Deluxe Corporation dba ColoCrossing

Type 2 SOC 1

2023



REPORT ON MANAGEMENT'S DESCRIPTION OF DELUXE CORPORATION DBA COLOCROSSING'S SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

Pursuant to Statement on Standards for Attestation Engagements No. 18 (SSAE 18) Type 2

April 1, 2022 to March 31, 2023

Table of Contents

SECTION 1 ASSERTION OF DELUXE CORPORATION DBA COLOCROSSING'S MANAGEMENT 1

SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT 4

SECTION 3 DESCRIPTION OF DELUXE CORPORATION DBA COLOCROSSING'S INTERNET HOSTING SERVICES SYSTEM 8

OVERVIEW OF OPERATIONS 9
Company Background 9
Description of Services Provided 9
Boundaries of the System 10
Subservice Organizations 10
Significant Changes Since the Last Review 10
CONTROL ENVIRONMENT 11
Integrity and Ethical Values 11
Commitment to Competence 11
Management's Philosophy and Operating Style 11
Organizational Structure and Assignment of Authority and Responsibility 11
Human Resources Policies and Practices 12
RISK ASSESSMENT 12
CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES 12
Integration with Risk Assessment 12
Selection and Development of Control Activities Specified by the Service Organization 13
MONITORING 13
On-Going Monitoring 13
Reporting Deficiencies 13
INFORMATION AND COMMUNICATION SYSTEMS 14
Information Systems 14
Communication Systems 14
COMPLEMENTARY USER ENTITY CONTROLS 15

SECTION 4 DESCRIPTION OF DELUXE CORPORATION DBA COLOCROSSING'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS 16

GUIDANCE REGARDING DESCRIPTION OF DELUXE CORPORATION DBA COLOCROSSING'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS 17
PHYSICAL SECURITY 18
ENVIRONMENTAL SECURITY 22
NETWORK MONITORING AND INCIDENT MANAGEMENT 25

SECTION 1

ASSERTION OF DELUXE CORPORATION DBA COLOCROSSING'S MANAGEMENT

ASSERTION OF DELUXE CORPORATION DBA COLOCROSSING'S MANAGEMENT

April 10, 2023

We have prepared the description of Deluxe Corporation dba ColoCrossing's information technology general control system for the Internet Hosting Services System entitled "Description of Deluxe Corporation dba ColoCrossing's Internet Hosting Services System" throughout the period April 1, 2022 to March 31, 2023, (description) for user entities of the system during some or all of the period April 1, 2022 to March 31, 2023, and their user auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of ColoCrossing controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

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

a. The description fairly presents the information technology general control system made available to user entities of the system during some or all of the period April 1, 2022 to March 31, 2023 as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

    i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including:

        (1) the types of services provided.

        (2) the procedures, within both automated and manual systems, by which services are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities.

        (3) how the system captures significant events and conditions, other than transactions.

        (4) the process used to prepare reports and other information for user entities.

        (5) services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them.

        (6) the specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of the service organization's controls.

        (7) other aspects of our control environment, risk assessment process, information and communication systems (including related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

    ii. includes relevant details of changes to the service organization's system during the period covered by the description.

iii. does not omit or distort information relevant to the scope of the information technology general control system, while acknowledging that the description is prepared to meet the common needs of broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the Internet Hosting Services System information technology general control system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period April 1, 2022 to March 31, 2023, to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of ColoCrossing's controls throughout the period April 1, 2022 to March 31, 2023. The criteria we used in making this assertion were that:

   i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;

   ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

   iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.



Tim Worrall
Senior Manager of Data Center and Technical Operations
Deluxe Corporation dba ColoCrossing

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Deluxe Corporation dba ColoCrossing

Scope

We have examined Deluxe Corporation dba ColoCrossing's ('ColoCrossing' or 'the Company') description of its information technology general control system for the Internet Hosting Services System entitled "Description of Deluxe Corporation dba ColoCrossing's Internet Hosting Services System" throughout the period April 1, 2022 to March 31, 2023, (description) and the suitability of the design and operating effectiveness of ColoCrossing's controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Assertion of Deluxe Corporation dba ColoCrossing's Management" (assertion).

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of ColoCrossing's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design and operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section 1 of this report, ColoCrossing has provided their assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. ColoCrossing is responsible for preparing the description and their assertion, including the completeness, accuracy, and method of presentation of the description and the assertions, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period April 1, 2022 to March 31, 2023. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description, based on the criteria in management's assertions
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description

- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved
- Evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization in their assertion

Independence and Ethical Responsibilities

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements, and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in its information technology general control system. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become inadequate or fail.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4.

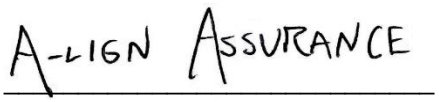
Opinion

In our opinion, in all material respects, based on the criteria described in ColoCrossing's assertion,

a. the description fairly presents the information technology general control system that was designed and implemented throughout the period April 1, 2022 to March 31, 2023.
b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period April 1, 2022 to March 31, 2023 and user entities applied the complementary user entity controls contemplated in the design of ColoCrossing's controls throughout the period April 1, 2022 to March 31, 2023.
c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period April 1, 2022 to March 31, 2023, if user entity controls assumed in the design of ColoCrossing's controls operated effectively throughout the period April 1, 2022 to March 31, 2023.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of ColoCrossing, user entities of ColoCrossing's information technology general control system during some or all of the period April 1, 2022 to March 31, 2023, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.



Tampa, Florida
April 10, 2023

SECTION 3

DESCRIPTION OF DELUXE CORPORATION DBA COLOCROSSING'S INTERNET HOSTING SERVICES SYSTEM

OVERVIEW OF OPERATIONS

Company Background

ColoCrossing, a DBA founded by Velocity Servers Inc in 2007, provides Internet Hosting Services System ranging from dedicated servers to colocation in various datacenters around the country. Major markets served include Buffalo, NY; Chicago, IL; Dallas, TX; Los Angeles, CA; San Jose, CA; Seattle, WA; Atlanta, GA; and New York City, NY.

ColoCrossing and all its assets were acquired by Deluxe Corporation (NYSE: DLX) in June of 2018.

Description of Services Provided

ColoCrossing offers Dedicated Servers, Colocation, and Network Services out of the Buffalo, NY facility.

Dedicated Servers

Fully dedicated machines with root access are sold in various configurations depending on customer needs. ColoCrossing manages the infrastructure around the server and provides assistance to customers on an as needed basis.

Colocation

Colocation is available from a single 1U server to full 42U racks. ColoCrossing manages the utility power, backup power generator and uninterruptible power supply (‘UPS’) devices, and network should the customer elect to connect to the ColoCrossing BUF1 network.

Network

ColoCrossing always maintains at least three upstream Internet service providers, which currently include Cogent Communications, TeliaSonera, and GTT. The Company’s network infrastructure capacity currently exceeds 120 Gbit/s to the Internet.

ColoCrossing also offers Distributed Denial of Service (‘DDoS’) mitigation services through RioRey’s RS30 DDoS mitigation appliances. These are also configured in a redundant fashion.

Network data is captured and analyzed by multiple separate systems for redundancy purposes. With respect to alerting and gather data metrics about the network, ColoCrossing utilizes Zabbix and PRTG software suites. Each of these systems provides alerting to the engineering team should an issue arise.

Physical Security

ColoCrossing is located within a multi-tenant building located in downtown Buffalo, NY. It features a security desk which has security staffed Monday to Friday, 9AM to 5PM. During off-hours, the front door remains locked and all those entering the building require use of a key-fob. ColoCrossing’s office and datacenter is located on the third floor of the facility.

The two doors into the datacenter are locked at all times. Each door has cameras located above it to capture video of anyone who enters and leaves the facility. The doors are protected by two-factor biometric and key-card access controls.

All employees of ColoCrossing are issued a key card and have their fingerprints taken. Access to the datacenter is granted based on their job responsibilities.

Critical systems within the datacenter itself are further protected by additional security measures. A combination lock prevents access into the network cage and no employee is allowed to enter it unless specific instructions are given by management to do so. The power room is protected by key-card access, and only employees whose job involves work within are allowed to enter it. Customer cabinets are locked by separate key.

Customers who require access to their cabinets must first contact ColoCrossing and provide their arrival time and date for the facility. First and last name along with identification is required to be given access to the datacenter. Once they arrive, a ColoCrossing staff member will allow them to enter the facility and unlock their cabinet once identities have been verified.

Significant Events

ColoCrossing has implemented automated and manual procedures to capture and address significant event and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the Colocation services. Please see the procedures, monitoring, and risk assessment procedures described in the relevant sections of this report for further details.

Functional Areas of Operation

The ColoCrossing staff provides support for the above services in each of the following functional areas:

- Executive Management - provides strategic vision of the company and planning of operations
- Development Team - works on software “Portal” which runs company operations and customer interactions
- Engineering Team - manages and maintains the network and systems. Provides customer support at a high level
- Datacenter Team - manages deployment of customer environments and provides first level customer support

Boundaries of the System

The scope of this report includes Internet Hosting Services System performed in the Datacenter located at 325 Delaware Avenue, Buffalo NY, 14202.

Subservice Organizations

No subservice organizations were included in the scope of this assessment.

Significant Changes Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization’s last review.

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 ColoCrossing's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of ColoCrossing'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.

Specific control activities that the service organization has implemented in this area are described below:

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

Commitment to Competence

ColoCrossing'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.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements
- Training is provided to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style

ColoCrossing'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.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole

Organizational Structure and Assignment of Authority and Responsibility

ColoCrossing's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes 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.

ColoCrossing'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 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. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.

Human Resources Policies and Practices

ColoCrossing's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. ColoCrossing's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

RISK ASSESSMENT

ColoCrossing's risk assessment process identifies and manages risks that could potentially affect ColoCrossing's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. ColoCrossing identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by ColoCrossing, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

ColoCrossing's executive team regularly meets to assess risk within the organization from an operational and strategic perspective. Members of the executive management team listen to each other and other team members on what to do to properly mitigate risks to a reasonable level.

CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, ColoCrossing has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of those objectives.

Selection and Development of Control Activities Specified by the Service Organization

Control activities are a part of the process by which ColoCrossing strives to achieve its business objectives. ColoCrossing has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the overall objectives of the organization.

ColoCrossing's control objectives and related control activities are included in Section 4 (the "Testing Matrices") of this report to eliminate the redundancy that would result from listing the items 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 ColoCrossing's description of the data center services system.

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 control activities. 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 ensure that they are operating as intended and that controls are modified as conditions change. ColoCrossing's 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 policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Management's close involvement in ColoCrossing's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's 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 ColoCrossing's personnel.

Vendor Management

No critical vendors are assessed.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

INFORMATION AND COMMUNICATION SYSTEMS

Information Systems

ColoCrossing has implemented mechanisms to track and record operational data to make strategic decisions and ensure objectives are consistently achieved. Information gathered from systems enable ColoCrossing to understand business trends in order to maximize efforts and provide optimal services.

Infrastructure

Primary infrastructure used to provide ColoCrossing's Internet Hosting Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Routers	Juniper MX480 (2)	Edge network device
Switches	Juniper EX4550	Distribution layer network device
UPS	APC Galaxy VM 225 kVA (2)	Uninterruptible Power Supplies provides power in the event of a failure of utility power during the transition to generator power
UPS	APC Symmetra 80 kVa (6)	Uninterruptible Power Supplies provides power in the event of a failure of utility power during the transition to generator power
Generator	Caterpillar 3508B	Backup power generator
DDoS Mitigation	RioRey RS30 (2)	DDoS Mitigation Appliances

Software

Primary software used to provide ColoCrossing's Internet Hosting Services System includes the following:

Primary Software	
Software	**Purpose**
"Portal"	Manages the infrastructure of the network, along with inventory and customer interactions
JunOS	Operating system of the Juniper routers and switches

Communication Systems

Communication is an integral component of ColoCrossing's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. At ColoCrossing, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

All team members utilize e-mail, as well as real-time communication through text-messaging platforms on a daily basis. Meetings with all members of the team are held once monthly, typically on the first Wednesday of the month in order to bring all members to complete understanding of where the business is going.

COMPLEMENTARY USER ENTITY CONTROLS

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

The following complementary user entity controls should be implemented by user entities 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 entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to ColoCrossing.
2. User entities are responsible for notifying ColoCrossing of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of ColoCrossing services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize ColoCrossing services.
6. User entities are responsible for providing ColoCrossing with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying ColoCrossing of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

SECTION 4

DESCRIPTION OF DELUXE CORPORATION DBA COLOCROSSING'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

GUIDANCE REGARDING DESCRIPTION OF DELUXE CORPORATION DBA COLOCROSSING'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

A-LIGN ASSURANCE's examination of the controls of ColoCrossing was limited to the control objectives and related control activities specified by the management of ColoCrossing and did not encompass all aspects of ColoCrossing's operations or operations at user organizations. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 18 (SSAE 18).

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

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries 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.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether a SSAE 18 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;
- 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: Controls provide reasonable assurance that physical access to system data and functions is properly authorized and administered.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.1	Documented physical security policies and procedures are in place to guide personnel in physical security administration.	Inspected the physical security policy to determine that documented physical security policies and procedures are in place to guide personnel in physical security administration.	No exceptions noted.
1.2	Areas designated as data center areas remain secure 24x7 and are only accessed by authorized personnel and or approved vendors for approved purposes, including maintenance, construction and installation activities, transfer of supplies and equipment, or during emergency situations.	Observed the presence and use of a badge access system to determine that areas designated as data center areas remain secure 24x7 and are only accessed by authorized personnel and or approved vendors for approved purposes, including maintenance, construction, and installation activities, transfer of supplies and equipment, or during emergency situations.	No exceptions noted.
		Inspected the badge access log extract and badge access user listing to determine that areas designated as data center areas remain secure 24x7 and are only accessed by authorized personnel and or approved vendors for approved purposes, including maintenance, construction and installation activities, transfer of supplies and equipment, or during emergency situations.	No exceptions noted.
1.3	Data center access points require a keycard with biometric verification to obtain access.	Observed the data center access points to determine that access points require a keycard with biometric verification to obtain access.	No exceptions noted.
		Inspected the badge access user listing and zone definitions to determine that access points require a keycard with biometric verification to obtain access.	No exceptions noted.

CONTROL AREA 1 PHYSICAL SECURITY

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that physical access to system data and functions is properly authorized and administered.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.4	A video surveillance system is in place to monitor and record activity in areas including the following: • Front Doors • Cabinet Rows • Network Cage • Electrical Room and uninterruptable power supply (UPS) Equipment • Back Room Storage Area • Datacenter Technicians Workstations	Observed the closed circuit television security cameras and the network operation center (NOC) to determine that a video surveillance system was in place to monitor and record activity in areas including the following: • Front Doors • Cabinet Rows • Network Cage • Electrical Room and UPS Equipment • Back Room Storage Area • Datacenter Technicians Workstations	No exceptions noted.
		Inspected the video surveillance configurations and the oldest retained video footage to determine that a video surveillance system was in place to monitor and record activity in areas including the following: • Front Doors • Cabinet Rows • Network Cage • Electrical Room and UPS Equipment • Back Room Storage Area • Datacenter Technicians Workstations	No exceptions noted.
1.5	A video surveillance system is in place with footage retained for 30 days.	Inquired of the Sr. Manager of Data Center and Technical Operations regarding the video surveillance system to determine that a video surveillance system is in place with footage retained for 30 days.	No exceptions noted.
		Inspected the video surveillance console and the oldest retained video footage to determine that a video surveillance system is in place with footage retained for 30 days.	No exceptions noted.

CONTROL AREA 1 PHYSICAL SECURITY

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that physical access to system data and functions is properly authorized and administered.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.6	The ability to request badge access changes is restricted to user accounts accessible by persons holding the following positions: • Sr. Manager of Data Center and Technical Operations • Operations Coordinator	Inquired of the Sr. Manager of Data Center and Technical Operations regarding badge access to determine that the ability to request badge access changes was restricted to user accounts accessible by persons holding the following positions: • Sr. Manager of Data Center and Technical Operations • Operations Coordinator	No exceptions noted.
		Inspected the badge access administrator user listing to determine that the ability to request badge access changes was restricted to user accounts accessible by persons holding the following positions: • Sr. Manager of Data Center and Technical Operations • Operations Coordinator	No exceptions noted.
1.7	A hiring checklist is used to request new user access to the badge access system.	Inquired of the Sr. Manager of Data Center and Technical Operations regarding the onboarding process to determine that a hiring checklist was used to request new user access to the badge access system.	No exceptions noted.
		Inspected the badge access user listing and hiring checklist for a sample of new hires to determine that a hiring checklist was used to request new user access to the badge access system.	No exceptions noted.
1.8	Visitors to the facility and server room are required to be escorted by an authorized employee.	Observed the visitor process throughout the facility to determine that visitors to the facility and server room were required to be escorted by an authorized employee.	No exceptions noted.
		Inspected the physical security policy to determine that visitors to the facility and server room were required to be escorted by an authorized employee.	No exceptions noted.

CONTROL AREA 1 **PHYSICAL SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that physical access to system data and functions is properly authorized and administered.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.9	Visitors to the facility and server room are required to sign a visitor log prior upon arrival.	Observed the visitor process throughout the facility to determine that visitors to the facility and server room were required to sign a visitor log prior upon arrival.	No exceptions noted.
		Inspected the visitor log to the facility and server room to determine that visitors to the facility and server room were required to sign a visitor log prior upon arrival.	No exceptions noted.
1.10	Physical access privileges to the corporate office facility are revoked as a component of the termination process.	Inquired of the Sr. Manager of Data Center and Technical Operations regarding the offboarding process to determine that physical access privileges to the corporate office facility were revoked as a component of the termination process.	No exceptions noted.
		Inspected the physical security policy to determine that physical access privileges to the corporate office facility were revoked as a component of the termination process.	No exceptions noted.
		Inspected the badge access user listing and the termination checklist for a sample of terminated employees to determine that physical access privileges to the corporate office facility were revoked as a component of the termination process.	Testing of this control activity disclosed that no personnel were terminated during the review period.

CONTROL AREA 2 **ENVIRONMENTAL SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that environmental protections are in place and operational to prevent likely disruptions to processing.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	General		
2.1	Documented incident handling policies and procedures are in place to guide personnel in the incident management process.	Inspected incident handling procedures to determine that documented incident handling policies and procedures are in place to guide personnel in the incident management process.	No exceptions noted.
	Fire and Smoke Protection		
2.2	Fire detection and prevention systems are present throughout the facility including smoke detection devices, handheld fire extinguishers, and pre-action dry pipe fire suppression.	Observed the data center facility to determine that fire detection and prevention systems were present throughout the facility including smoke detection devices, handheld fire extinguishers, and pre-action dry pipe fire suppression.	No exceptions noted.
2.3	Handheld fire extinguishers are inspected on an annual basis to ensure that the pressure is within the recommended levels.	Observed the fire extinguisher inspection tags to determine that handheld fire extinguishers were inspected on an annual basis to ensure that the pressure was within the recommended levels.	No exceptions noted.
2.4	The pre-action dry pipe fire suppression systems are tested and inspected by a third-party provider on an annual basis.	Inspected the pre-action dry pipe suppression system inspection report to determine that the pre-action dry pipe fire suppression systems were tested and inspected by a third-party provider on an annual basis.	No exceptions noted.
	Power		
2.5	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.	Observed the UPS units to determine that a UPS was in place to provide power to critical infrastructure equipment in the event of a temporary power loss or power surge.	No exceptions noted.
2.6	The UPS units are inspected and maintained on a monthly basis.	Inspected the completed UPS inspection report for a sample of months to determine that the UPS units were inspected and maintained on a monthly basis.	No exceptions noted.

CONTROL AREA 2 **ENVIRONMENTAL SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that environmental protections are in place and operational to prevent likely disruptions to processing.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.7	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 onsite generator to determine that generators fueled by diesel fuel were in place to provide power to the data center in the event of an extended power outage.	No exceptions noted.
		Inspected the generator re-fueling services contract to determine that generators fueled by diesel fuel were in place to provide power to the data center in the event of an extended power outage.	No exceptions noted.
2.8	The generators are tested on a monthly basis.	Inquired of the data center infrastructure admin regarding generator testing to determine that the generators were tested on a monthly basis.	No exceptions noted.
		Inspected the completed generator testing results for a sample of months to determine that the generators were tested on a monthly basis.	No exceptions noted.
2.9	Preventive maintenance inspections and service is performed on the generators on an annual basis.	Inspected the completed generator inspection report to determine that preventive maintenance inspections and service was performed on the generators on an annual basis.	No exceptions noted.
	Temperature and Humidity Monitoring (Cooling)		
2.10	Temperature and humidity sensor systems are in place in the facility that notifies authorized personnel via e-mail distribution group of readings outside of the defined parameters.	Observed the environmental monitoring devices on the data center cabinets to determine that temperature and humidity sensor systems were in place in the facility that notified authorized personnel via e-mail distribution group of readings outside of the defined parameters.	No exceptions noted.

CONTROL AREA 2 **ENVIRONMENTAL SECURITY**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that environmental protections are in place and operational to prevent likely disruptions to processing.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the environmental monitoring system dashboard and an example alert e-mail from a sensor to determine that temperature and humidity sensor systems were in place in the facility that notified authorized personnel via e-mail distribution group of readings outside of the defined parameters.	No exceptions noted.
2.11	The facility is equipped with multiple heating, ventilation, and air conditioning ('HVAC') units that provide redundancy in the event of one unit's failure.	Observed the onsite HVAC units to determine that the facility was equipped with multiple HVAC units that provided redundancy in the event of one unit's failure.	No exceptions noted.
2.12	The HVAC units are inspected monthly.	Inspected the executed contract for HVAC maintenance and the maintenance reports for a sample of months to determine that the HVAC units were inspected monthly.	No exceptions noted.
	Flood and Leak Detection		
2.13	Production equipment within the colocation areas of the data center facilities is placed on racks to protect infrastructure from localized flooding.	Observed the racks housing the equipment to determine that production equipment within the colocation areas of the data center facilities was placed on racks to protect infrastructure from localized flooding.	No exceptions noted.
2.14	The data center equipment sit on raised racks to elevate equipment and help facilitate cooling.	Observed the raised floors within the colocation center to determine that data center equipment sat on raised racks to elevate equipment and help facilitate cooling.	No exceptions noted.

CONTROL AREA 3 NETWORK MONITORING AND INCIDENT MANAGEMENT

Control Objective Specified by the Service Organization: Controls 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	Documented incident handling policies and procedures are in place to guide personnel in the incident handling process.	Inspected the incident handling policies and procedures to determine that documented monitoring and incident response management policies and procedures are in place to guide personnel in the incident management process.	No exceptions noted.
3.2	A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was required in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		Inspected the firewall configurations to determine that a firewall is in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
3.3	Logging and monitoring software is used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity.	Inquired of the Sr. Manager of Data Center and Technical Operations regarding monitoring software to determine that logging and monitoring software was used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity.	No exceptions noted.
		Inspected the Zabbix monitoring console configurations and an example alert notification to determine that logging and monitoring software was used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity.	No exceptions noted.
3.4	The monitoring system is configured to notify Information Technology ('IT') personnel of potential threats.	Inquired of the Sr. Manager of Data Center and Technical Operations regarding monitoring system configuration to determine that the monitoring system was configured to notify IT personnel of potential threats.	No exceptions noted.

CONTROL AREA 3 NETWORK MONITORING AND INCIDENT MANAGEMENT

Control Objective Specified by the Service Organization: Controls 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
		Inspected the monitoring system configurations and an example alert notification to determine that the monitoring system was configured to notify IT personnel of potential threats.	No exceptions noted.
3.5	The data center maintains redundant links to the Internet to help ensure service continually.	Inquired of the Sr. Manager of Data Center and Technical Operations regarding Internet connection redundancy to determine that the data center maintained redundant links to the Internet to help ensure service continually.	No exceptions noted.
		Inspected the executed Internet Service Provider (ISP) service contracts to determine that the data center maintained redundant links to the Internet to help ensure service continually.	No exceptions noted.
3.6	Routing and switching products are used to provide full redundancy.	Inquired of the Sr. Manager of Data Center and Technical Operations regarding switching products to determine that routing and switching products were used to provide full redundancy.	No exceptions noted.
		Observed the datacenter for routing and switching products to determine that routing and switching products were used to provide full redundancy.	No exceptions noted.
3.7	All network devices were dual corded to redundant power circuits from separate UPS feeds.	Observed network devices to determine that all network devices were dual corded to redundant power circuits from separate UPS feeds.	No exceptions noted.
3.8	The entity has implemented redundant Distributed Denial of Service (‘DDoS’) prevention devices within the data center.	Inquired of the Sr. Manager of Data Center and Technical Operations regarding DDoS prevention devices to determine that the entity had implemented redundant DDoS prevention devices within the data center.	No exceptions noted.

CONTROL AREA 3 **NETWORK MONITORING AND INCIDENT MANAGEMENT**

Control Objective Specified by the Service Organization: Controls 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
		Inspected the rWeb console to determine that the entity had implemented redundant DDoS prevention devices within the data center.	No exceptions noted.