Data Doc Imaging

Independent Service Auditor's Report on Controls at a Service Organization Relevant to Security(SOC 2, Type II) on the Imaging Services and Information Management System

For the period October 1, 2019 to December 31, 2020

An Independent Service Auditor Report issued by
Dixon Hughes Goodman LLP

table of contents

DIXON HUGHES GOODMAN LLP

section I: independent service auditor's report

To: Management of Data Doc Imaging
Charlotte, North Carolina

Scope

We have examined Data Doc Imaging's ("Data Doc") accompanying description of its Imaging Services and Information Management System found in Section III titled "management's description of its system and controls" throughout the period October 1, 2019 to December 31, 2020 (description) based on the criteria for a description of a service organization's system set forth in DC 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 Data Doc's controls stated in the description throughout the period October 1, 2019 to December 31, 2020, to provide reasonable assurance that Data Doc's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, processing integrity, and privacy (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Data Doc uses a subservice organization to provide IT Support Services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Data Doc, to achieve Data Doc's service commitments and system requirements based on the applicable trust services criteria. The description presents Data Doc's controls, the applicable trust services criteria, and the types of complementary subservice organization's controls assumed in the design of Data Doc'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 Data Doc, to achieve Data Doc's service commitments and system requirements based on the applicably trust services criteria. The description presents Data Doc's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Data Doc'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

Data Doc 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 Data Doc's service commitments and system requirements were achieved. In Section II, Data Doc has provided the accompanying assertion titled "management's assertion" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Data Doc is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and its 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.

DIXON HUGHES GOODMAN LLP

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 a 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 report users may consider important to meet their informational needs. There are inherent limitations in 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 or 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.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in Section IV of this report, "description of trust services criteria, related controls and results" of this report.

DIXON HUGHES GOODMAN LLP

Opinion

In our opinion, in all material respects,

- the description presents Data Doc's Imaging Services and Information Management System that was designed and implemented throughout the period October 1, 2019 to December 31, 2020 in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period October 1, 2019 to December 31, 2020 to provide reasonable assurance that Data Doc's service commitments and system requirements would be achieved based on the applicable trust services criteria, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Data Doc's controls throughout that period.
- the controls stated in the description operated effectively throughout the period October 1, 2019 to December 31, 2020 to provide reasonable assurance that Data Doc'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 Data Doc's controls operated effectively throughout that period.

DIXON HUGHES GOODMAN LLP

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Data Doc; user entities of Data Doc's Imaging Services and Information Management System during some or all of the period October 1, 2019 to December 31, 2020; business partners of Data Doc subject to risks arising from interactions with the Imaging Services and Information Management System; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and 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
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Dixon Hughes Goodman LLP

Charlotte, North Carolina

March 8, 2021

section II: management's assertion

We have prepared the accompanying description of Data Doc's Imaging Services and Information Management System titled "management's description of its system and controls" throughout the period October 1, 2019 to December 31, 2020 (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the Imaging Services and Information Management System that may be useful when assessing the risks arising from interactions with Data Doc's system, particularly information about system controls that Data Doc has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, processing integrity, and privacy (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Data Doc uses a subservice organization to provide IT Support Services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Data Doc to achieve Data Doc's service commitments and system requirements based on the applicable trust services criteria. The description presents Data Doc's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Data Doc'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, along with controls at Data Doc, to achieve Data Doc's service commitments and system requirements based on the applicable trust services criteria. The description presents Data Doc's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

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

1) The description presents Data Doc's Imaging Services and Information Management System that was designed and implemented throughout the period October 1, 2019 to December 31, 2020 in accordance with the description criteria.
2) The controls stated in the description were suitably designed throughout the period October 1, 2019 to December 31, 2020 to provide reasonable assurance that Data Doc's service commitments and system requirements would be achieved based on the applicable trust services criteria, if controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Data Doc's controls throughout that period.
3) The controls stated in the description operated effectively throughout the period October 1, 2019 to December 31, 2020 to provide reasonable assurance that Data Doc'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 Data Doc's controls operated effectively throughout that period.

Data Doc

section III: management's description of its system and controls

Information Regarding the System Description

The description of Data Doc's system provided in this report is specific to the procedures and processes in place at Data Doc's Charlotte location.

System Overview

Background

Data Doc is a leader in information management based in Charlotte, North Carolina. Data Doc has over three decades of knowledge and experience in processing information and data for a wide range of clients across the United States. Data Doc offers single source convenience and expertise on a full range of automated data storage and retrieval systems. Data Doc specializes in putting company data into today's varying formats.

Data Doc offers a variety of data management solutions:

- *Computer Output to Laser Disk* (COLD): COLD technology makes searching for information more efficient and less time consuming. Report files are easily indexed to optical media such as CD or DVD. This information is then viewed from the CD or DVD or downloaded to a client server. The information appears exactly as it would be printed on paper.

- *Computer Output Microfiche* (COM): COM is still proven to be one of the most cost effective and secure methods to archive data. The life expectancy of fiche is over 150 years. Because fiche is unalterable, secure, easy to read and economical it remains the storage solution of choice for many companies and government agencies.

- *Film Conversions:* DataDoc converts microfiche or microfilm (105mm, 35mm, 16mm film or aperture cards) to an electronic image. These images can then be loaded into any document management system for instant retrieval or saved as a PDF file for viewing and printing.

- *Document Management System:* DataDoc's document management system is scalable and can accommodate businesses of any size. The document management system locates and captures documents whether paper or digital format and organizes them in an efficient way. Using a consistent method and central depository for storing all documents greatly improves access to important business information, driving efficiency gains in virtually every process. Digital document management allows your employees to read, share and modify the same document, without the confusion of multiple versions. A centralized document depository integrates smoothly with your existing applications such as email, accounting, enterprise resource planning (ERP) and client relationship management (CRM) platforms, resulting in streamlined operations.

- *Document Scanning and Image Conversion*: This solution to information management provides Data Doc clients with the ability to scan and index their documents to a digital format. Their information is then readily available to them via a personal computer or network. This technology frees valuable floor space and eliminates misfiled documents.

- *Data Storage*: Data Doc provides clients with a secure way to store their terabytes of data. From short-term storage to long-term archive storage of mission critical data, Data Doc has been storing data for a diverse group of clients for over 30 years.

Infrastructure

System

Data Doc's network infrastructure is composed of a Microsoft Windows environment primarily consisting of 4 Windows servers. The FTP server stores data prior to processing while the other 3 servers handle processing the data or storage of the data post processing. Additionally, Data Doc runs dumb terminals connected to imaging devices (scanners, microfiche, etc.). DataDoc servers, workstations and equipment used in processing clients' information and data files are part of a closed segmented network using multi-layer firewall protection so that network and Internet access from any of these devices is not possible.

Software

Operations Software

Data Doc operates and supports software packages such as Microsoft Windows, FTP/SFTP, WSFTP, and FileZilla.

Security Software

Workstations are equipped with antivirus software. Antivirus software definitions are automatically updated to protect data from infection by malicious code or viruses.

People

Data Doc's management meets regularly to provide the overall direction of the company. Management plans and budgets on an annual basis. Data Doc, in Charlotte, has a staff of approximately 19 employees.

Procedures

Management has developed procedures to ensure the security of client data. These procedures include employee confidentiality and non-disclosure agreements, employee annual training, and limited operation of USB ports on local workstations

Imaging Services

Input data that is to be imaged is received from authorized client users via secure FTP connections to the Data Doc FTP server. Data Doc classifies all Information and data files received from their clients as highly confidential. Employees have signed the Data Doc confidentially form and understand they will be exposed to sensitive client data and are responsible for maintaining the security and integrity of such information.

Any release of data to which an employee may have access is a violation of Data Doc policy and will result in personnel action, and possible legal action. Data Doc client data is taken from the secured FTP using an automated

process via WSFTP. Data is then put into a client-specific location on the network using FileZilla. Team members are then notified that information is available for imaging.

Data

Data Doc's data includes client data in physical or digital form. Data Doc receives client data files via FTP or SFTP. The information is taken from the secured FTP using an automated process via WSFTP. Data is then put into a client specific location on the network using FileZilla where it is stored for 30 days then deleted.

Information Security policies have been implemented in order to protect the security of their critical client data, their computing resources, and their business interests. Data Doc considers all client information confidential and does not disclose client information to third parties, discontinue, or change confidentiality practices.

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring of Controls

Control Environment

Management Philosophy

A company's internal control environment reflects the overall attitude, awareness, and actions of management, the Board of Directors and others concerning the importance of controls and the emphasis given to controls in the company's policies, procedures, methods and organizational structure.

Ethical and behavioral standards have been established, communicated, and reinforced through normal management activities and documented policies and procedures. Corporate control activities include the following:

- Organizational policy statements and codes of conduct are documented and communicate management's intended values and behavioral standards.
- Employee policies and procedures contain organizational policy statements and codes of conduct to which all employees are required to adhere.
- Policies and procedures are in place for handling confidential information and complying with applicable laws, regulations, and corporate requirements.
- Employees are required to agree not to disclose proprietary or confidential information, including guest information, to unauthorized parties.
- Employees are required to sign an acknowledgement form indicating they have read the Data Doc Employee Handbook and understand their responsibility for adhering to the established rules, terms, policies and procedures, and conditions.

Each employee is instructed to report any suspected violation or exception to these policies by other employees or clients.

Security Management

Data Doc is organized to manage its services and internal operations so that client and internal needs are met and external compliance is achieved. The organization is hierarchical, which is conducive to control through segregation of responsibilities.

Security Policies

Policies are reviewed and approved by management annually, are maintained on the intranet, and are available to all employees.

Personnel Security

Personnel policies and procedures are documented in the Data Doc Employee Handbook. Background and reference checks are performed for sensitive positions that warrant such investigations prior to being hired. New employees are required to review the Data Doc Employee Handbook that contains policies relating to the confidentiality of client data. New employees acknowledge their acceptance of the policies by signing a confidentiality agreement and acknowledgement of the information security policies and returning it to management. A termination checklist is used by the HR department to initiate the process to remove both logical and physical access for terminated employees.

Physical Security and Environmental Controls

Access to Data Doc's facility and data center is restricted to authorized individuals. Exterior doors require keypad to enter the facility. Visitors to the facility and data center are required to sign a guest log, and be escorted by a Data Doc employee. Security cameras are strategically placed at external and internal entry point locations. These cameras are monitored 24 hours per day 7 days per week. An independent security company monitors the alarm system 24 x 7.

The following environmental controls have been implemented to help protect the facility and data center:

- Uninterruptible power supply (UPS)
- Air conditioning
- Fire suppressions systems
- Emergency Lighting

Change Management

Change management encompasses all changes to hardware, software, or applications in the shared IT infrastructure. This includes modification, changes, or additions to the network services (LAN/WAN), and computer hardware and software. Any significant or high risk changes are subject to formal change management procedures. Change requests are documented by the change requestor and reviewed by management. Changes are promoted into the production environment after being authorized by an appropriate person.

System Monitoring

Firewalls are utilized to provide segmentation between the network and the Internet. Access to administer the firewall is restricted to network administrators. File Transfer Protocol (FTP) servers reside in a demilitarized zone (DMZ) that is separate from the internal network but is protected by external and internal firewalls.

The Windows operating system is kept current through the use of Windows updates. Security patches are regularly monitored, tested and implemented when appropriate.

Operating system, firewall and intrusion prevention system (IDS) logs are reviewed to detect unauthorized access attempts to the Data Doc network.

Problem Management

Security incidents and other IT related problems are reported to management. Issues are tracked and monitored until resolved.

Data Backup and Recovery

Data backups are scheduled and monitored on a regular basis. Backups at Data Doc are performed daily using Windows backup server to back up the Windows operating systems locally. The backups are stored on a local drive and rotated offsite monthly.

System Account Management

Security policies and procedures have been documented and communicated throughout the organization. Policies are updated and employees are required to train and sign off annually. Access to the network and applications is granted to authorized personnel by management. New user access, changes to user access and removal of user access follows a formal process where system privileges are authorized by managers via the use of a User Access Request Form. Reviews of user access privileges are performed annually by management.

Administrative access to Windows Active Directory is restricted to authorized employees.

Password parameters, including the required minimum length, periodic password expiration and account lockout have been implemented to provide control over authentication.

Risk Assessment Process

Management conducts ongoing risk evaluation and develops risk mitigation strategies within its various functional departments on an ongoing basis to identify, analyze, and manage risks that could adversely affect operations. Events and changes that potentially impact operations are evaluated immediately by management to determine their impact on the company's risk profile and to services provided to clients. Management's involvement in daily operations allows them to learn about risks related to operations through direct personal involvement with employees and outside parties.

Information and Communication

To help align business strategies and goals with operating performance, management is committed to maintaining effective communication with all personnel. Data Doc has documented policies, procedures, and guidelines which establish minimum safeguards, assign roles and responsibilities, provide accountability, and address penalties for noncompliance. Data Doc policy and procedure is communicated to all relevant personnel by Human Resources when they are hired and annually thereafter.

Monitoring of Controls

Management is involved in periodic meetings in order to discuss the status of service delivery or other matters that impact client service. Issues or suggestions identified by personnel are readily brought to the attention of management to be addressed and resolved. Management monitors compliance with established policies, procedures, laws and regulations to which the company is subject. Management monitors the control environment to consider whether controls are operating as intended and that control activities are modified appropriately for changing conditions. Continuous monitoring activities are in place to assess the quality of internal control over time. Corrective actions are initiated through company meetings, department meetings, client conference calls, and informal notifications as needed.

Applicable Trust Services Criteria

Although the trust services criteria and related controls are presented and tested in Section IV, "Trust Services Security Principle, Criteria, Related Controls and Tests of Controls", Data Doc notes that the circumstances that warrant the operation of control activities designed to meet Criteria 6.2.1, 7.4.1, 8.1.2, 8.1.3, 8.1.4 did not occur during the report period because no users changed roles, no security incident's occurred and no significant, high risk or emergency changes were performed at Data Doc. Data Doc further notes that due to the size and non-complex structure of the company, controls to meet criteria 1.2 are not applicable. Data Doc ownership maintains control over day-to day-operations and internal control.

Trust Services Criteria and Related Controls

The Company's applicable Trust Services Criteria and related controls are included within Section IV of this report. Although the applicable Trust Services Criteria and related controls are presented within Section IV, they are, nevertheless, an integral part of the Company's description of Its System as described within this section.

Complementary Subservice Organization Controls and Monitoring

Data Doc's controls related to its system covers only a portion of overall internal control for each user entity of Data Doc. It is not feasible for the applicable trust services criteria related to Data Doc's system to be achieved solely by Data Doc. Therefore, each user entity's internal controls must be evaluated in conjunction with Data Doc's controls and the related tests and results described in Section IV of this report, considering the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Subservice Organization	Service(s) Provided	Relevant Criteria Addressed
Apex3 Solutions	A service provider used for IT Support Services. The following control groupings are critical to achieving the applicable control objectives: • The subservice organization is responsible for maintaining controls over Network support and monitoring In addition, Data Doc has identified the following controls to help monitor the subservice organization: • Monitoring daily activity reports and working closely with the subservice organization to maintain controls.	CC 3.0 CC 4.0 CC 6.0 CC 7.0 CC 8.0

Complementary User Entity Controls

Data Doc's services are designed with the assumption that certain controls will be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report. Data Doc's management makes control recommendations to user organizations and provides the means to implement these controls in many instances. Data Doc also provides best practice guidance to Data Docs regarding control elements outside the sphere of Data Doc responsibility.

This section describes additional controls that should be in operation at user organizations to complement the Data Doc controls. The list of user organization control considerations presented below do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Therefore, each Data Doc's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

Complementary User Entity Controls (CUECs)	Related Criteria
User entities are responsible for ensuring the confidentiality of any user IDs and passwords assigned to them for use with Data Doc Secure FTP.	CC 6.1
User entities are responsible for immediately notifying Data Doc of any actual or suspected information security breaches.	CC 7.3, 7.4
User entities are responsible for understanding and complying with their contractual obligations to Data Doc.	CC 2.2, 2.3
Users are responsible for notifying Data Doc of changes made to contact information in a timely manner.	CC 2.2, 2.3

section IV: description of trust services criteria, related controls and results

A. INFORMATION PROVIDED BY DIXON HUGHES GOODMAN LLP

This report, including the description of tests of controls and results thereof in Section IV of this report, is intended solely for the information and use of the Company, user entities of the Company's System during some or all of the Specified Period, those prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the Company;
- How the Company's System interacts with user entities, subservice organizations, or other parties;
- Internal control and its limitations;
- Complementary user entity controls and how they interact with related controls at the Company to meet the Applicable Trust Services Criteria;
- The Applicable Trust Services Criteria; and
- The risks that may threaten the achievement of the Applicable Trust Services Criteria and how controls address those risks.

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

This report, when combined with an understanding of the user control considerations in place at user locations, is intended to assist user organizations in assessing control risks.

The scope of our testing of the Company's controls was limited to the controls specified by the Company contained in Section IV of this report. Management believes these are the relevant key controls for the stated criteria. Other than specifically identified controls related to subservice organizations as described in Sections III and IV, our review was not extended to controls in effect at the user organizations, subservice organizations, or third-party vendors.

B. TYPES AND DESCRIPTION OF THE TESTS OF OPERATING EFFECTIVENESS

Various testing methods are used to assess the operating effectiveness of controls during the Specified Period. The table below describes the various methods which were employed in testing the operating effectiveness of controls that are in place at the Company.

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Type	Description
Inquiry	Inquired of appropriate personnel and corroborated with management
Observation	Observation of the application, performance, or existence of the control
Inspection	Inspection of documents and reports indicating performance of the control

C. TRUST SERVICES CRITERIA, CONTROLS, TESTS PERFORMED AND RESULTS OF TESTING

The following matrices describe the Company's controls and the testing performed to determine whether the controls were suitably designed and were operating effectively throughout the period to meet the criteria.

Criteria Group 1: Common Criteria Related to Control Environment

CC 1.0 Common Criteria Related to Control Environment			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.1	**The entity demonstrates a commitment to integrity and ethical values.**		
1.1.1	Personnel are required to read and accept the code of conduct and statement of confidentiality and privacy practices upon their hire.	Selected a sample of new employees and verified that they had signed the organizations confidentiality policy.	No Exceptions Noted.
1.1.2	Personnel must pass a criminal background check before they may be hired by the entity.	Selected a sample of new employees and verified that background checks had been performed.	No Exceptions Noted.
CC 1.2	**The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.**		
1.2.1	Criteria 1.2.1 not applicable		
CC 1.3	**Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**		
1.3.1	The entity has an organizational chart that defines organizational structures, reporting lines, authorities, and responsibilities.	Inspected the organization chart to verify that Data Doc has established an organizational structure to align authority, responsibility, and segregation of duties to appropriate personnel.	No Exceptions Noted.
CC 1.4	**The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**		
1.4.1	The experience and training of candidates for employment or transfer are evaluated before they assume the responsibilities of their position.	Inquired of personnel responsible for the design, development, and operation of systems regarding their qualifications, resumes, certifications, job history and resources available to fulfill their responsibilities.	No Exceptions Noted.
CC 1.5	**The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**		
1.5.1	Data Doc has defined roles and responsibilities in written job descriptions.	Inspected an example of defined roles and responsibilities in written job descriptions.	No Exceptions Noted.

Criteria Group 2: Common Criteria Related to Information and Communication

CC 2.0 Common Criteria Related to Information and Communication			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.1	**The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.**		
2.1.1	System descriptions are available to authorized external users that delineate the boundaries of the system and describe relevant system components as well as the purpose and design of the system. Documentation of the system description is available to authorized clients via the entity's client-facing website.	Inspected a network diagram and inquired of management to determine system boundaries are illustrated to clients.	No Exceptions Noted.
CC 2.2	**The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**		
2.2.1	Procedures exist that instruct security commitments to internal system users in the event of a breach.	Inspected Data Doc's Information Security Policy to verify a description of the system and its boundaries are in place and communicated to authorized users.	No Exceptions Noted.
2.2.2	Personnel are required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon hire and annually thereafter.	Obtained and reviewed a sample of employees to verify that they had read and accepted the code of conduct and the statement of confidentiality and privacy practices upon hire and annually thereafter.	No Exceptions Noted.

CC 2.0 Common Criteria Related to Information and Communication			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.3	**The entity communicates with external parties regarding matters affecting the functioning of internal control.**		
2.3.1	Personnel are required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon hire and annually thereafter.	Obtained and reviewed a sample of employees to verify that they had read and accepted the code of conduct and the statement of confidentiality and privacy practices upon hire and annually thereafter.	No Exceptions Noted.
2.3.2	Policy and procedures documents for significant processes are available to employees.	Inspected relevant policies and procedures to ascertain the policies were reviewed and approved. Inspected documentation from the period to verify a formal sign-off of the policy by the President.	No Exceptions Noted.
2.3.3	Policy and procedures documents for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so), are published and available to employees.	Inspected Incident Response Procedures to ascertain procedures exist for the identification and escalation of incidents and security breaches.	No Exceptions Noted.

Criteria Group 3: Common Criteria Related to Risk Assessment

CC 3.0 Common Criteria Related to Risk Assessment			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 3.1	**The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.**		
3.1.1	Management performs an assessment at least annually to identify the information required and expected to support the internal control and the achievement of service commitments and system requirements.	Inspected the Data Doc Information Security Risk Assessment and determined that it identifies the information required to support internal controls and the achievement of service commitments and system requirements.	No Exceptions Noted.
CC 3.2	**The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.**		
3.2.1	Firewalls, and routers are utilized by Information Technology. Reports from the firewall are monitored for suspicious activity and alerts are configured to send emails. Management tracks mitigations for medium and high-risk alerts.	Inquired of management to determine if IDS, firewalls, and routers are utilized by Information Technology. Inspected network diagrams to determine if appropriate devices are in place to secure the network.	No Exceptions Noted.
CC 3.3	**The entity considers the potential for fraud in assessing risks to the achievement of objectives.**		
3.3.1	Firewalls, and routers are utilized by Information Technology. Reports from the firewall are monitored for suspicious activity and alerts are configured to send emails. Management tracks mitigations for medium and high-risk alerts.	Inquired of management to determine if IDS, firewalls, and routers are utilized by Information Technology. Inquired of management to determine if remediation of medium and high-risk alerts are retained. Inspected configuration of firewall alerts to confirm emails are produced for review.	No Exceptions Noted.
CC 3.4	**The entity identifies and assesses changes that could significantly impact the system of internal control.**		
3.4.1	Management performs an assessment at least annually to identify the information required and expected to support the internal control and the achievement of service commitments and system requirements.	Inspected the Data Doc Information Security Risk Assessment and determined that it identifies the information required to support internal controls and the achievement of service commitments and system requirements.	No Exceptions Noted.

Criteria Group 4: Common Criteria Related to Monitoring Activities

CC 4.0 Common Criteria Related to Monitoring Activities			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 4.1	**The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.**		
4.1.1	Monitoring software is used to identify and evaluate ongoing system performance, changing resource utilization needs, and unusual system activity. This software sends a message to the assigned personnel for investigation and resolution when specific predefined thresholds are met.	Obtained and reviewed procedures for remediation of medium and high-risk incidents.	No Exceptions Noted.
CC 4.2	**The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective actions, including senior management and the Board of Directors, as appropriate.**		
4.2.1	Operations and security personnel follow defined protocols for resolving and escalating reported events.	Obtained and reviewed system scan configurations and the system scan issues log.	No Exceptions Noted.
4.2.2	Operations and security personnel follow defined protocols for resolving and escalating reported events.	Obtained and inspected documented procedures for reporting security incidents.	No Exceptions Noted.

Criteria Group 5: Common Criteria Related to Control Activities

CC 5.0 Common Criteria Related to Control Activities			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.1	**The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.**		
5.1.1	Management performs an assessment at least annually to identify the information required and expected to support the internal control and the achievement of service commitments and system requirements.	Inspected the Information Security Risk Assessment and determined that it identifies the information required to support internal controls and the achievement of service commitments and system requirements.	No Exceptions Noted.
CC 5.2	**The entity also selects and develops general control activities over technology to support the achievement of objectives.**		
5.2.1	Management performs an assessment at least annually to identify the information required and expected to support the internal control and the achievement of service commitments and system requirements.	Inspected the Information Security Risk Assessment and determined that it identifies the information required to support internal controls and the achievement of service commitments and system requirements.	No Exceptions Noted.
CC 5.3	**The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**		
5.3.1	Operations and security personnel follow defined protocols for resolving and escalating reported events.	Obtained and inspected documented procedures for reporting security incidents.	No Exceptions Noted.

Criteria Group 6: Common Criteria Related to Logical and Physical Access Controls

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.1	**The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.**		
6.1.1	Only unique IDs are used on the Network. Each unique ID is assigned to an employee upon their completion of a signed employee agreement.	Inspected user IDs in the Windows network application to determine if each user has a unique ID.	No Exceptions Noted.
		Inspected user IDs in the Windows network application that was assigned the administrator attribute to determine if access is commensurate with job responsibilities.	
6.1.2	Access to system components requires a documented access request form and manager approval prior to access being provisioned.	Inspected access request forms for a sample of new hires that received access to the system components to determine if an access provisioning request was approved prior to access being provisioned.	Exceptions Noted – documentation was not completed for the sampled new hires.
CC 6.2	**Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.**		
6.2.1	Employee access to protected resources is created or modified by the security group based on an authorized change request from the system's asset owner.	Inspected user lists and inquired of management to determine if only authorized information security personnel create changes or delete user profiles within the network.	No Exceptions Noted.
		Inquired of management to determine that no employee required access or departmental change during the period.	DHG determined there were no changes during the period.

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.3	**The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.**		
6.3.1	Password complexity standards are established to enforce control over access.	Obtained and inspected network password and account configurations settings to determine if authentication parameters conform to Data Doc's defined standard setting requirements.	No Exceptions Noted.
CC 6.4	**The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.**		
6.4.1	User access requests for a specific role are approved by the user manager and are reviewed at least annually.	Inspected new user lists and selected a sample of new hires to determine if access request forms were appropriately approved prior to access being provisioned.	Exceptions noted – documentation was not completed for the sampled new hires.
CC 6.5	**The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.**		
6.5.1	Formal data retention and disposal procedures are in place to guide the secure disposal of the company's and customers' data.	Inspected data retention and disposal procedures to determine procedures are in place.	No Exceptions Noted.
6.5.2	The facility is secured via the following controls: 1. A locked door with keypad entry. 2. Surrounded with a barbed wire fence. 3. Live feed cameras that are monitored 24/7 by a third party. 4. Appropriate environmental controls (HVAC and fire suppression). 5. Installed and Operational UPS.	Observed the facility and inquired of management to determine appropriate physical protections are in place.	No Exceptions Noted.

CC 6.0 Common Criteria Related to Logical and Physical Access Controls			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.6	**The entity implements logical access security measures to protect against threats from sources outside its system boundaries.**		
6.6.1	External points of connectivity are protected by a firewall. The firewall alerts are monitored by Data Doc daily and a third party 24/7.	Inspected firewall and alerting configurations to determine appropriate monitoring is in place.	No Exceptions Noted.
CC 6.7	**The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.**		
6.7.1	VPN, SSL, secure file transfer program (SFTP), and other encryption technologies are used for defined points of connectivity and to protect communications between the processing center and users connecting to the processing center from within or external to customer networks. USB access is restricted.	Inquired of management as to the use of encryption to transfer confidential customer information and protect user authentication information. Obtained and inspected screenshots of encryption on each applicable device.	No Exceptions Noted.
CC 6.8	**The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.**		
6.8.1	Antivirus software is installed on workstations, laptops, and servers supporting such software.	Inspected AV definitions reports to determine all machines are covered.	No Exceptions Noted.

Criteria Group 7: Common Criteria Related to System Operations

CC 7.0 Common Criteria Related to System Operations			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.1	**To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.**		
7.1.1	Monitoring software is used to identify and evaluate ongoing system performance, changing resource utilization needs, and unusual system activity. This software sends a message to the assigned personnel for investigation and resolution when specific predefined thresholds are met.	Inspected monitoring dashboards to determine system performance, resource utilization, and system activity is actively being monitored.	No Exceptions Noted.
7.1.2	Firewalls, and routers are utilized by Information Technology. Reports from the firewall are monitored for suspicious activity and alerts are configured to send emails.	Inquired of management to determine if IDS, firewalls, and routers are utilized by Information Technology. Inquired of management to determine if remediation of medium and high-risk alerts are retained. Inspected configuration of firewall alerts to confirm emails are produced for review.	No Exceptions Noted.

CC 7.0 Common Criteria Related to System Operations			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.2	**The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.**		
7.2.1	Daily incremental backups are performed using an automated system.	Inspected software settings to confirm infrastructure and software monitoring tools have been implemented. Obtained and inspected documentation of successful daily backups.	No Exceptions Noted.
CC 7.3	**The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.**		
7.3.1	Operations and security personnel follow defined protocols for resolving and escalating reported events	Obtained and reviewed system scan configurations and the system scan issues log. Obtained and inspected documented procedures for reporting security incidents.	No Exceptions Noted.
CC 7.4	**The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.**		
7.4.1	Operations and security personnel follow defined protocols for resolving and escalating reported events.	Obtained and inspected applicable policies and procedures to confirm defined protocols for resolving and escalating reported events.	DHG determined no security events occurred during the period.
CC 7.5	**The entity identifies, develops, and implements activities to recover from identified security incidents.**		
7.5.1	Daily incremental backups are performed using an automated system.	Inspected documentation of completed backups.	No Exceptions Noted.

Criteria Group 8: Common Criteria Related to Change Management

CC 8.0 Common Criteria Related to Change Management			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 8.1	**The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.**		
8.1.1	Significant or high-risk system change requests are evaluated to determine the potential effect of the change on security commitments and requirements throughout the change management process.	Inspected the Information Security Policy to verify a formal change management process is in place.	No Exceptions Noted.
8.1.2	High risk or significant system change requests that affect security are required to have a change ticket created.	Selected a sample of high risk or significant system changes for the application and operating system environments to determine if documentation and approvals relating to the changes were documented.	DHG determined there were no high risk or significant system changes during the period.
8.1.3	High risk or significant system change requests must be reviewed and approved by the owner of the infrastructure or software prior to work commencing on the requested change.	Selected a sample of high risk or significant system changes for the application and operating system environments to determine if documentation and approvals relating to the changes were documented and only authorized personnel have the ability to make changes.	DHG determined no such incidents took place during the period.
8.1.4	For high severity incidents, a root cause analysis is prepared and reviewed by management. Based on the root cause analysis, change requests are prepared and controls are updated to reflect the planned incident and problem resolution.	Inspected Change Management Policy and the Incident response procedures to determine appropriate procedures are in place.	DHG determined no such incidents took place during the period.

Criteria Group 9: Common Criteria Related to Risk Mitigation

CC 9.0 Common Criteria Related to Risk Mitigation			
Control No.	**Control Activity Description**	**Tests Performed by Service Auditor**	**Results of Testing**
CC 9.1	**The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.**		
9.1.1	Management performs an assessment at least annually to identify the information required and expected to support the internal control and the achievement of service commitments and system requirements.	Inspected the Data Doc Information Security Risk Assessment and determined that it identifies the information required to support internal controls and the achievement of service commitments and system requirements.	No Exceptions Noted.
CC 9.2	**The entity assesses and manages risks associated with vendors and business partners.**		
9.2.1	Information sharing agreements are in place with key related parties and vendors. These agreements include the scope of services and security commitments applicable to that entity.	Inspected third party subservice organization contract and determined that it identifies the information required to support internal controls and the achievement of service commitments and system requirements.	No Exceptions Noted.