



A-LIGN



DC BLOX, Inc.
Type 2 SOC 3
2020



SOC 3 FOR SERVICE ORGANIZATIONS REPORT

February 1, 2020 To July 31, 2020

Table of Contents

SECTION 1 ASSERTION OF DC BLOX, INC. MANAGEMENT	1
SECTION 2 INDEPENDENT SERVICE AUDITOR’S REPORT	3
SECTION 3 DC BLOX, INC.’S DESCRIPTON OF ITS DATA CENTER HOSTING AND CLIENT PORTAL SERVICES SYSTEM THROUGHOUT THE PERIOD FEBRUARY 1, 2020 TO JULY 31, 2020.....	7
OVERVIEW OF OPERATIONS.....	8
Company Background	8
Description of Services Provided	8
Principal Service Commitments and System Requirements.....	8
Components of the System.....	9
Boundaries of the System.....	11
Changes to the System Since the Last Review.....	11
Incident Since the Last Review.....	11
Criteria Not Applicable to the System	11
Subservice Organizations.....	12
COMPLEMENTARY USER ENTITY CONTROLS.....	13

SECTION 1
ASSERTION OF DC BLOX, INC. MANAGEMENT

ASSERTION OF DC BLOX, INC. MANAGEMENT

August 10, 2020

We are responsible for designing, implementing, operating, and maintaining effective controls within DC BLOX, Inc.'s ('DC BLOX' or 'the Company') Data Center Hosting and Client Portal Services System throughout the period February 1, 2020 to July 31, 2020, to provide reasonable assurance that DC BLOX's service commitments and system requirements relevant to Security and Availability (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "DC BLOX, Inc.'s Description of Its Data Center Hosting and Client Portal Services System throughout the period February 1, 2020 to July 31, 2020" 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 February 1, 2020 to July 31, 2020, to provide reasonable assurance that DC BLOX'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, Confidentiality, Processing Integrity and Privacy* (AICPA, *Trust Services Criteria*). DC BLOX's objectives for the system in applying 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 "DC BLOX, Inc.'s Description of Its Data Center Hosting and Client Portal Services System throughout the period February 1, 2020 to July 31, 2020".

DC BLOX uses Weiser Security Services ('the subservice organization') to provide physical security guard and CCTV monitoring services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DC BLOX, to achieve DC BLOX's service commitments and system requirements based on the applicable trust services criteria. The description presents DC BLOX's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DC BLOX'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 DC BLOX'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 DC BLOX'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 February 1, 2020 to July 31, 2020 to provide reasonable assurance that DC BLOX's service commitments and system requirements were achieved based on the applicable trust services criteria.



Dave Brown
Director of Security and Compliance
DC BLOX, Inc.

SECTION 2
INDEPENDENT SERVICE AUDITOR'S REPORT



INDEPENDENT SERVICE AUDITOR'S REPORT

To: DC BLOX, Inc.

Scope

We have examined DC BLOX's accompanying description of Data Center Hosting and Client Portal Services System titled "DC BLOX, Inc.'s Description of Its Data Center Hosting and Client Portal Services System throughout the period February 1, 2020 to July 31, 2020" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period February 1, 2020 to July 31, 2020, to provide reasonable assurance that DC BLOX'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* (AICPA, *Trust Services Criteria*).

DC BLOX uses Weiser Security Services to provide physical security guard and CCTV monitoring services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DC BLOX, to achieve DC BLOX's service commitments and system requirements based on the applicable trust services criteria. The description presents DC BLOX's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DC BLOX'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 DC BLOX, to achieve DC BLOX's service commitments and system requirements based on the applicable trust services criteria. The description presents DC BLOX's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of DC BLOX'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

DC BLOX 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 DC BLOX's service commitments and system requirements were achieved. DC BLOX has provided the accompanying assertion titled "Assertion of DC BLOX, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. DC BLOX is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted 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, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- 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 the description is presented in accordance with the description criteria.
- 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.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 DC BLOX's Data Center Hosting and Client Portal Services System were suitably designed and operating effectively throughout the period February 1, 2020 to July 31, 2020, to provide reasonable assurance that DC BLOX's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on DC BLOX'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 DC BLOX, user entities of DC BLOX's Data Center Hosting and Client Portal Services during some or all of the period February 1, 2020 to July 31, 2020, business partners of DC BLOX subject to risks arising from interactions with the Data Center Hosting and Client Portal Services, and those who have sufficient knowledge and understanding of the complementary user entity controls and complementary subservice organization 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 10, 2020

SECTION 3

DC BLOX, INC.'S DESCRIPTION OF ITS DATA CENTER HOSTING AND CLIENT PORTAL SERVICES SYSTEM THROUGHOUT THE PERIOD FEBRUARY 1, 2020 TO JULY 31, 2020

OVERVIEW OF OPERATIONS

Company Background

DC BLOX was founded in 2014 with the objective of providing high-performance data center, network and related services to Tier 2 markets. DC BLOX 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 Atlanta, Georgia.

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

Description of Services Provided

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

Data Center Services

DC BLOX provides data center services 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. DC BLOX 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

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

Carrier Grade Network Services

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

Customer support

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

Principal Service Commitments and System Requirements

DC BLOX designs its processes and procedures to meet its objectives for its Data Center Hosting and Client Portal Services. Those objectives are based on the service commitments that DC BLOX makes to user entities, the laws and regulations that govern the provision of Data Center Hosting and Client Portal Services, and the financial, operational, and compliance requirements that DC BLOX has established for the services.

The Data Center Hosting and Client Portal Services of DC BLOX 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 DC BLOX 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

DC BLOX establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in DC BLOX’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 DC BLOX’s Data Center Hosting and Client Portal Services System includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
Routers	Juniper MX-240 Juniper MX-204	Upstream Internet connectivity and BGP routing
Switches	Ciena 8700 Ciena 6500 Ciena 5142 Ciena 5160 Ciena 5170 Juniper EX3300 Juniper EX3400 Juniper EX4600	Core network routing and network port capacity
Firewalls	Fortinet VM64-HV	Restricts traffic to and from internal and management networks, as well as providing VPN services.

Software

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

Primary Software		
Software	Operating System	Purpose
Altaro VM Backup	Windows Server 2016	Backups of virtual machines used to monitor and manage production networks.
Cacti	CentOS 7	Network performance monitoring, historical, and trending analysis.
Ciena OneControl	Oracle Linux	Management of all Ciena network equipment.
Microsoft Hyper-V	Windows Server 2016	Virtualization platform
Nagios	Ubuntu 16.04	Network health monitoring and alerting
VT Scada	Windows Server 2016	Data center facilities and environmental monitoring and alerting

People

DC BLOX 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 all 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: All 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 all Network Elements, Element Management Systems, and Network Management Systems across the entire DC BLOX footprint and infrastructure
 - This includes the DC BLOX private Optical Transport Network, Layer2/Ethernet Service Delivery Network, and IP Transit Network Support for the DC BLOX'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; 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 DC BLOX'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 with a view to offering 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 DC BLOX. Compliance: Responsible for ensuring all controls are being met in accordance with compliance guidelines and prepare for and complete 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 security of company

Data

DC BLOX 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

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

Boundaries of the System

The scope of this report includes the DC BLOX Data Center Hosting and Client Portal Services System performed in the Chattanooga, Tennessee; Huntsville, Alabama; Birmingham, Alabama; and Atlanta, Georgia facilities.

This report does not include the physical security guard and CCTV monitoring services provided by Weiser Security Services at the Chattanooga, Tennessee; Huntsville, Alabama; Birmingham, Alabama and Atlanta, Georgia facilities.

Changes to the System Since the Last Review

Since the organization's last review, DC BLOX has added the Customer Portal in the scope of this report and added an additional location for Data Center Hosting Services performed in the Birmingham, Alabama facility.

Incident 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 and Availability criterion were applicable to the DC BLOX's Data Center Hosting and Client Portal Services System.

Subservice Organizations

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

Complementary Subservice Organization Controls

DC BLOX'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 DC BLOX's services to be solely achieved by DC BLOX control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of DC BLOX.

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 DC BLOX facility and data center managers if they encounter something out of the ordinary.

DC BLOX 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, DC BLOX 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

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

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 DC BLOX.
2. User entities are responsible for notifying DC BLOX 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 DC BLOX 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 DC BLOX services.
6. User entities are responsible for providing DC BLOX with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying DC BLOX 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.