

TM
R

Knowledge | Guidance | Compliance

ios

i

-

A



**REPORT ON CONTROLS PLACED IN OPERATION
AND TESTS OF OPERATING EFFECTIVENESS**

September 1, 2010 – February 28, 2011

TABLE OF CONTENTS

SECTION 1 INDEPENDENT SERVICE AUDITOR'S REPORT	2
SECTION 2 DESCRIPTION OF CONTROLS PROVIDED BY THE SERVICE ORGANIZATION .5	
OVERVIEW OF OPERATIONS	6
Company Background.....	6
Description of Services Provided.....	6
CONTROL ENVIRONMENT	7
Integrity and Ethical Values.....	7
Commitment to Competence.....	7
Board of Directors Participation.....	7
Management's Philosophy and Operating Style	7
Organizational Structure and Assignment of Authority and Responsibility	8
RISK ASSESSMENT	8
CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES	8
MONITORING.....	8
INFORMATION AND COMMUNICATION SYSTEMS	9
Information Systems	9
Communications Systems.....	9
COMPLEMENTARY USER ORGANIZATION CONTROLS	9
SECTION 3 TESTING OF CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES PROVIDED BY THE SERVICE AUDITOR	10
PHYSICAL SECURITY	12
PHYSICAL SECURITY	13
PHYSICAL SECURITY	14
ENVIRONMENTAL SECURITY	15
NETWORK MONITORING AND INCIDENT MANAGEMENT	18
SECTION 4 OTHER INFORMATION PROVIDED BY MANAGEMENT	19

SECTION 1
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Corporate Colocation, Inc.:

We have examined the accompanying description of controls related to the Colocation services of Corporate Colocation, Inc. (the "service organization") performed at the Los Angeles, California, facility. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of Corporate Colocation, Inc.'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 and subservice organizations applied the controls contemplated in the design of Corporate Colocation, Inc.'s controls; and (3) such controls had been placed in operation as of February 28, 2011. The control objectives were specified by the management of Corporate Colocation, Inc. 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 Colocation services presents fairly, in all material respects, the relevant aspects of Corporate Colocation, Inc.'s controls that had been placed in operation as of February 28, 2011. 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 and subservice organizations applied the controls contemplated in the design of Corporate Colocation, Inc.'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 of this report, to obtain evidence about their effectiveness in meeting the control objectives, described in the Section 3, during the period from September 1, 2010 to February 28, 2011. The specific controls and the nature, timing, extent, and results of the tests are listed in Section 3. This information has been provided to user organizations of Corporate Colocation, Inc. 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 Section 3, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Section 3 were achieved during the period from September 1, 2010 to February 28, 2011.

The relative effectiveness and significance of specific controls at Corporate Colocation, Inc. 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 Corporate Colocation, Inc. is as of February 28, 2011, and information about tests of the operating effectiveness of specific controls covers the period from September 1, 2010 to February 28, 2011. 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 Corporate Colocation, Inc. 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 (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended solely for use by the management of Corporate Colocation, Inc., its users, and the independent auditors of its users.

The information in Section 4 of this report is presented by Corporate Colocation, Inc. to provide additional information to user organizations and is not a part of Corporate Colocation, Inc.'s description of controls placed in operation. The information in Section 4 has not been subjected to the procedures applied in the examination of the description of the controls related to the telephony, workforce management, and fiscal application services of Corporate Colocation, Inc., and accordingly, we express no opinion on it.

A-align CPAs

March 9, 2010

SECTION 2

**DESCRIPTION OF CONTROLS PROVIDED
BY THE SERVICE ORGANIZATION**

OVERVIEW OF OPERATIONS

Company Background

Corporate Colocation, Inc. (Corporate Colocation) located in Los Angeles, California was established in 2000. A California Privately Held Corporation, Corporate Colocation is a pioneer in data center operations and network management. Corporate Colocation purchased Mzima Colocation in 2004 and has had a constant trajectory of growth since that time.

Description of Services Provided

Colocation

Electrical Specs:

Cabinet Power Capacity

- Up to 10kW available per cabinet.

UPS

- 2 Power Buses (A + B)
- 2 x ACTIVE UPS (200 kVA ea.) banks for each bus.

Diesel Generators

- 2 x 2.0 Megawatt ACTIVE diesel generators
- 1 x 2.0 Megawatt PASSIVE diesel generators
- Total of 6.0 Megawatts
- Each generator has 4000 gallons directly attached
- Each generator has a dedicated fuel polisher to maintain clean fuel
- Agreement with primary fuel vendor for 48 hour turn-around on supplying additional fuel.
- Agreement with secondary fuel vendor for 4 hour turn-around on supplying additional fuel.
- Vendor = Caterpillar

Power Grid

- 4.0 Megawatt feed from LADWP Grid A
- Backup 4.0 Megawatt feed from LADWP Grid B

Connectivity/Providers/Bandwidth:

- ATT / Level3 / HE / Packet Exchange locally available
- Access to ALL PROVIDERS via dark fiber to One Wilshire MMR
- From 10 Mbps – 10Gbps available bandwidth options

Physical:

- Total square footage = 30,000 sq. ft.
- Colocation area = 15,000 sq. ft.
- Satellite Platform on roof for mounting dish/antennae.
- Rack Types are:
 - 4-post = Chatsworth
 - 19" between rails (external dimensions = 85" H x 24" W x 42" D)
 - 2-post = Chatsworth

Cooling:

- 3 x 400 Ton ACTIVE Chillers
- 1 x 200 Ton PASSIVE Chiller

Environmental:

- Floor is reinforced concrete slab
- Standard square hole rails in all cabinets
- Standard media: Fiber with SC or LC connectors; CAT6, COAX
- Installation readiness: 1-2 weeks for cage build out. Power and Cross-connects can be delivered inside 48 hours.
- Pre-Action Dry-Pipe VESDA fire suppression system

Security:

- 24x7 On-Site Security Guards present for gaining access
- 24x7 On-Site technical support
- Biometric Access Scanners:
 - Access to the Data Center floor requires both a key card as well as a matching biometric finger scan
 - Dedicated cages come standard with an additional door with access keys.
 - Additional biometric finger scanners for dedicated cages are available.
- CCTV captures all areas of the data center facility.
- Both the shared floor space as well as all private cages are equipped with CCTV which digitally records all activity.
- Cabinets are available either “open” or “closed”:
 - Closed cabinets are outfitted with standard keyed locks.

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 Corporate Colocation, Inc.’s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Corporate Colocation, Inc.’s ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. 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 as by example.

Commitment to Competence

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

Board of Directors Participation

Corporate Colocation, Inc.’s control consciousness is influenced significantly by its board of directors. The board of directors oversees management activities and meets on a regular basis to discuss matters pertinent to the organization’s operations and to review financial results.

Management’s Philosophy and Operating Style

Corporate Colocation, Inc.’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.

Organizational Structure and Assignment of Authority and Responsibility

Corporate Colocation, Inc.'s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Corporate Colocation, Inc.'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.

RISK ASSESSMENT

Corporate Colocation, Inc. has placed into operation a risk assessment process to identify and manage risks that could affect the organization's ability to provide reliable 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 risk assessment activities include the following:

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

Management's recognition of risks that could affect the organization's ability to provide reliable processing for its user organizations is generally implicit, rather than explicit. Management's involvement in the daily operations allows them to learn about risks 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

Corporate Colocation, Inc.'s control objectives and related control activities are included in Section 3 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 3. Although the control objectives and related control activities are included in Section 3, they are, nevertheless, an integral part of Corporate Colocation, Inc.'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 Section 3, 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

Strict peer review protocols and division of responsibilities and weekly management meetings to discuss outstanding items and issues provides for real time monitoring of operational activities. Regular conference calls with vendors and client organizations assist in the monitoring process. Senior management is extremely involved in the day to day operations of the company and provides for hands on monitoring. An independent financial audit and compliance audit take place to allow for monitoring of operations by outside parties.

INFORMATION AND COMMUNICATION SYSTEMS

Information Systems

Corporate Colocation, Inc. utilizes commercially available applications to monitor the physical and environmental controls. Corporate Colocation, Inc. does not maintain or have logical access to client's production environments.

Communications 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 a higher level within Corporate Colocation, Inc. Management believes that open communication channels help ensure that exceptions are reported and acted on. Management's communication activities are made electronically, verbally, and through the actions of management.

COMPLEMENTARY USER ORGANIZATION CONTROLS

Corporate Colocation, Inc.'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 Corporate Colocation, Inc.'s services to be solely achieved by Corporate Colocation, Inc. control procedures. Accordingly, user organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Corporate Colocation, Inc.

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.

1. User organizations and subservice organizations are responsible for understanding and complying with their contractual obligations to Corporate Colocation, Inc.
2. User organizations are responsible for notifying Corporate Colocation, Inc. of changes made to technical or administrative contact information.
3. User organizations are responsible for maintaining their own system(s) of record.
4. User organizations are responsible for ensuring the supervision, management and control of the use of Corporate Colocation, Inc.'s services by their personnel.
5. User organizations are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Corporate Colocation, Inc.'s services.
6. User organizations are responsible for securing, monitoring and maintaining the key badges assigned to their personnel.

SECTION 3

TESTING OF CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES PROVIDED BY THE SERVICE AUDITOR

Guidance Regarding Information Provided By The Service Auditor

A-lign CPAs' examination of the controls of Corporate Colocation, Inc. was limited to the control objectives and related control activities specified by the management of Corporate Colocation, Inc. and did not encompass all aspects of Corporate Colocation, Inc.'s operations or operations at user organizations. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standard No. 70 (SAS 70).

Our examination of the control activities were performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquires of service organization personnel. Inquires were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.

In determining whether a SAS 70 report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the processing of the user organization's transactions;
- Understand the flow of significant transactions through the service organization;
- Determine whether the control objectives are relevant to the user organization's financial statement assertions; and
- Determine whether the service organization's controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the user organization's financial statements and determine whether they have been implemented.

Control Area 1

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
1.1	The doors at the facility are locked at all times and can only be opened by an authorized key badge card.	Observed the doors at the facility to determine that the doors at the facility were locked at all times and could only be opened an authorized key badge card.	No relevant exceptions noted.
1.2	A visitor access log is used at the facility which identifies the visitor name, arrival and departure date and times.	Observed a sample of the data center visitor access log to determine that a visitor access log was used at the facility which identified the visitor name, arrival and departure date and times.	No relevant exceptions noted.
1.3	A physical access key badge system exists to control access movement into and throughout the facilities.	Observed the key badge system in operation to determine that a physical access key badge system existed to control access movement into and throughout the facilities.	No relevant exceptions noted.
1.4	A key badge assignment listing exists to monitor and maintain user access rights in the facility.	Inspected the key badge cardholder assignment document to determine that a key badge assignment list existed to monitor and maintain user access rights in the facility.	No relevant exceptions noted.
1.5	Only authorized personnel can access the key badge system to create and update user access rights which include the following personnel: <ul style="list-style-type: none"> • Chief Executive Officer • President 	Observed the key badge system administrators user access list to determine that only authorized personnel can access the key badge system to create and update user access rights which included the following personnel: <ul style="list-style-type: none"> • Chief Executive Officer • President 	No relevant exceptions noted.
1.6	All key badge access attempts are logged and can be used for investigative purposes to identify any suspicious activity.	Observed a sample of the door access report to determine that all key badge attempts were logged and can be used for investigative purposes to identify any suspicious activity.	No relevant exceptions noted.

Control Area 1

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
1.7	A biometric access control system exists to control access movement into and throughout the data center floor.	Observed the biometric access control system during access to the facility to determine that a biometric access control system existed to control access movement into and throughout the data center floor.	No relevant exceptions noted.
1.8	Closed circuit television security cameras are present in the facility which record activity in the facility 24 hours a day, 7 days a week.	Observed the closed circuit television security cameras to determine that closed circuit television security cameras were present in the facility which recorded activity in the facility 24 hours a day, 7 days a week.	No relevant exceptions noted.
1.9	Closed circuit television security cameras are present in the facility which record images to a central digital video recorder (DVR) and the images are stored for a minimum of 5 days.	Observed the digital security camera system image history to determine that closed circuit television security cameras were present in the facility which record images to a central digital video recorder (DVR) and the images were stored for a minimum of 5 days.	No relevant exceptions noted.
1.10	Security management is maintained and supported at the facility by a third party monitoring company.	Observed the third party security guards on duty during access to the facility to determine that security management was maintained and supported at the facility by a third party monitoring company.	No relevant exceptions noted.
1.11	An equipment removal authorization form must be completed and submitted to the facility security management in order to remove any equipment from the secure facilities.	Inquired of the Chief Executive Officer regarding physical security policies to determine that an equipment removal authorization form must be completed and submitted to the facility security management in order to remove any equipment from the secure facilities.	No relevant exceptions noted.

Control Area 1**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
1.12	A verbal authorization is required for each visitor requesting unassisted access to the secure facilities from one of the following individuals: <ul style="list-style-type: none">• Chief Executive Officer• President• Chief Technology Officer	Inquired of the Chief Executive Officer regarding physical security policies to determine that a verbal authorization was required for each visitor requesting unassisted access to the secure facilities from one of the following individuals: <ul style="list-style-type: none">• Chief Executive Officer• President• Chief Technology Officer	No relevant exceptions noted.

Control Area 2

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
	<p><u>Controls applicable to suites 502 and 510 of the Data Center located in Los Angeles, California</u></p>		
2.1	<p>Fire detection and prevention systems are present throughout the facility including:</p> <ul style="list-style-type: none"> • Smoke detection devices • Hand held fire extinguishers • Pre-action dry pipe fire suppression 	<p>Observed the facility to determine that fire detection and prevention systems were present throughout the facility including:</p> <ul style="list-style-type: none"> • Smoke detection devices • Hand held fire extinguishers • Pre-action dry pipe fire suppression 	No relevant exceptions noted.
2.2	<p>Handheld fire extinguishers are inspected on an annual basis to ensure that the pressure is within the recommended levels.</p>	<p>Observed the handheld fire extinguishers to determine that handheld fire extinguishers were inspected on an annual basis to ensure that the pressure was within the recommended levels.</p>	No relevant exceptions noted.
2.3	<p>The pre-action dry pipe fire suppression systems are tested and inspected by a third party provider on an annual basis.</p>	<p>Inspected the results of the third party inspection to determine that the pre-action dry pipe fire suppression systems were tested and inspected by a third party provider on an annual basis.</p>	No relevant exceptions noted.
2.4	<p>An uninterruptable power supply (UPS) is in place to provide power to critical infrastructure equipment in the event of a temporary power loss or power surge.</p>	<p>Observed the UPS in the facility to determine that an UPS was in place to provide power to critical infrastructure equipment in the event of a temporary power loss or power surge.</p>	No relevant exceptions noted.
2.5	<p>The UPS units are inspected and maintained by a third party on an annual basis.</p>	<p>Inspected the results of the annual inspections to determine that the UPS units were inspected and maintained on an annual basis.</p>	No relevant exceptions noted.

Control Area 2

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
2.6	Two 2000KW generators fueled by diesel fuel are in place to provide power to the data center in the event of an extended power outage.	Observed the generators to determine that two 2000KW generators fueled by diesel fuel were in place to provide power to the facility in the event of an extended power outage.	No relevant exceptions noted.
2.7	The generators are tested on a monthly basis.	Inspected the generator test logs to determine that the generators were tested on a monthly basis.	Test of the control activity disclosed that for the sample of monthly generator tests logs performed during the review period, testing of the generators did not occur during the three months beginning September 2010 ending November 2010.
2.8	Preventive maintenance inspections, service and testing is performed on each of the generators on a semi-annual basis.	Inspected the semi-annual preventive maintenance logs to determine that preventive maintenance inspections, service and testing was performed on each of the generators on a semi-annual basis.	No relevant exceptions noted.
2.9	Temperature and humidity sensor systems are in place in the facility that notifies authorized personnel via email distribution group of readings outside of the defined parameters.	<p>Observed the integrated temperature and humidity sensor systems to determine that redundant temperature and humidity sensor systems were in place in the facility that notified authorized personnel via email distribution group of readings outside of the defined parameters.</p> <p>Inspected the configuration of the integrated temperature and humidity sensor systems to determine that redundant temperature and humidity sensor systems were in place in the facility which notified authorized personnel via email distribution group of readings outside of the defined parameters.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

Control Area 2**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
2.10	The facility is equipped with multiple computer room air conditioning (CRAC) units that provide redundancy in the event of one unit's failure.	Observed the CRAC units within the facility to determine that facility was equipped with multiple CRAC units that provide redundancy in the event of one unit's failure.	No relevant exceptions noted.
2.11	The CRAC units are inspected and maintained by a third party on a monthly basis.	Inspected the monthly inspection and maintenance results for all CRAC units to determine that the CRAC units were inspected and maintained by a third party on a monthly basis.	No relevant exceptions noted.
2.12	Integrated water detection sensors exist within the CRAC units to alert personnel of readings outside of the defined parameters.	Observed the integrated water detection sensors to determine that integrated water detection sensors existed within the CRAC units to alert personnel of readings outside of the defined parameters	No relevant exceptions noted.
2.13	The facility is equipped with multiple airside condenser units that provide cooled air to the data center.	Observed the airside condenser units to determine that the facility was equipped with multiple airside condenser units that provide cooled air to the data center.	No relevant exceptions noted.

Control Area 3**NETWORK MONITORING AND INCIDENT MANAGEMENT**

Control Objective Specified
by the Service Organization:

Control activities provide reasonable assurance that the communications network is monitored for availability and incidents are tracked and resolved in a timely manner.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	Two internet backbone connections provide redundancy of internet connectivity into the each of the two data center suites.	Inspected the network diagram to determine that two internet backbone connections provide redundancy of internet connectivity into each of the two data center suites.	No relevant exceptions noted.
3.2	A monitoring application is utilized to proactively identify and automatically alert IT personnel via email when specific network events occur.	Inspected screenshot of the proactive network monitoring application to determine that a monitoring application was utilized to proactively identify and automatically alert IT personnel via email when specific network events occurred.	No relevant exceptions noted.
3.3	A monitoring application is utilized to automatically alert IT personnel via email when specific network events are logged.	Inspected screenshot of the configuration of the reactive monitoring application to determine that a monitoring application was utilized to automatically alert IT personnel via email when specific network events were logged.	No relevant exceptions noted.
3.4	Network incidents are logged in a central ticketing system and resolution of the ticket is documented.	Inspected a sample of network incidents to determine that network incidents were logged in the ticketing system and resolution of the ticket was documented.	No relevant exceptions noted.

SECTION 4

OTHER INFORMATION PROVIDED BY MANAGEMENT

MANAGEMENT’S RESPONSE TO TESTING EXCEPTIONS

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Testing Exceptions
2.7	The generators are tested on a monthly basis.	Inspected the generator test logs to determine that the generators were tested on a monthly basis.	Test of the control activity disclosed that for the sample of monthly generator tests logs performed during the review period, testing of the generators did not occur during the three months beginning September 2010 ending November 2010.	Management advised that monthly generator testing was not performed during the months September, October and November as a result of restrictions relating to the local smog ordinance.