VPN configuration • Encryption standards	No relevant exceptions noted.
	Firewall System Administration		
8.2	A firewall system is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the firewall ruleset to determine that a firewall system was in place to filter unauthorized inbound network traffic from the Internet.	No relevant exceptions noted.

MATRIX 8 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.3	Network Address Translation (NAT) services are enabled on the firewall system.	Inspected the firewall ruleset to determine that NAT services were enabled on the firewall system.	No relevant exceptions noted.
8.4	The firewall system is configured to allow specific services to specific destinations and deny undefined traffic.	Inspected the firewall ruleset to determine that the firewall system was configured to allow specific services to specific destinations and deny undefined traffic.	No relevant exceptions noted.
8.5	Management maintains business justification for firewall rules.	Inspected the firewall rules justifications to determine that management maintained business justification for firewall rules.	No relevant exceptions noted.
8.6	The firewall system is configured to log certain network activity to the daily production monitoring report.	Inspected the production monitoring report for a nonstatistical sample of days during the review period to determine that the firewall system was configured to log certain network activity to the daily production monitoring report.	No relevant exceptions noted.
8.7	Management reviews firewall logs on a daily basis.	Inquired of the vice president regarding log reviews to determine that management reviewed firewall logs on a daily basis.	No relevant exceptions noted.
		Inspected production monitoring reports for a nonstatistical sample of days during the review period to determine that management reviewed firewall logs on a daily basis.	No relevant exceptions noted.

MATRIX 8 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.8	Management restricts the ability to modify the firewall system, configuration or rules to the vice president.	Inquired of the vice president regarding firewall administration to determine that management restricted the ability to modify the firewall system, configuration or rules to the vice president.	No relevant exceptions noted.
		Inspected the access control list (ACL) to determine that management restricted the ability to modify the firewall system to a single user account.	No relevant exceptions noted.
	Remote Access		
8.9	Management utilizes encrypted virtual private network (VPN) channels for secured remote network access.	Inspected VPN encryption configurations to determine that management utilized encrypted VPN channels for secured remote network access.	No relevant exceptions noted.
8.10	Management restricts the ability to administer VPN access to the vice president.	Inquired of the vice president regarding VPN administration to determine that management restricted the ability to administer VPN access to the vice president.	No relevant exceptions noted.
		Inspected the VPN ACL to determine that management restricted the ability to administer VPN access to a single user account.	No relevant exceptions noted.

MATRIX 8 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.11	Remote dial-up access authentication requires users to authenticate via username and password. Vulnerability Assessment	Inspected the remote access authentication configuration to determine that remote dial-up access authentication required users to authenticate via username and password.	No relevant exceptions noted.
8.12	Management reviews a production monitoring report to analyze network events and expose possible network security breaches on a daily basis.	Inquired of the vice president regarding monitoring reviews to determine that management reviewed a production monitoring report to analyze network events and expose possible network security breaches on a daily basis. Inspected the production monitoring report for a nonstatistical sample of days during the review period to determine that management reviewed a production monitoring report to analyze network events and expose possible network security breaches on a daily basis.	No relevant exceptions noted. No relevant exceptions noted.

MATRIX 8 **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.13	Management utilizes a third party vulnerability assessment application to perform scans of the production network on a monthly basis.	Inspected vulnerability assessments for a nonstatistical sample of months during the review period to determine that management utilized a third party vulnerability assessment application to perform scans of the production network on a monthly basis.	No relevant exceptions noted.
	Encryption		
8.14	Hyper text transfer protocol secure (HTTPS) is used to secure data transmitted to the production servers.	Inspected the web server connection settings to determine that HTTPS was used to secure data transmitted to the production servers.	No relevant exceptions noted.

MATRIX 9 **DISASTER RECOVERY**

Control Objective Specified by the Service Organization: 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.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
9.1	Management has a documented disaster recovery plan that details the following: • Client, employee, vendor, & supplier lists • Data backup & retrieval procedures • Warm site business continuity services • Additional data procedures	Inspected the current disaster recovery manual to determine that management had a documented disaster recovery plan that detailed the following: • Client, employee, vendor, & supplier lists • Data backup & retrieval procedures • Warm site business continuity services • Additional data procedures	No relevant exceptions noted.
9.2	The documented disaster recovery plan provides guidance to personnel on their responsibilities during a business interruption or natural disaster.	Inspected the disaster recovery manual to determine that the documented disaster recovery plan provided guidance to personnel on their responsibilities during a business interruption or natural disaster.	No relevant exceptions noted.
9.3	Management has contracted with a third party warm site provider to restore full system capability, including external network connections, in the event of a business interruption or a natural disaster.	Inspected the third party warm site provider contract to determine that management had contracted with a third party warm site provider to restore full system capability, including external network connections, in the event of a business interruption or a natural disaster.	No relevant exceptions noted.
9.4	Management performs testing of the disaster recovery plan every eighteen months.	Inspected disaster recovery test results to determine that management performed testing of the disaster recovery plan during the previous eighteen months.	No relevant exceptions noted.