SCALEMATRIX
Cloud. Colocation. Managed IT.

AICPA System Organization Control (SOC) 3 Report

Security, Availability, and Confidentiality Trust Services Principles (TSP)

Reporting on ScaleMatrix's Data Center Services
and the Suitability of Design of Controls as of August 31, 2017.

ScaleMatrix | San Diego, California

Prepared Pursuant to
Attestation Standards, Section 101 of the AICPA Codification Standards (AT Section 101)
by:

NDNB

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITOR'S REPORT

ScaleMatrix
5775 Kearny Villa Road
San Diego, CA 92123

We have examined **ScaleMatrix's** description of controls of its **Data Center Services** system in **San Diego, California** (the description), and the suitability of the design of controls to meet the criteria for the **Security, Availability, and Confidentiality** Principles set forth in *TSP Section 100, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, 2016,* along with applicable subject matter published within *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®) - AICPA Guide, 2015, Trust Services Principles and Criteria, 2016, as issued by the AICPA Assurance Services Executive Committee (ASEC), and Codification of Statements on Standards for Attestation Engagements, 2017,* as of **August 31, 2017**.

Additionally, the scope of this engagement also includes provisions relevant to *Statement on Standards for Attestation Engagements No. 18, Attestation Standards: Clarification and Recodification*. Specifically, SSAE 18 effectively recodifies and supersedes all relevant prior SSAE pronouncements relevant to the applicable Service Organization Report herein. As such, this report reflects necessary changes in assessment and reporting criteria for meeting the standards put forth in SSAE 18.

The scope of this report, while utilizing the above-referenced publications containing subject matter for all five (5) Trust Service Principles, was limited to the **Security, Availability, and Confidentiality** Trust Services Principles.

The Management of **ScaleMatrix** is responsible for the assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the **Data Center Services** system covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of the controls related to the **Security, Availability, and Confidentiality** of the **Data Center Services** system; (2) testing the **Data Center Services** controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations in controls at a service organization, errors or fraud may occur and not be detected. Controls may not always operate effectively to meet the applicable Trust Services Criteria. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Furthermore, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the controls to meet the applicable Trust Services Criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

In our opinion, **ScaleMatrix** maintained, in all material respects, effective controls over the **Security, Availability, and Confidentiality** of the **Data Center Services** system to provide reasonable assurance the **Data Center Services** itself was protected against unauthorized access (both physical and logical), and personal information was collected, used, retained, and disclosed in conformity with the commitments in the entity's privacy notice and with criteria set forth in Generally Accepted Privacy Principles issued by the AICPA/CICA (found in Appendix D).

NDNB
Atlanta, Georgia.
August 1, 2018.

SCALEMATRIX
Cloud. Colocation. Managed IT.

II. WRITTEN STATEMENT of ASSERTION

We have prepared the description of **ScaleMatrix's Data Center Services** (the description) as of **August 31, 2017**, relevant to the criteria for a description of a Service Organization's system in the AICPA Guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, and/or Privacy* (the description criteria).

The description is intended to provide users with information about the **Data Center Services** system, particularly the system controls intended to meet the criteria for the **Security, Availability, and Confidentiality** Principles set forth in *TSP Section 100, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, 2016,* along with applicable subject matter published within *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®) - AICPA Guide, 2015, Trust Services Principles and Criteria, 2016, as issued by the AICPA Assurance Services Executive Committee (ASEC), and Codification of Statements on Standards for Attestation Engagements, 2017,"* as of **August 31, 2017**.

ScaleMatrix maintains effective controls over the **Security, Availability, and Confidentiality** of its **Data Center Services** environment to provide reasonable assurance that:

- The system is protected, both logically and physically, against unauthorized access ***(Security)***;
- The system is available for operation and use as committed or agreed to ***(Availability)***; and,
- Information that is designated "confidential" is protected as committed or agreed ***(Confidentiality)***.

Our attached description of the relevant environment summarizes those aspects of the relevant system covered by our assertion.

Sincerely,

Name:	Chris Orlando	Rebecca Montee
Title:	CEO	Senior Director, Program Management & Development
Date:	August 31, 2017.	August 31, 2017.
Signature:		

III. DESCRIPTION of the SYSTEM provided by SCALEMATRIX

Background

ScaleMatrix is a Hybrid Service Provider delivering an array of cloud, colocation, managed services, data protection, and connectivity solutions under one simple umbrella. As developers of ground-breaking data center efficiency technology, ScaleMatrix offers a cutting edge product catalog with white-glove support services at market prices which benefit from these proprietary cost-saving innovations.

ScaleMatrix can satisfy everything from small start-ups to Fortune 500 enterprises by leveraging their years of knowledge, infrastructure, strategic partnerships, and technology experience. ScaleMatrix architects, deploys, and manages solutions in one of their two primary data center locations, leverages 12 hybrid data centers across the United States, or can deploy into a client's private data center. ScaleMatrix seeks to provide the most innovative Hybrid Solutions in the industry.

ScaleMatrix was founded in 2010 with an executive leadership team that has been on the forefront of the data center and cloud computing industries for over two decades. Building a new 50,000 square-foot facility in San Diego, California has afforded ScaleMatrix the opportunity to deploy the latest in data center technologies. Among these technologies is ScaleMatrix's proprietary, patent pending, rack enclosure, which will redefine cooling efficiency standards within the industry.

The San Diego campus is comprised of two buildings. The 50,000 square foot data center and the 45,000 square foot Launch Center make up the 95,000 square foot state-of-the-art facility located in the Kearny Mesa section of San Diego, California. Converted to a data center in 2010, the facility offers robust data center space, outstanding floor load bearing capacity, stable electrical feeds and significant riser space. The carrier-neutral center is designed to accommodate clients occupying minimal space up to large cages and private suites, and is used to house the ScaleMatrix cloud offerings. Density is controlled using the ScaleMatrix Dynamic Density solution, which provides for controlled thermal rejection solutions ranging from 2,000w per rack to 52,000w per rack in direct proximity to one another. This innovative solution is provided by encapsulating the traditional cold and hot aisle within the rack itself. The rack is NEMA-3 sealed to provide superior environmental control.

ScaleMatrix's data center provides carrier-neutral colocation access 24x7, with a local 24x7 support NOC which functions in support of both the cloud and colocation offerings. Armed security is provided, with client access verified via human interaction at the building envelope, followed by biometrics at all entrances to the data floor and office spaces. Additionally, access to each rack is individually controlled via rack-dedicated biometric readers.

ScaleMatrix's current product and services offering consists of the following:

Cloud Services:

- VMWare suite of services
- Dell and Intel hardware
- Strictly controlled and reportable physical access
- Shared or dedicated firewalls and IDS / IPS solution
- DDoS mitigation driven by Arbor Networks
- 24x7 qualified and trained NOC staff
- Secure provisioning and de-provisioning
- Documented & witnessed hardware and data disposal policies

Colocation:

- Customized cages or suites
- Rack-level biometrics
- Full inventory controls with reporting
- Real-time access control changes

Infrastructure:

- Up to 52,000w per standard 45u rack
- 2N (physically and electrically separated) UPS and PDU structure feeding to client
- N+1 sealed cooling system
- Rack-dedicated clean gas fire suppression

Network Services:

- Carrier-neutral access to multiple service providers
- Cross connections and dark fiber services available
- DWDM and CWDM solutions available via dark fiber

Security:

- Armed security
- Internal and external cameras, with DVR retention of 120 days minimum
- No client building access without human interaction
- No data floor or office access without multiple layers of physical authentication

Managed Services:

- 24x7 Operations Center
- 24x7 monitoring solutions
- Managed services including full I.T. outsourcing
- Turn-key equipment installation services provided

Infrastructure (Facilities, Equipment, and Networks)

Change Management

All changes which could impact the production environment require approval of the Change Advisory Board. As set forth in the *Change Management Policy*:

“This policy covers all changes to hardware, software, or applications in the I.T. and Facilities infrastructure of ScaleMatrix. This includes modification, changes, or additions to our network services (LAN/WAN), server hardware and software, and support facilities (such as electricity) for our I.T. and Facilities infrastructure. Any changes that might affect the infrastructure upon which ScaleMatrix personnel and clients rely to conduct normal business operations are within the scope of this policy.”

The ScaleMatrix Change Management Policy is a solutions-driven policy, which is to say that any alteration or change to be made to the current environment which may affect a production solution meets the minimum criteria for a change request review to be required before the solution is altered. The Change Advisory Board meets twice a week and reviews all changes, approving or rejecting them as appropriate.

The Change Board (CAB) consists of department heads and subject matter experts, and has final say over all change and solution modification activities. Modifications of an emergency nature are submitted to the CAB for review at the next meeting, and must be accompanied by an Incident Report and Root Cause Analysis (RCA). The RCA may be delayed one additional meeting if information is still being gathered.

Logical Security

Internal Users

Logical security elements outline risk management steps taken in regards to the activities of valid computer users by controlling the resources they can access, as well as the type of access permitted regarding applications and other related I.T. systems.

Logical Security Policies and Procedures for Windows Domain

ScaleMatrix user accounts, regardless of system, are controlled using integration with Microsoft's Active Directory service. ScaleMatrix's logical security policies and procedures effectively address access to system-wide resources. They include the following:

- Identifying resources that require protection, along with the security requirements of various systems/applications. Stakeholders are identified for all assets.
- Identifying how the asset is to be stored and accessed, and by whom.
- Executing against an approval process for removals, additions, and changes to the access system.

Access Rights for New Users

New users are assigned privileges and permissions based on their job descriptions and responsibilities within the organization. New users are notified of their ability to access systems manually. Security parameters for the user ID and password will include the following:

Microsoft Active Directory Password System Attributes

- Temporary passwords which must be changed upon initial log-in
- Enforced password complexity standards
- Password masking on login screens
- Passwords must be changed every 42 days for system access security measures
- Enforced password history rules
- Group passwords / user accounts are only permitted where a system is technically incapable of having multiple user accounts

Changing and Modifying User Access

System access often requires changes, such as the ability to access additional systems, or the removal of access to one system and addition of access to another. In such cases, authorized I.T. personnel will correspond with appropriate department heads and data stakeholders to confirm the changes for employee user access. Following the approval and confirmation of changes, system access activities for that particular employee will be implemented.

Periodic Review of User Access

ScaleMatrix conducts a semi-annual review of all users that have access to company-wide systems, including those with administrative access rights.

Virtual Private Network (VPN) Access
ScaleMatrix restricts VPN access to a select number of employees, and controls and logs all activity conducted via VPN.

Terminating User Access
Immediately upon termination for any employee, ScaleMatrix promptly removes all privileges for that particular employee. Management routinely reviews a list of terminated employees to ensure timely and appropriate disabling of accounts.

System administrators with super user or root / administrative-level access that have been terminated are also handled in the same consistent manner, but with additional caution and oversight being utilized. Because of the access rights afforded to them, ScaleMatrix undertakes a log file analysis for at least the previous 90 days, with results published to the leadership team.

Guest Privileges for User Access
Access to ScaleMatrix systems is never granted without a pre-existing contractual relationship and mutual non-disclosure agreement. Access to production internal controls systems is not permitted without VP or higher authorization.

Vendor-Supplied Defaults for Passwords
Vendor-supplied default passwords are always changed before permitting any system to move out of the Engineering department / off the sandbox VLAN. Systems which cannot retain passwords in compliance with internal policies are not eligible to be deployed.

Network Security

Network security elements ensure the protection of networks and their services from unauthorized modification, destruction, intrusion, or disclosure. Network security provides assurance that a network provides Confidentiality, Integrity, and Availability for all users and solutions.

Network Security Management Practices
Network security management practices are communicated to all employees through regularly scheduled weekly and monthly training sessions, as well as through issuance of security management policies and procedures for ScaleMatrix. Topics regarding all aspects of ScaleMatrix's network infrastructure are discussed with all new employees, and are expected to be adhered to at all times during employment. Employees are expected to develop their security skills and knowledge, and are measured in this knowledge by passing industry-leading certifications (typically ISACA, IISSCC, Cisco, Juniper, or other specific technical provider).

Network Topology
ScaleMatrix maintains current, updated network topology documents regarding the network infrastructure and all supporting network components. Additionally, the network topology documents detail current technical hardware systems and all other ancillary components.

VPN Administration
Virtual Private Networks (VPN) are used for connecting over public networks, and are also used to connect from network-to-network internally, as needed.

Data Communication and Transmission

ScaleMatrix utilizes industry-accepted best practices for all data communication and transmission activities and events. ScaleMatrix's principles for data communication and transmission ensure confidentiality, privacy, integrity, availability, and non-repudiation.

Network Logging

ScaleMatrix conducts logging activities on critical systems, and also reviews activity logs to identify any suspicious activity or anomalies within their network. All systems designated as part of a production solution are default monitored, and may not be commissioned without a monitoring solution being structured in support of the solution.

Network Monitoring

ScaleMatrix performs continuous monitoring of all mission-critical functions, including electrical power distribution, cooling functionality, humidity, personnel on premises, ticket response times, networking functionality, internet health and routing disparities, and internet traffic flowing through the ScaleMatrix systems. All internet traffic flowing through the ScaleMatrix systems is configured to be monitored by the ScaleMatrix security department, and checks exist to automatically mitigate DoS and DDoS attacks, both directly and via use of BGP communities with the ScaleMatrix upstream providers.

Monitoring exceptions are reported daily to managers, and weekly to senior managers. All critical exceptions are escalated as per written instructions to at least director-level personnel.

Firewalls

ScaleMatrix uses Cisco and Juniper Firewalls to protect all systems from intrusion attempts over the internet. All communications must pass through one or more firewalls, and the firewalls permit only traffic that is authorized (default deny rules). The placement of firewalls, firewall settings, and configurations are conducted by authorized personnel only.

Network Device Configuration

ScaleMatrix I.T. personnel are responsible for the appropriate setup, configuration, and maintenance of routers, switches, and all other network devices.

Hardening Procedures

All critical systems and components utilized internally by ScaleMatrix are appropriately configured for the purposes of ensuring maximum efficiency and reliability, while mitigating any security threats. All services running on equipment must be justified, or the services are removed and/or disabled at commissioning.

Anti-Virus

ScaleMatrix's program for virus protection consists of software loaded onto all critical systems that require protection, as well as related components within the organization. ESET NOD 32 is utilized throughout the organization for laptops and desktops, with a Barracuda appliance protecting the mail server, and the corporate gateway.

Physical Security & Environmental Security

Physical security elements are safeguards enacted to ensure only authorized individuals have access to various physical locations, such as movement within corporate facilities, along with access to data warehouses, computer operation centers, and any other critical locations.

Environmental security elements are the protective measures utilized to protect physical surroundings from damage elements, such as fire, water, smoke, electrical surges, spikes, outages, and any other hidden dangers. Environmental safeguards are implemented throughout ScaleMatrix's corporate facility for ensuring the safety of the employees, company property, and all other pertinent physical elements within proximity to the facility.

General Physical Security and Environmental Security Elements

The following physical security attributes are in place at the organization's facilities, located in San Diego, CA.

- Appropriate locks and access control mechanisms on all entry points
- Adequate lighting at night for all major areas of the facility
- Handicap accessible for physically impaired individuals (the elevator is not permitted for that use)
- Fire extinguishers placed in mission-critical areas
- Smoke detectors in mission-critical areas
- Video surveillance/closed-circuit video monitoring in place

Building Codes

The facility where ScaleMatrix is located has been built to meet or exceed all required building codes, complete with a Certificate of Occupancy being issued. Permits are required for any changes to the building infrastructure, thus the facility would be re-inspected for code compliance. Documented emergency exit plans exist and are displayed throughout the facility.

Visitors

All persons entering the data center are granted entry into the security lobby through the main facility entrance by Security or NOC personnel, who must physically unlock the front door. Entry is noted in the Visitor Log. Visitors are not allowed access to the facility beyond the lobby area until they have checked in, received a visitor badge, and are met by a designated employee who will escort them beyond the lobby area. Visitors are required to wear a visitor badge which must be affixed to the front of the body between shoulder and hip in a visible manner, and must be escorted at all times within the data center.

Sensitive and Critical Areas

Areas with sensitive documents, materials, and computer-related equipment and components are protected by locked doors, and can only be accessed by authorized personnel within ScaleMatrix.

Additional Noted Physical Security and Environmental Security Elements and Supporting Controls

- UPS systems are configured in a 2N service, which is continued as 2N to client
- Generators are properly sized to run the entire committed load
- Generator function is validated via third-party inspection
- Generators are supplied with adequate fuel for 24 hours of continuous operation at 100% load, assuming generator failures; with no assumption of failure, there is sufficient fuel for 48 hours at 100% maximum possible load.
- Generators are configured to permit failure of any single generator (N+1)
- Full end-to-end solution provides at least N+1 at each point with 2N inside the UPS perimeter
- Multiple air handlers and water chillers are in place to provide cooling redundancy (N+1 or N+2 depending)
- Third-party validation via inspection of the function of cooling solution
- Aggressive 24x7 SCADA monitoring and automatic alerting of exceptions
- SCADA controls system fully isolated from the internet
- Armed on-site security

- Security procedures are documented and followed, with exceptions reported for remediation
- Visitors are required to register and records are retained of all visitors for a period of at least one year
- All personally identifiable information (PII) gathered by security is protected with appropriate controls
- All persons on property are required to wear identification badges
- All entry controls past the untrusted front lobby require multiple layers of physical authentication; all other entrances are vestibule entrances which also require multiple layers of physical authentication.

Computer Operations

Computer operations elements consist of daily activities that help facilitate core operational components of any organization. Computer operations activities provide assurance that an organization performs critical functions relating to tape/media, system monitoring, patch management, and other ancillary activities.

Computer Operations Policies and Procedures

Documented policies and procedures are maintained in a user manual for general computer operations activities, such as tape/media backup policies and procedures.

Backup Process and Notification of Completions/Failures

Backups are conducted using a mix of manual and automatic systems, as described in the specifications for each solution. This method ensures that no more than one day's working data will be missing in the event of a data loss incident. Specifically, ScaleMatrix's backup procedures are as follows:

- All backups are to be mirrored between the San Diego and Houston offices, and all backups are to be maintained digitally in both locations for a period of three (3) years.
- All full backups will take place between the hours of 10PM and 5AM Pacific Time. This timeframe has been selected to minimize the impact of server downtime that may be caused by the need to take servers offline in order to perform the backup itself. If this backup schedule in some way interferes with a critical work process, then the affected user(s) is to notify the I.T. Department so that exceptions or alternative arrangements can be made.
- Image backups and flash backups will be taken every 15 minutes for tier one applications or on change of data.
- A full backup will be performed each night.
- A full backup will be performed at the end of each month to the monthly backup storage server. This backup will not be interacted with except during a declared DR event.
- All manual server backups performed must be noted in the server backup log immediately upon completion. All server backup log sheets must be kept in an appropriately labeled three-ring binder in an agreed-upon, centralized location. The log must include:
    - Server name
    - Date and time of backup
    - Name of administrator performing the backup
    - Files backed up and/or skipped
    - Software used to perform the backup
    - Backup medium used and its label/name
    - Whether the backup was successful or not
- If, for some reason, the backup crashes, cannot be completed, or is missed, then it must be completed by 9AM the following morning. The reason for non-completion of the originally scheduled backup must be noted in the server backup log and escalated as an exception. In addition, if a backup fails more than one day in a row, end users in the organization must be notified.

Warranties, Maintenance Agreements, and Service Agreements

All of ScaleMatrix's critical systems, components, and related hardware devices are covered by warranties and maintenance agreements, along with service agreements.

Maintenance and Patch Management

For internal Microsoft Windows systems, a server is currently used to push patches out from a central authority. Patches are first pushed to a test or development system, and are then evaluated after a 72-hour period. For internal Unix and Linux systems, patching is conducted via the Yum updating system, with patches first applied to development and pre-production servers, and then to production servers following an evaluation period. Lastly, networking systems are always patched manually, with patches first applied into a development or sandbox environment, which is fully separated from the production environments.

Software (Systems, Applications, and Utilities)

ScaleMatrix utilizes a mixture of proprietary-developed systems and applications, along with vendor-purchased systems and applications for helping administer and facilitate their core business processing transaction functions. As such, information systems, as well as all related hardware components and software applications, are routinely reviewed for ensuring maximum efficiency, along with validity and user appropriateness of all Information Technology components.

People (Developers, Operators, Users, and Managers)

ScaleMatrix is dedicated to providing accurate and timely information to critical decision processes for all of its clients. Management instills a philosophy that enables all employees to share in the success and growth of the company. A highly skilled and diverse group of employees comprise the organization's management team; these individuals are ultimately responsible for the vision and direction of ScaleMatrix. These members meet on a structured, routine basis to discuss a wide range of topics, and are also responsible for establishing policy and addressing all operational, financial, and social aspects of the organization. Employees are looked upon by management as "team players" who are instrumental in shaping and building an organization with high ethical standards, coupled with a unique, successful business model repossessions industry.

Furthermore, ScaleMatrix strives to build and foster a workplace environment which encourages communication and open forum discussions on a wide range of topics, technical issues for internal operations, and client needs, including ways to improve the internal corporate culture. Employees are routinely evaluated and given feedback from management regarding their professional skills, work habits, and attainment of goals. Teamwork is critical to ScaleMatrix's success, thus the organization is ready and willing to invest into each one of its valued employees.

"People" for which are instrumental for the daily operations of the Data Center Services system include the following:

- CEO
- CSMO
- CFO
- Additional I.T. Personnel, such as engineers and administrators

Procedures (Automated and Manual)

ScaleMatrix has in place numerous policy documents for purposes of establishing documented and formalized standards and procedures to be followed at all times throughout the organization. These policies are kept current by authorized personnel, are required to be read and acknowledged by all ScaleMatrix personnel, and form a critical component of the organization's adherence to the core concepts of confidentiality, integrity, and availability (CIA) of all system resources.

Data (Transaction Streams, Files, Databases, and Tables)

"Data" is defined as "The information used and supported by a system," and therefore includes specific customer information that is owned, operated, maintained, and/or controlled by ScaleMatrix within its Data Center Services system. As such, this report is limited to the controls in operation to support the operational infrastructure services as defined for its Data Center Services. The scope boundary includes specific systems residing in the ScaleMatrix's production environment.

Applicability of Report

This report has been prepared to provide information on ScaleMatrix's Data Center Services that may be relevant to the requirements of its customers to meet the Trust Services Principles for Security, Availability, Confidentiality, and Privacy. The report has been prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system which each customer may consider important. This report is limited to the controls in operation to support the operational services as defined in the ScaleMatrix Data Center Services scope boundary. Additionally, the authorized users of the system providing these services are limited to ScaleMatrix personnel.