A-LIGN

DCBLOX, Inc.

Type 2 SOC 3

2024

DC BLOX

A-LIGN.COM

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

August 1, 2023 to July 31, 2024

Table of Contents

SECTION 1

ASSERTION OF DCBLOX, INC. MANAGEMENT

ASSERTION OF DCBLOX, INC. MANAGEMENT

August 5, 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within DCBLOX, Inc.'s ('DCBLOX' or 'the Company') Data Center Hosting and Client Portal Services System throughout the period August 1, 2023 to July 31, 2024, to provide reasonable assurance that DCBLOX's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "DCBLOX, Inc.'s Description of Its Data Center Hosting and Client Portal Services System throughout the period August 1, 2023 to July 31, 2024" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period August 1, 2023 to July 31, 2024, to provide reasonable assurance that DCBLOX's service commitments and system requirements were achieved based on the trust services criteria. DCBLOX's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "DCBLOX, Inc.'s Description of Its Data Center Hosting and Client Portal Services System throughout the period August 1, 2023 to July 31, 2024".

DCBLOX uses Weiser Security Services ('Weiser' or 'subservice organization') to provide physical security and monitoring services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DCBLOX, to achieve DCBLOX's service commitments and system requirements based on the applicable trust services criteria. The description presents DCBLOX's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DCBLOX's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve DCBLOX's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of DCBLOX's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period August 1, 2023 to July 31, 2024 to provide reasonable assurance that DCBLOX's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of DCBLOX's controls operated effectively throughout that period.

Dave Brown

Dave M. Brown
Director, Security and Compliance
DCBLOX, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To DCBLOX, Inc.:

Scope

We have examined DCBLOX, Inc.'s ('DCBLOX' or 'the Company') accompanying assertion titled "Assertion of DCBLOX, Inc. Management" (assertion) that the controls within DCBLOX's Data Center Hosting and Client Portal Services System were effective throughout the period August 1, 2023 to July 31, 2024, to provide reasonable assurance that DCBLOX's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

DCBLOX uses Weiser to provide physical security and monitoring services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DCBLOX, to achieve DCBLOX's service commitments and system requirements based on the applicable trust services criteria. The description presents DCBLOX's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DCBLOX's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at DCBLOX, to achieve DCBLOX's service commitments and system requirements based on the applicable trust services criteria. The description presents DCBLOX's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of DCBLOX's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

DCBLOX is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that DCBLOX's service commitments and system requirements were achieved. DCBLOX has also provided the accompanying assertion (DCBLOX assertion) about the effectiveness of controls within the system. When preparing its assertion, DCBLOX is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

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

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

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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

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

Opinion

In our opinion, management’s assertion that the controls within DCBLOX’s Data Center Hosting and Client Portal Services System were suitably designed and operating effectively throughout the period August 1, 2023 to July 31, 2024, to provide reasonable assurance that DCBLOX’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of DCBLOX’s controls operated effectively throughout that period.

The SOC logo for Service Organizations on DCBLOX’s website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of DCBLOX, user entities of DCBLOX's Data Center Hosting and Client Portal Services System during some or all of the period August 1, 2023 to July 31, 2024, business partners of DCBLOX subject to risks arising from interactions with the Data Center Hosting and Client Portal Services System, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
August 5, 2024

SECTION 3

DCBLOX, INC.’S DESCRIPTION OF ITS DATA CENTER HOSTING AND CLIENT PORTAL SERVICES SYSTEM THROUGHOUT THE PERIOD AUGUST 1, 2023 TO JULY 31, 2024

OVERVIEW OF OPERATIONS

Company Background

DCBLOX was founded in 2014 with the objective of providing high-performance data center, network and related services to underserved growing markets. DCBLOX customers can realize lower infrastructure costs, increased agility to expand, lower network latency and higher infrastructure reliability. These benefits are delivered via a concurrently maintainable modular data center design that brings higher efficiency of operation connected via a fully redundant private optical network created to offer high-capacity performance and resiliency. The organization is based in Atlanta, Georgia, with data center locations in Birmingham, Alabama, Huntsville, Alabama, Chattanooga, Tennessee, and Greenville, South Carolina.

Industries served by DCBLOX include Manufacturing, Media Services, Telecommunications, Consulting, IT Services, Advertising, Healthcare, Educational institutions, and Government agencies.

Description of Services Provided

DCBLOX provides a full suite of data center colocation, interconnection, and carrier grade connectivity services.

Data Center Services

DCBLOX provides Data Center Services System that can be configured to meet each specific client's needs. Clients are able to request full cabinet, and half cabinet colocation space in power densities ranging from 2kW up to 8kW. Customers with certain power requirements may have the option for a wholesale arrangement which enables the customer to sign a long-term lease and reserve larger amounts of power at utility rates. DCBLOX also provides "Smart Hands" through the data center operations which will perform rudimentary tasks on behalf of the customer without the customer having to travel to the data center.

Interconnection

DCBLOX provides the ability for customers to interconnect with various carrier service providers that are tenants in the data center. Customers request cross connects and DCBLOX provides and manages the physical connections for customers. DCBLOX also provides virtual cross-connects to interconnect with carriers built-in to remote DCBLOX data centers.

Carrier Grade Network Services

Through DCBLOX's fiber optic network customers can opt for Dedicated Internet Access, Ethernet Private Lines and Ethernet Transport, and Cloud Provider Connectivity. Dedicated Internet Access is fully protected and redundant to deliver high reliability. Ethernet Private Line services are fully protected through redundant fiber routes. Ethernet Transport can be delivered protected or unprotected. Ethernet services can be Metro or Long Haul.

Customer Support

DCBLOX Customer Portal provides customers with real time management of DCBLOX services, services related to customer requests such as physical access to their racks and remote hands support of their equipment. Portal hosting is onsite in DCBLOX data centers.

Principal Service Commitments and System Requirements

DCBLOX designs its processes and procedures to meet its objectives for its Data Center Hosting and Client Portal Services System. Those objectives are based on the service commitments that DCBLOX makes to user entities, the laws and regulations that govern the provision of Data Center Hosting Services, and the financial, operational, and compliance requirements that DCBLOX has established for the services. The Data Center Hosting and Client Portal Services System of DCBLOX adhere to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which DCBLOX operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

DCBLOX establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in DCBLOX's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes.

Components of the System

Infrastructure

Primary infrastructure used to provide DCBLOX's Data Center Hosting and Client Portal Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Routers	Juniper MX-240, Juniper MX-204, Arista DCS 7280	Upstream Internet connectivity and Border Gateway Protocol (BGP) routing
Switches	Ciena 8700, Ciena 8100, Ciena 6500, Ciena 5142, Ciena 5142, Ciena 5160, Ciena 5170, Juniper EX3300, Juniper EX3400, Juniper EX4600	Core network routing and network port capacity

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Firewalls	Fortinet VM64-HV Fortigate 200F Fortigate 60E Fortigate 50E	Restricts traffic to and from internal and management networks, as well as providing Virtual Private Network (VPN) services

Software

Primary software used to provide DCBLOX's Data Center Hosting and Client Portal Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Altaro VM Backup	Windows Server 2022	Backups of virtual machines used to monitor and manage production networks
Cacti	CentOS 7	Network performance monitoring, historical, and trending analysis
Ciena Manage, Control and Plan (MCP)	Linux	Management of Ciena network equipment
Microsoft Hyper-V	Windows Server 2022	Virtualization platform
Nagios	Ubuntu 16.04	Network health monitoring and alerting
VT Scada	Windows Server 2022	Data center facilities and environmental monitoring and alerting
Genetec	Windows Server 2019 Windows Server 2022	Data center video monitoring and access control

People

DCBLOX personnel support the above services in each of the following functional areas:

- Technology - Manages technology infrastructure and the development of new and existing products. Identify opportunities and risks for the business. Manage Research and Development (R&D). Communicate the company's technology strategy to partners, management, investors, and employees. Maintain current information about technology standards and compliance regulations.
- Operations - Data center operations include processes and operations performed within a data center. There are several functional areas with data center operations:
  - Infrastructure Operations: Installing, maintaining, monitoring, patching, and updating server, storage, and network resources.
  - Power and cooling: Processes that ensure enough power is supplied to the data center facility and the cooling system is operational.
  - Management: Creation, enforcement, and monitoring of policies and procedures within data center processes.
- Network Strategy - Network strategy ensures the operation of the networking infrastructure, including the following:
  - Commissioning, Provisioning, and Operations of Network Elements, Element Management Systems, and Network Management Systems across the entire DCBLOX footprint and infrastructure.

    - This includes the DCBLOX private Optical Transport Network, Layer2/Ethernet Service Delivery Network, and IP Transit Network Support for the DCBLOX's Network Operations Center (NOC).
- Sales - Identifies business opportunities by identifying prospects and evaluating their position in the industry; researching and analyzing sales options. Sells products by establishing contact and developing relationships with prospects, recommending solutions. Maintains relationships with clients by providing support, information, and guidance, researching, and recommending new opportunities; and recommending profit and service improvements. Identifies product improvements or new products by remaining current on industry trends, market activities, and competitors.
- Data Center Engineering - Data center engineering includes optimizing the performance of DCBLOX's data center from an infrastructure perspective. Data Center Engineering is also responsible for helping locate and build out new data centers. This involves designing, engineering, and overseeing the building of new data centers.
- Product/Marketing - Product Marketing is responsible for developing positioning, messaging, competitive differentiation, and enabling the Sales and Marketing teams to ensure they are aligned and work efficiently to generate and close opportunities. Product Marketing is strategic marketing at the product or product line level.
- Service Delivery - Service Delivery is responsible for the principles, standards, policies, and constraints to be used to guide the design, development, deployment, operation, and retirement of services delivered by a service provider to offer a consistent service experience to the Data Center user community.
- Security and Compliance - Accountable for the building, managing, and implementing controls, processes, and procedures related to securing the facilities, infrastructure, network, and data for DCBLOX. Compliance: Responsible for ensuring controls are being met in accordance to compliance guidelines and preparing for and completing audits for compliance programs. Security: Processes, tools, and technologies that ensure physical and logical security in the data center premises. Day-to-day security operations and log review of equipment throughout the company to maintain the security of the company.

Data

DCBLOX does not directly interact with customer data, but rather provides a secure, reliable environment for customers to store their systems and data.

Processes, Policies and Procedures

DCBLOX has established formal policies and procedures that describe physical security, logical access, computer operations, change control, and data communication standards. Teams are expected to adhere to the DCBLOX policies and procedures that define how services should be delivered. These are located on the company's SharePoint and can be accessed by any DCBLOX team member.

<u>Physical Security</u>

Wholly occupied facilities are protected by fencing around the entire perimeter. Each wholly occupied facility has a designated reception area, attended 24 hours per day by a security guard.

Each facility utilizes high-definition video surveillance systems to monitor activity around and inside the data center. Video is stored for a minimum of 120 days.

Each exterior door or door into a restricted area within the facility is assigned to a door zone, which is used by the access card/ID system to control access. Access to zones is restricted through the use of access control lists. Employees and vendors granted access cards are assigned to roles based on their responsibilities and business justification for access.

Visitors check in with the security guard at the data center entrance. Visitors present a valid, government-issued photo ID before being granted any data center access. The visitor's name, employer, and purpose for a visit are recorded in a visitor log, and their visit is to be approved by a DCBLOX employee who is authorized to sign non-employees into the facility. The visitor will be issued a temporary ID badge to be worn throughout their visit. This temporary badge does not permit access through any secured doors within the facility.

Data centers entrances are controlled by a combination of two doors; access through the exterior door is gained by using a key card to deactivate the locking mechanism, and access through the interior door is granted by using a Personal Identification Number (PIN).

Upon an employee's termination of employment, Human Resources (HR) generates an employee termination request on the last day of employment. This record is routed to the access administrators for deletion. In addition, terminated employees turn over their access cards/IDs during their exit interview. These cards are then returned to security guards at each location for deactivation and destruction.

On a quarterly basis, the Operations Director works with individual Facility Managers to review access to the secure zones of the data center. Any required changes are addressed through the service request system and changes are made as necessary.

Environmental Security

DCBLOX's data center facilities include several environmental safeguards including:

- Birmingham:
  - Power:
    - Up to 5MW critical load; expandable up to 60MW
    - N+1 generator backup
    - N+1 UPS systems
    - Dual UPS feeds to cabinets
    - 24-hour on-site fuel storage
  - Cooling:
    - N+1 cooling
    - Hot aisle containment
    - High efficiency Direct Expansion (DX)
    - RDHX (Rear door heat exchanger) for HPC (High performance compute)
    - Chilled water plant/CRAH (water chilled heat exchangers)
  - Fire detection and prevention:
    - Pre-action fire suppression systems
    - VESDA smoke detection
    - Handheld fire extinguishers
    - Hydrogen sensors in the UPS rooms
    - LiON Tamer (Lithium Ion battery combustion gas monitoring)
- Chattanooga:
  - Power:
    - Up to 1MW critical load; expandable up to 3.5MW
    - Dual 1600 Amp Smart Grid Utility Service
    - Power fed from diverse substations
    - Dual UPS feeds to cabinets
    - 36-hour on-site fuel storage
    - N+N generator backup
    - N+N UPS systems
  - Cooling:
    - N+1 cooling
    - Hot aisle containment

        - 240 Ton air-cooled chiller plant
        - 240 Ton high efficiency dry cooler plant
    - Fire detection and prevention:
        - Pre-action fire suppression systems
        - VESDA smoke detection
        - Handheld fire extinguishers
- Huntsville:
    - Power:
        - Up to 1.5MW critical load; expandable up to 13.5MW
        - N+1 generator backup
        - N+1 UPS systems
        - Dual UPS feeds to cabinets
        - Dual transformers
        - 24-hour on-site fuel storage
    - Cooling:
        - N+1 cooling
        - High-efficiency DX
        - Hot aisle containment
    - Fire detection and prevention:
        - Pre-action fire suppression systems
        - VESDA smoke detection
        - Handheld fire extinguishers
- Greenville:
    - Power:
        - Up to 3MW critical load in phase 1; expandable up to 18MW
        - N+1 generator backup
        - N+1 UPS systems
        - Dual UPS feeds to cabinets
        - 24-hour on-site fuel storage
    - Cooling:
        - N+1 cooling
        - Hot aisle containment
        - High Efficiency DX
    - Fire Suppression:
        - Fire detection and prevention
        - Pre-action fire suppression systems
        - VESDA smoke detection
        - Handheld fire extinguishers

Environmental safeguards are monitored continuously by DCBLOX data center operations teams utilizing SCADA and BMS systems.

Logical Access

DCBLOX uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles. In situations in which incompatible responsibilities cannot be segregated, DCBLOX implements monitoring of one or more of the responsibilities.

Resources are included in the asset inventory system and Operations Management is responsible for maintaining an accurate up-to-date list.

Employees and approved vendor personnel connect to DCBLOX system resources using an Active Directory user ID and password. Connections to network equipment are validated using native user authentication. Passwords conform to defined password standards and are enforced through parameter settings in Active Directory or administrative policy for network equipment. Active Directory password settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and requiring reentry of the user ID and password after a period of inactivity on production servers. Employees accessing the system from outside the DCBLOX network are required to use a VPN system that is integrated into Active Directory.

Upon hire, employees are assigned to a position in the HR management system. Prior to the employees' start date, HR generates a list of the employee user IDs to be created and access to be granted. The report is used by administrators to create user IDs and assign access rules. Access rules have been pre-defined based on the defined roles.

On an annual basis, access to production systems, networks, and environments is reviewed by system administrators and data center managers. In evaluating role access, group members consider job descriptions, duties requiring segregation, and risks associated with access. Administrators present results to Operations Management and Security/Compliance for review, and any required changes are indicated and implemented immediately within the confines of DCBLOX's change management process.

HR generates a list of terminated employees upon any termination. This report is used by system administrators and the Operations team to disable or delete employee access immediately.

Computer Operations - Backups

DCBLOX maintains a backup and recovery system that enables the company to restore any lost data from its production network, management, and monitoring systems. Data is backed up and secured to storage systems located at an alternate DCBLOX data center and protected in locations that are logically separated from the rest of the network. Operations personnel receive notifications of backup tasks and respond immediately in the event of backup failures.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

DCBLOX monitors the capacity utilization of physical space, environmental control systems, network infrastructure, and network links to ensure that service delivery matches SLAs. DCBLOX evaluates the need for additional capacity in response to growth of existing customers, the addition of new customers, and business development targets. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center space, power, redundant power, and cooling
- Network equipment resources (ports, Central Processing Unit (CPU), memory, etc.)
- Network bandwidth

DCBLOX has implemented a patch management process to ensure infrastructure systems are patched in accordance with vendor recommended operating system patches. The DCBLOX Operations team and system owners work cooperatively to review proposed patches to determine whether the patches are applied. System owners and Operations are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. DCBLOX staff validate that patches or updates have been installed and, if applicable, that reboots have been completed, and that the systems are still performing as expected.

Change Control

DCBLOX maintains a formal Change Management Policy to guide personnel in documenting and implementing system changes. Changes to network connectivity, virtual infrastructure, virtual servers, physical servers, patching, financial systems, file servers, camera systems, cameras, access control, UPS, Generator, PDU, fire suppression, storage, load balancers, system updates, provisioning and decommissioning activities are in scope for change control procedures.

Change management procedures include change request and initiation processes, documentation requirements, testing requirements, and required approval procedures.

A ticketing system is utilized to document the change management procedures for system and infrastructure changes. Management approves changes prior to implementation in the production environment and documents those approvals within the ticketing system.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet to management and administrative networks. Network Address Translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees and internal IP ranges.

Redundant virtual infrastructure clusters are used on production facing data center server environments to help ensure there are no single points of failure on the production facing management, monitoring, and backup systems.

Redundancy is built into physical connections providing intra data center connectivity services and other external facing network customer services. There is no single point of failure on the network fiber infrastructure between data centers, helping to ensure the connections providing Internet access to customers stay online.

The data center switching infrastructure connecting colocation services are fully redundant up to the customer equipment (if equipped). Redundant network connectivity services are an option.

Vulnerability scanning is performed using a third-party vendor on a monthly basis in accordance with DCBLOX policy. The vendor uses industry standard scanning technologies which is combined with a formal methodology specified by DCBLOX. Scans are performed during non-peak hours following maintenance windows. The installation of tools or other software on DCBLOX systems is implemented within the confines of the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the production infrastructure through the Internet through the use of VPN technology. Access to the production infrastructure is tightly controlled.

Boundaries of the System

The scope of this report includes the DCBLOX Data Center Hosting and Client Portal Services System performed in the Chattanooga, Tennessee; Huntsville, Alabama; Birmingham, Alabama; Greenville, South Carolina facilities.

This report does not include the physical security and monitoring services provided by Weiser Security Services at the Chattanooga, Tennessee; Huntsville, Alabama; Birmingham, Alabama; Greenville, South Carolina.

Changes to the System Since the Last Review

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

Incidents Since the Last Review

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

Criteria Not Applicable to the System

All Common/Security and Availability criteria were applicable to DCBLOX's Data Center Hosting and Client Portal Services System.

Subservice Organizations

This report does not include the physical security and monitoring services provided by Weiser Security Services.

Subservice Description of Services

Weiser Security Services provides physical security guard and CCTV monitoring services for DCBLOX's in-scope system.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by Weiser Security Services to provide additional assurance that the Trust Services Criteria described within this report are met:

Subservice Organization - Weiser Security Services		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4, CC7.2	Video surveillance of the data centers is monitored continuously by security guards.
		Security guards monitor other data center facilities video surveillance system while the guard at that location is on patrol.
		Security guards patrol the data center facilities.
		Security guards check visitor's ID's before access is granted to the facilities.
		Security guards alert DCBLOX facility and data center managers if they encounter something out of the ordinary.

DCBLOX management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria through written contracts, such as SLAs. In addition, DCBLOX performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and the subservice organization.
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

COMPLEMENTARY USER ENTITY CONTROLS

DCBLOX'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 Trust Services Criteria related to DCBLOX's services to be solely achieved by DCBLOX control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of DCBLOX.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria 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 DCBLOX.
2. User entities are responsible for notifying DCBLOX of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of DCBLOX 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 DCBLOX services.
6. User entities are responsible for providing DCBLOX with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying DCBLOX of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
8. User entities are responsible for properly disposing of data, software, and infrastructure components.