360ADVANCED

SOC 2® TYPE 2 REPORT ON CONTROLS RELEVANT TO SECURITY AND AVAILABILITY FOR DATA CENTER SERVICES

DATABANK HOLDINGS, LTD.

OCTOBER 1, 2018 TO SEPTEMBER 30, 2019

DATABANK

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations™

DATABANK HOLDINGS, LTD.
Table of Contents

SECTION 1:

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To DataBank Holding, Ltd.:

Scope

We have examined the accompanying description of DataBank Holding, Ltd.'s ("DataBank") Data Center Services system throughout the period October 1, 2018 to September 30, 2019, 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*), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2018 to September 30, 2019, to provide reasonable assurance that DataBank'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*).

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

DataBank's management 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 DataBank's service commitments and system requirements were achieved. DataBank's management has provided the accompanying assertion titled "Management's Assertion" included in Section 2 of this report about the description and the suitability of design and operating effectiveness of controls stated therein. Management 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 a description of a service organization's system and the suitability of the design and operating effectiveness of the 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 conclusion about the suitability of the design or operating effectiveness of 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 presented in Section 4 of this report.

Basis for Modified Opinion

The accompanying description of the DataBank Data Center Services system includes controls tested at the locations in which the Data Center Services system operate. The tests of operating effectiveness of controls did not extend to the Atlanta, Georgia location as that facility was not operating for a period long enough within the examination period to evaluate and opine on the effectiveness of those controls.

Opinion

In our opinion, except for the matter described in the preceding paragraph, in all material respects:

a. the description presents DataBank's Data Center Services system that was designed and implemented throughout the period October 1, 2018 to September 30, 2019, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period October 1, 2018 to September 30, 2019, to provide reasonable assurance that DataBank's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if user entities applied the complementary controls assumed in the design of DataBank's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period October 1, 2018 to September 30, 2019, to provide reasonable assurance that DataBank's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of DataBank's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of DataBank, user entities of DataBank's Data Center Services system during some or all of the period October 1, 2018 to September 30, 2019, business partners of DataBank subject to risks arising from interactions with the Data Center Services 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, and other parties
- Internal control and its limitations
- Complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- 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 these specified parties.

December 2, 2019
St. Petersburg, Florida

SECTION 2:

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

December 2, 2019

We have prepared the accompanying description of DataBank Holding, Ltd.'s ("DataBank") Data Center Services system throughout the period October 1, 2018 to September 30, 2019, 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*). The description is intended to provide report users with information about the Data Center Services system that may be useful when assessing the risks arising from interactions with DataBank's system, particularly information about system controls that DataBank 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 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*).

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

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

a. the description fairly presents DataBank's Data Center Services system that was designed and implemented throughout the period October 1, 2018 to September 30, 2019, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period October 1, 2018 to September 30, 2019, to provide reasonable assurance that DataBank's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the user entities applied the complementary controls assumed in the design of DataBank's controls throughout that period.

c. Except for the matter described in paragraph d. below, the controls stated in the description operated effectively throughout the period October 1, 2018 to September 30, 2019, to provide reasonable assurance that DataBank's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary sub-service organization controls (if applicable) and complementary user entity controls assumed in the design of DataBank's controls operated effectively throughout that period.

d. We understand that the testing of controls, for purposes of determining that controls within our description were suitably designed and placed into operation, was performed for the Atlanta Georgia facility; however, due to the short operational period of the facility during the examination period (45 days), the Service Auditor's opinion could not be extended to the operating effectiveness of controls at the Atlanta Georgia facility.

/s/ DataBank Holding, Ltd.

Kevin Ooley – President and Chief Financial Officer

Mark A. Houpt – Chief Information Security Officer

SECTION 3:

DATABANK'S DESCRIPTION OF CONTROLS

SCOPE OF REPORT AND DISCLOSURES

Overview

This description of the system of controls provided by DataBank Holding, Ltd.'s ("DataBank") management, as related to Standards for Attestation Engagements No. 18 '*Attestation Standards: Clarification and Recodification*', specifically AT-C Section 105, '*Concepts Common to All Attestation Engagements*' and AT-C Section 205, '*Examination Engagements*,' considers the direct and indirect impact of risks and controls that DataBank's management has determined are likely to be relevant to its user entities' internal controls intended to mitigate risks related to security, availability, processing integrity, confidentiality, or privacy.

Trust Services Categories and Related Criteria

The five attributes of a system are known as *categories*, and they are defined as follows:

- *Security*: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

  Security refers to the protection of

  i. information during its collection or creation, use, processing, transmission, and storage and

  ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

- *Availability*: Information and systems are available for operation and use to meet the entity's objectives.

  Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

- *Processing Integrity*: System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

  Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether the system achieves the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation. Because of the number of systems used by an entity, processing integrity is usually only addressed at the system or functional level of an entity.

- *Confidentiality*: Information designated as confidential is protected to meet the entity's objectives.

  Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

- *Privacy*: Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.

Although the confidentiality criteria applies to various types of sensitive information, privacy applies only to personal information.

The privacy criteria are organized into eight categories:

a. *Notice and communication of objectives.* The entity provides notice to data subjects about its objectives related to privacy.

b. *Choice and consent.* The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.

c. *Collection.* The entity collects personal information to meet its objectives related to privacy.

d. *Use, retention, and disposal.* The entity limits use, retention, and disposal of personal information to meet its objectives related to privacy.

e. *Access.* The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.

f. *Disclosure and notifications.* The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy.

g. *Quality.* The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its objectives related to privacy.

h. *Monitoring and enforcement.* The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

The trust services criteria may be used when evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability, or processing integrity of information and systems, or the confidentiality or privacy of the information processed by the entity. As such, they may be used when evaluating whether the entity's controls were effective to meet the criteria relevant to any of those categories, either individually or in combination with controls in other categories.

Scope

The scope that management has determined appropriate for the Data Center Services system includes the controls to meet the applicable trust services criteria. Management is responsible for identification of risks associated with the system of controls, and for the design and operation of controls intended to provide reasonable assurance that the applicable trust services criteria would be met.

As part of its overall SOC 2® program, DataBank management sets and determines the scope and timing of each report. This description of the system has been prepared by DataBank management to provide information on controls applicable to meet the criteria for the Security and Availability principles at the 16 Databank data center locations listed on the following page:

The scope of this examination included the cloud, managed, and co-location services for the following set of locations:

- Dallas, Texas (2) DFW1, and DFW3
- Lenexa, Kansas (3) MCI1, MCI2, and MCI3
- Eagan, Minnesota (1) MSP2
- Baltimore, Maryland (1) BWI1

The scope of the examination for co-location services included all of the above locations, plus the following additional locations:

- Richardson, Texas (1) DFW2
- Edina, Minnesota (1) MSP1
- Salt Lake City, Utah (1) SLC1
- Bluffdale, Utah (3) SLC2, SLC3, and SLC4
- Pittsburgh, Pennsylvania (1) PIT1
- Cleveland, Ohio (1) CLE1
- Atlanta, Georgia (1) ATL

Sub-Service Organizations

DataBank does not rely on any sub-service organizations as part of the Data Center Services system included in the scope of this report.

Significant Changes during the Examination Period

During to the period of this examination, DataBank's Atlanta (ATL1), Kansas City #3 (MCI3), and Salt Lake City #4 (SLC4) data centers went live. These locations were included in the scope of the report. The opening dates for these locations were:

- MCI3, May 2019
- SLC4, July 2019
- ATL1, August 2019

Subsequent Events

Management is not aware of any relevant events that occurred subsequent to the period covered by management's description included in Section 3 of this report through the date of the service auditor's report that would have a significant effect on management's assertion.

System Incidents

Management is not aware of any system incidents that resulted in a significant failure in the effectiveness of controls or the achievement of the service commitments or system requirements during the period covered by management's description included in Section 3 of this report.

Using the Work of the Internal Audit Function

The service auditor did not utilize any work of an Internal Audit function in preparing this report.

OVERVIEW OF OPERATIONS AND THE SYSTEM

Company Overview and Background

DataBank is a provider of information technology Data Center Services to commercial, governmental, and not-for-profit customers across the United States. DataBank maintains its headquarters in Dallas, Texas and has data center facilities throughout the United States. DataBank facilities are designed to provide customers with 100% uptime for their critical business IT infrastructure. With redundant power delivery, multi-homed multi-terabyte Internet access hubs, and storage area networks, DataBank's Data Center Services offerings include customized technology solutions designed specifically to help organizations manage their risk and improve their overall business performance.

Overview of the Data Center Services system

Overviews of DataBank's Data Center Services, are as follows:

Databank's Dedicated and Cloud Hosting

DataBank provides customers with dedicated and cloud hosting services defined by custom service agreements. Dedicated and cloud hosting services may include system administration, network administration, system monitoring, and customer support. DataBank applies these services to the technology infrastructure and supports the software hosted at DataBank data center facilities.

As necessary, DataBank also provides implementation of standard vendor-supplied system changes into the operating environment.

DataBank Managed Services

DataBank offers several add-on options to its standard cloud hosting or co-location services. Examples of optional managed services include data / system backup, data / system recovery, firewall administration and management, and customer-defined security and operational monitoring.

DataBank Co-location

DataBank provides its customers the option to fully manage their own information technology environment while it is hosted at DataBank's data center facilities. In its co-location services offering, DataBank maintains the physical access controls to its data center facilities and provides Internet bandwidth while the customer assumes the other ongoing support and management responsibilities. Co-location services may be bundled with certain aspects of its managed service offering, and as a result, in some cases, DataBank may have administrative access to customer systems.

Principal Service Commitments and System Requirements

DataBank describes the services and the scope of work provided to their customers through documented Master Service Agreements and Terms of Use. Security processes and obligations are also described on their website. Service responsibilities are documented and agreed upon by both DataBank and their customers before services are provided.

DataBank's management designs its processes and procedures related to Data Center Services system to meet its security and availability objectives. Those objectives are based on the service commitments that DataBank's management makes to user entities, the laws and regulations that govern the provision of Data Center Services system and the financial, operational, and compliance requirements that DataBank has established for the services. The Data Center Services system of DataBank are subject 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 DataBank operates. Certain systems within the Data Center Services system of DataBank are subject to the security requirements of the Payment Card Industry Data Security Standard (PCI DSS), as well as state privacy security laws and regulations in the jurisdictions in which DataBank operates.

Security commitments are standardized and include, but are not limited to, the following:

- Data centers with guards, cameras, biometric entry prevent physical incursions
- Redundant Tier 1 Internet carriers connected to border routers and firewalls filter known threats
- A variety of perimeter protections to cloud services hosts
- DataBank's security team works to craft rules to prevent false positives
- Anti-virus software combined with a host intrusion prevention system and central reporting

OVERVIEW OF RELEVANT INFRASTRUCTURE

The Data Center Services system is comprised of the following components:

- Infrastructure – the physical structures, IT, and other hardware
- Software – the application programs and IT system software that supports application programs
- People – the personnel involved in the governance, operation, and use of a system
- Procedures – the automated and manual procedures
- Data – transaction streams, files, databases, tables, and output used or processed by the system

Infrastructure

The DataBank data centers offer facilities and infrastructure to provide Data Center Services for its customers. Each facility is designed with data halls where customer equipment resides. Single racks, cabinets, and / or isolated cages are offered to customers within the several thousand square feet of data hall space at each facility.

The following describes the in-scope components supporting the Data Center Services system:

System / Application	Description
ScienceLogic	Network monitoring
Nagios	Network monitoring
WebCTRL	Environmental monitoring
Benchmark Automation	Environmental monitoring
Lenel OnGuard	Physical access system
Net2	Physical access system
HandNet	Physical access system
HP Insight Manager	HP Server Monitoring
Dell Open Manage	Dell Server Monitoring

Software

DataBank also utilizes Nagios or ScienceLogic to provide for network and system monitoring of the data center facilities and services contracted to be provided. Nagios or Science Logic is the primary application used for monitoring services (depending upon location) and has been configured with thresholds and alerts designed to provide support and management notifications with enough time to adjust and make changes prior to an outage or limitation in services being provided.

The other applications listed in the table above are also used to monitor and safeguard the systems.

People

The roles and responsibilities of key functions include the following:

- **Chief Executive Officer (CEO)**: Raul Martynek serves as the CEO of DataBank. He joined DataBank in June of 2017 as the Chief Executive Officer. In this role, he provides overall strategic direction of the company and its operations. Mr. Martynek is a 20+ year veteran in the telecom and Internet Infrastructure sector. He most recently served as a Senior Advisor for Digital Bridge Holdings LLC. Prior to Digital Bridge, he served as Chief Executive Officer for New Jersey-based data center and managed services operator Net Access, LLC. Net Access was acquired in November 2015 by Denver-based data center operator Cologix. Prior to Net Access, he was the CEO of Voxel dot Net, Inc., a global managed hosting, and cloud company, which was acquired by Internap Network Services Corp. in early 2012. Mr. Martynek also served as the Chief Restructuring Officer of Smart Telecom, a Dublin, Ireland-based fiber carrier which was acquired by Digiweb in 2009. Before that he evaluated investment opportunities in the telecommunications and Internet sector as a Senior Advisor at Plainfield Asset Management, a $4B hedge fund. Prior to Plainfield, Mr. Martynek spent 13 years with telecom and Internet provider InfoHighway Communications Corp.; first as a Chief Operating Officer of Eureka Networks and then as President and Chief Executive Officer of InfoHighway. InfoHighway was acquired by Broadview Networks in 2007. Mr. Martynek earned a Bachelor of Arts in Political Science from Binghamton University and received a Master's Degree in International Affairs from Columbia University School of International and Public Affairs.

- **President and Chief Financial Officer (CFO):** Kevin Ooley has served as the CFO of DataBank since 2011. He has over 20 years of extensive experience in delivering shareholder value through the creation and implementation of growth and operational strategies. Prior to joining DataBank, Mr. Ooley served as the CFO for the Thompson Media Group and as a Principal at Lovett Miller & Co., a growth capital private equity firm based in Florida. He was also the Director of Strategy for iXL Enterprises and a Manager in Accenture's Strategic Services practice. Mr. Ooley holds a Bachelor of Industrial Engineering from the Georgia Institute of Technology.

- **Chief Technology Officer (CTO)**: Vlad Friedman is a seasoned IT veteran with over 25 years of mission-critical IT experience. Mr. Friedman joined the DataBank management team as CTO in September 2017 with the acquisition of Edge Hosting. In his current role as DataBank's Chief Technology Officer, Vlad guides the direction for development, implementation, and management of the company's overall technology strategies. Prior to DataBank, Mr. Friedman founded and served as CEO of Edge Hosting, a compliance-driven IaaS, and PaaS Managed Cloud Hosting service provider, in 1998 as a spin-off from his first IT venture ACS, which was started in 1991 while he was still a student at the University of Maryland. ACS was a software startup that created the only packaged solution for large scale automotive logistics processing that was widely adopted by auto manufacturers, port processors and transportation carriers around the globe. Under Mr. Friedman's direction, Edge Hosting flourished to thousands of servers in geographically diverse data centers, hosting highly secure, mission-critical hosting for web and line-of-business applications.

- **EVP of Corporate Development**: Justin Puccio joined the company's senior leadership team as Executive Vice President of Corporate Development in mid-2017 with a 20 year track-record of industry accomplishments. Mr. Puccio leads the company's growth strategy and acquisition efforts. Prior to joining DataBank, Mr. Puccio served as a Director for Signal Hill, a tech-focused investment bank where he helped launch the internet infrastructure practice and managed several successful prominent industry transactions. Prior to Signal Hill, Mr. Puccio served as President and Founder of Satori Networks, Inc., a telecommunications research firm specializing in consulting services, industry research, and complex network builds. Mr. Puccio also possesses diverse expertise in wholesale and enterprise technology applications, carrier relations, and corporate management, which stems from his roles in regional executive management at OnFiber Communications and Eureka Networks, and sales with Level 3 and MCI. Mr. Puccio graduated from Middlebury College.

- **Senior Vice President of Sales**: Stephen Callahan adds to the DataBank collective experience in cloud, hosting, data center, and telecommunications services. He brings over 20 years of executive sales leadership to the DataBank Executive team. In his role as Senior Vice President of Sales, Mr. Callahan is responsible for guiding DataBank's sales operations, sales programs, and channel strategy. Prior to DataBank, Mr. Callahan served as the SVP of Sales for New York-based Packet Host. Previous to Packet Host, he was the SVP of Sales and Marketing for Cologix, formerly Net Access. He also served as SVP - Global Sales at Internap Network Services Corporation, and as a Board Member of Internap Japan, where he originally joined in the acquisition of Voxel dot Net, a global managed hosting and cloud company, where he served as SVP of Sales and Marketing. In addition, Mr. Callahan has also held a number of senior sales leadership roles with MCI (now Verizon Business), eLink Communications, Eureka GGN, InfoHighway Communications and Broadview Networks. Mr. Callahan received his B.A. in History and Economics from Muhlenberg College.

- **CISO:** Mark A. Houpt joined DataBank in September of 2017 with the acquisition of Edge Hosting. Mr. Houpt has over 25 years of extensive information security and information technology experience in a wide range of industries and institutions. Mr. Houpt holds an MS-ISA (Masters Information Security and Assurance), numerous security and technical certifications (CISSP, CCSP, CEH, CHFI, Security +, Network+) and qualified for DoD IAT Level III, IAM Level III, IASAE Level II, CND Analyst, CND Infrastructure Support, CND Incident Responder, and CND Auditor positions and responsibilities. Mr. Houpt is an expert in understanding and the interpretation of FedRAMP, HIPAA, and PCI-DSS compliance requirements. Mark is an active member of ISC2, ASIS International, COMPTIA, IAPP, and ISACA, among other leading national and international security organizations. Mr. Houpt drives DataBank's information security and compliance initiatives to ensure that the company's solutions continuously meet rigorous and changing compliance and cyber-security standards. Mr. Houpt is responsible for developing and maintaining the company's security program roadmap and data center compliance programs.

- **Co-Founder & Strategic Account Sales:** As co-founder, Jerry Blair was instrumental in DataBank's inception in 2005. In his current role, Blair is charged with executing on the company's sales strategy. With a successful track record spanning more than 20 years in senior sales management, Mr. Blair's experience and proven ability to implement results-driven direct and channel-focused sales programs is a very welcome continued asset to the company. Prior to DataBank, Mr. Blair was Vice President of Sales for Switch and Data and LayerOne. He has also served as General Manager of Sales for Lucent Technologies and has held sales management positions with various industry leaders including ICG Communications, Nortel Communications and Wellfleet Communications.

Procedures

DataBank is responsible for maintaining and implementing information technology general computer controls related to computer processing supporting the Data Center Services. These controls provide the basis for reliance on information / data from the systems used by user entities for financial reporting.

Physical Security

DataBank security systems include badge and biometric access authentication at each data center door, logging of door access attempts, and video surveillance for access to and within the DataBank data centers common areas including access doors and passage ways. Electronic badge access systems and biometric hand readers provide access controls at each facility's data center entry points. Video surveillance technology has been implemented to monitor and record access to and activity within the common areas of the facilities.

The properties are constructed of reinforced concrete and structural steel poured in place with concrete decking present between floors. The exterior walls consist of precast concrete panels, and common face brick and limestone. Electronic badge access systems and biometric readers provide access controls at data centers' entry points including at each data hall entrance. Certain data halls within the data centers offer raised flooring space for customer equipment. Customer equipment may be maintained in separate, secured and locked steel cages or cabinets.

Physical access to facilities is typically restricted to colocation customers. Cloud Hosting services customers would access systems virtually.

Customers designate two or more persons with the ability to modify an authorized access list and provide the name, driver's license number, e-mail address and phone number of each employee that requires access. Authorized persons with badge and biometric access may have up to 24 hour per day access to customer space within their respective data hall only. Customers are required to provide advanced noticed of escorted or one-time access for vendors and employees. Visitors are required to check in at the security guard station, sign the visitor log, and exchange a driver's license for a temporary access card or escort. Security personnel are either onsite or monitoring via video surveillance 24 hours per day. Video surveillance cameras at each location are supported by systems which retain at minimum 90 days of video activity.

DataBank has digital video systems in place at each of their facilities; these video systems monitor movement into and throughout the common shared spaces of the facilities . The video system is motion-sensitive and records any movement in its line of sight. The digital video systems are configured to retain activity logs for a minimum of 90 days.

Environmental Security

Power Capabilities

The aspects and elements of the power delivery system are configured in a redundant design. The power is distributed via separate alternate current (AC) transformers feeding automatic switching gear. DataBank has deployed redundant generators to support both uninterruptible power supply (UPS) system loads and the associated cooling loads. IT load is protected by multiple redundant UPS systems. The watts per square foot provided for IT load are based on cooling capacity, and the ability to maintain an acceptable temperature in the event of a computer room air handler (CRAH) unit failure. DataBank installs new generators and UPS systems as customer orders and capacity dictate.

Fire Suppression and Cooling

DataBank employs a double inter-lock, dry-pipe fire suppression system with photoelectric detectors tied to a single fire panel.

DataBank employs multiple cooling infrastructures across their facilities, including open and closed loop condenser water systems, closed loop glycol based high capacity cooling systems, and air-cooled chiller systems. The cooling systems are configured with redundancies to ensure adequate delivery and circulation of cool air.

Monitoring

Environmental monitoring systems are utilized to monitor the environmental conditions and devices throughout each facility. The environmental monitoring systems are configured to notify security and data center personnel through e-mail alerts when predefined thresholds are exceeded on monitored devices. The systems use devices throughout the facilities to monitor temperature, humidity, and leak detection.

Customer Provisioning

DataBank utilizes Master Service Agreements (MSAs) to define the terms of services provided by DataBank to each customer. DataBank documents the agreed upon services and communicates these service requirements to customers via a Completion Notice. The notification includes a description of services and contact information for reporting problems.

A "Provisioning Form" with initial customer system specifications is completed. Based on the requirements defined by the contract, DataBank may need to purchase the required systems or equipment support the customer organization, including hardware, support software, digital certificates, or data circuits.

Senior Management reviews the Provisioning Form. The Network Engineering staff members enter the preliminary information from the form onto the specific checklist needed for the implementation, choosing either the dedicated and cloud hosting checklist or the co-location checklist. Once Engineering personnel have completed the initial part of the checklist, they open an internal ticket and assign it to Project Management or Senior Management for review. At this point, the Client Services Team compares the Provisioning Form with the executed contract to ensure that contractual obligations are addressed, and that the implementation plan checklist matches the Provisioning Form.

After review by the Client Services Team, the Engineering staff sets up the new system(s) according to the implementation checklist. They document the actual project implementation details on either the dedicated and cloud hosting checklist or the co-location checklist. The completed checklists are stored electronically.

The engineering staff then opens another ticket to send the primary contact person the introductory implementation information, turning over their login credentials and thus making it a live implementation for the customer. However, customers are ultimately responsible for final approval and acceptance of their new implementation.

System Availability

DataBank has designed its network and has implemented monitoring controls to provide a highly available operating state for its customers. Policy and procedure manuals are in place and maintained for internal network infrastructure availability, backup, and recovery.

The facilities feature multiple redundant high-capacity Internet connections providing high availability to customers, regardless of service level, through the use of gigabit Ethernet Internet connections and redundant Gigabit/10, as well as Gigabit Ethernet point-to-point connections between the facilities, providing diverse paths into the data centers.

Change Management

DataBank performs hardware, operating system, and specific managed service changes on behalf of its customers upon receipt of a properly authorized request.

To understand the process for submission and tracking of customer-requested changes, please refer to the Ticket System section of this report.

DataBank is occasionally required to perform emergency hardware, operating system, and other specific managed changes on behalf of its dedicated and cloud hosting, co-location, and managed services customers. This typically occurs as a result of continuous monitoring functions and activities for high-risk alerts that DataBank determines can only be fixed by implementing a change. Such alerts arise from external security vulnerabilities, issues with hardware, services (for instance, protocols such as HTTP, FTP, SMTP, and DNS), power supply, and availability.

Customer organizations are ultimately responsible for controls that ensure the appropriate approval of changes they have requested DataBank to make to their environment. The customer is also responsible for controls over the implementation of and changes to business process software applications within their hosted, managed, or co-located system.

DataBank installs standard vendor-supplied operating system updates (commonly known as patching) for dedicated and cloud hosting customers. The Security Engineering staff monitors communications and updates from operating system vendors notifying DataBank that updates are available from their web sites.

Information Security

Access to the company network is restricted to organizational workstations and other approved devices. Unique accounts requiring user name and password are required to access workstations. Passwords to log on to user accounts are managed by Active Directory (AD) and maintain minimum length and complexity requirements.

Remote support of customer systems can be performed through use of a VPN. User name and password are required for employees to authenticate to the secure VPN.

DataBank uses commercially available firewall appliances for Managed Services (Firewall) customer systems. DataBank monitors and manages logical access to the managed firewalls on both a preventative and a detective level through the use of detective controls, processes, and technology.

DataBank also maintains firewall logging (syslog) servers at each location that receive continuous (24 x 7 x 365) logs of firewall activity. They are configured to retain a minimum of 90 days of activity, with the oldest day continuously overwritten by the log. The firewalls are configured to log informational and higher severity-level events and send them to the syslog server.

Backup Processes

DataBank's standard backup configuration for managed and cloud hosted services is to automatically perform daily backups of customer systems. Colocation customers receive no backups unless contracted. Deviations from the standard backup configuration are performed at the request of the customer. Customers' production data and operating system files are automatically backed up daily on an incremental basis and weekly on a full basis. Operations staff members use various commercially available backup software systems depending upon a customer's needs.

Backup jobs are configured to send either daily reports or real-time error notifications to DataBank's Engineering and Operations staff. Engineering staff members monitor the error notifications and start a ticket to notify the Engineering staff to review the operations log from the backup servers to diagnose the issue. If necessary, the Engineering Staff completes a ticket to document backup job restarts and corrections and route the ticket as appropriate based on the nature of the relationship with the customer.

Network Monitoring

Network monitoring is performed by DataBank to monitor the availability of network connections to customers hosted in DataBank facilities. DataBank management has documented the incident response policies and procedures in place to guide personnel in network outage response, escalation, and resolution activities.

DataBank utilizes an enterprise monitoring application to monitor the status of the networking systems provided to DataBank customers. The monitoring application monitors considerations such as, availability of the network, host services and ports, IP packet transmissions and loss. The enterprise monitoring application is configured to send e-mail alert notifications to IT personnel when predefined thresholds are exceeded on monitored systems and provides statistical reports to monitoring personnel. The monitoring personnel of DataBank are available 24x7 to monitor and resolve networking issues affecting DataBank customers. A ticketing system is utilized to manage system incidents, response, and resolution.

Data

DataBank does not process customer's data. Physical and logical access to customer systems containing customer data is limited to support personnel necessary to have such access and with permissions granted by the customer.

RELEVANT ASPECTS OF CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATIONS SYSTEMS, MONITORING, POLICIES AND PRACTICES

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal controls, providing discipline and structure. Aspects of DataBank's control environment that affect the services provided and / or the system of controls are identified in this section.

Integrity and Ethical Values

The effectiveness of controls is greatly influenced by the level of integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are crucial elements of DataBank's control environment, affecting the design, administration, and monitoring of other components. The communication and implementation of ethical behavior throughout the organization is designed to reduce the likelihood of personnel to engage in dishonest, illegal, or unethical acts.

DataBank enforces high ethical standards in the levels of communication to and through its employees. DataBank continuously audits its employees' communication with customer and outside resources to ensure compliance with these standards and addresses any issues as soon as they arise. DataBank emphasizes high standards during all of its interpersonal communications via meetings, email, and phone calls. Any questionable acts are dealt with immediately and positive acts are recognized and acknowledged in public forums in an effort to reinforce positive / constructive behaviors. Employees who violate these standards are disciplined according to company policies. Ethical standards specifically addressing security functions and needs have been developed and are communicated in a "Rules of Behavior" format.

Board of Directors

DataBank's control consciousness is influenced significantly by its Board of Directors. The Board communicates strategy, risk management, and operational objectives through quarterly board meetings. The objectives of the organization and communicated through Management Committee. Attributes include the Management Committee's experience and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management, and its interaction with internal and external auditors. The Management Committee was formed to oversee DataBank's risk management ownership and accountability. The committee consists of members of senior management from different operational areas including finance, executive oversight, engineering and operations, and business development. The committee identifies elements of business risk including threats, vulnerabilities, safeguards, and the likelihood of a threat, to determine the actions to be taken.

Commitment to Competence

Management has established a framework for the basic skills necessary to perform each of the jobs at DataBank. This framework is then augmented with more specific requirements for each position and for additional specialization within each position based upon any other skills an employee may have. The job descriptions for each position are descriptive, but remain fairly broad because of the nature of the work for which each position is responsible. The employee understands that there are general skills that all people within their given role must have and that the job description augments those skills. A skills development program is in place that provides technical training for the continued development of information technology and engineering personnel. Training practices include vendor training for support specific hardware and software components, conferences, and seminars on industry developments, technical certification courses, and newsletters and discussion forums for certain technologies.

Management's Philosophy and Operating Style

DataBank management philosophy and operating style is ultimately responsible for the system of internal controls. Virtually all employees have some role in controlling the organization. Some controls are established at the organization level, and management of the local unit establishes others. Management has formal policies and procedures in place to guide personnel on specific information processing functions.

Organizational Structure

Management has designed the organizational structure to provide quality service and accountability in support of DataBank's mission. In order to achieve quality in performance, they strive for continuous improvement in all that is done, plan and commit to accomplish targets, and are empowered to perform their duties. DataBank's operations are highly specialized and require the ability to adapt to industry changes and best practices. DataBank has a centralized, flat management framework, which allows them to quickly react to industry changes and have excellent response times to customer needs. In addition, the CEO is an active participant in day-to-day operations and managers' report directly to him. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are available to personnel via the intranet.

Human Resource Policies and Practices

DataBank's human resource policies and practices are clearly written and communicated where appropriate. Policies and procedures that are listed in the employee handbook include hiring, training, disciplinary actions, and termination procedures.

Risk Assessment

DataBank is committed to managing and minimizing risk by identifying, analyzing, evaluating, and treating exposures that may hinder, prevent, or otherwise impact the organization from achieving its goals. DataBank recognizes the need for risk management as a strong consideration in strategic and operational planning, day-to-day management and decision making at all levels in the organization.

The CISO is charged with development, implementation, and maintenance of the risk management strategy, with standards adopted from NIST SP 800-37. The CISO is also responsible for the dissemination of the corporate Risk Assessment policy at least annually, or with any changes. Annually, the organization performs a risk assessment which includes a risk ranking considering likelihood of occurrence and impact.

Annually, or as significant changes are made within the organization that affect risks, the executive management team reviews the risk assessments and plans appropriate mitigating action plans. Risk assessments at minimum address the following:

- Unauthorized access
- Malicious or unintended use of access control credentials
- Unauthorized disclosure
- Loss of or Disruption of services
- Modification or destruction of the information system

Information and Communication Systems

Information System

Databank has an information security policy to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time sensitive information and processes for security and system availability purposes that notify key personnel in the event of potential security issues or system outages.

Communication System

Management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities. This includes the ability to provide necessary training to the extent that personnel understand how their daily activities and roles relate to the overall support of services. DataBank management believes that open communication throughout the organization ensures that deviations from standards are identified, reported, and appropriately addressed.

DataBank has implemented an internal corporate network to disseminate information to employees. The network is the central repository for company communications. Individual departments are charged with designing and developing their procedures. Once a procedure is finalized, it is published to the internal network for company-wide distribution. Publishing to the corporate network is performed by information technology personnel who follow a two-step process to help ensure that changes are approved prior to release to the production site. Restrictive access controls are also applied if the material being published is not intended for general viewing (e.g., certain fee structures and management guidelines).

Ticketing System

DataBank has developed a number of means to manage customer communication and information sharing with customers; however, the most commonly used mechanism for collecting information that may be relevant to the customer is the DataBank Portal, an online ticket system.

The DataBank Portal ticket system is a web-based application that provides customers with the ability to submit issues or requests for changes to their account including changes to existing systems and orders for new services. To ensure that only authorized requests are accepted, each user is assigned a unique user ID and required to set a confidential password prior to being granted access. Multi-Factor authentication via a one-time password function is offered for customers that desire a high degree of integrity in their portal experience. Once an authorized service request is received via the ticket system, an email is automatically sent to the requester with the service request number confirming DataBank's receipt, and the request is then assigned to the appropriate team's queue. The team associated with the queue receives notification that a new request has been submitted to the queue. The request is assigned to the appropriate team member, who attempts to resolve the request. If additional information is required, the customer is contacted via the ticket, and the request is put on hold until the information is received thus creating a continual journal of dialogue and actions. The ticket system provides DataBank with the ability to formally capture documentation related to the request, confirmation of receipt, work performed, and the review and approval of tickets related to customers' systems.

This system is also used internally by DataBank to record alerts that are generated by monitoring software installed on customer hardware devices and to document the resolution of any issues with hardware or software related to the internal network infrastructure.

Monitoring

DataBank's management performs monitoring activities in order to assess the quality of internal control over time and monitors activities throughout the year and takes corrective actions to address deviations from company policy and procedures. Management utilizes a risk-based approach to monitor business units and other auditable entities throughout the organization, ensuring that enterprise-wide risks are prioritized and addressed in order of significance.

Management's close involvement in operations helps to identify significant variances from expectations regarding internal controls. Upper management immediately evaluates the specific facts and circumstances related to any suspected control breakdowns. A decision for addressing control's weaknesses is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. Management's ability to actively monitor customer's communications is an integral role in controlling the quality of the services provided.

The CEO holds regular meetings with the team managers to maintain oversight of team activities and company financial positioning.

Weekly operations and senior management meetings are held to discuss monitoring activities, issues, and other relevant topics pertaining to the operation of the Data Center and Managed Services. Monitoring activities are used to initiate corrective action through meetings, calls, and informal notifications.

Management has frequent involvement in DataBank's operations to help identify significant variances from expectations regarding internal controls. Controls addressing higher-priority risks and those most essential to reducing a given risk are evaluated more often. Additionally, DataBank's customer care group ensures that customer complaints are brought to management's attention in weekly senior management and operations meetings. Executive management immediately evaluates the specific facts and circumstances related to any suspected control breakdowns. A decision for addressing any controls weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel.

CATEGORIES, CRITERIA, AND RELATED CONTROLS

The categories, criteria, and related controls are included in Section 4 of this report, “Categories, Criteria, Related Controls and Tests of Operating Effectiveness”, to eliminate the redundancy that would result from listing them in this section and repeating them in Section 4. Although the criteria and related controls are included in Section 4, they are, nevertheless, an integral part of the organization’s description of controls.

COMPLEMENTARY CONTROL CONSIDERATIONS

DataBank's policies and procedures over its Data Center Services system cover only a portion of the overall internal control for each user entity. It is not feasible for DataBank's service commitments and systems requirements related to the Data Center Services system to be solely achieved by DataBank. DataBank's control policies and procedures were designed with the assumption that certain controls would be in place and in operation at the user entities. User entity internal controls must be evaluated, taking into consideration DataBank's controls and their own internal controls. DataBank's management does not make any representations regarding responsibility related to, or provide any assurance in regards to any such internal control or regulatory requirements for which the client must assess or comply.

This section describes some of the control considerations for the user entities, or "complementary controls", which should be in operation at the user entities to complement the controls at the service organization. User auditors / user entities should determine whether the user entities have established controls to ensure that the criteria within this report are met. The "complementary controls" presented below should not be regarded as a comprehensive list of all controls that should be employed by the user entities.

Control Considerations for User Entities

Physical Security

1. User entities are responsible for determining whether DataBank's security infrastructure is appropriate for its needs and for notifying DataBank of any requested modifications.
2. User entities are responsible for establishing and adhering to security procedures to prevent the unauthorized or unintentional use of facilities, information systems and infrastructure.
3. User entities are responsible for providing and maintaining a list of authorized personnel, vendors, and contractors as well as changes to technical or administrative contact information.
4. User entities are responsible for notifying DataBank of on-site visits of vendors and contractors prior to their arrival at a data center. Failure to follow procedures will result in denied access.
5. User entities are responsible for notifying DataBank of terminated employees with access to the DataBank data centers within a timely manner.
6. User entities are responsible for ensuring their cages, racks, and cabinets are locked and their equipment is secured prior to leaving the premises.

Network Monitoring

7. User entities are responsible for creating and communicating specific escalation procedures for problems with their services and for notifying DataBank of changes to their escalation procedures.

Customer Provisioning

8. User entities are responsible for securing appropriate approval of new implementation.
9. User entities are responsible for establishing logical access controls to limit their employees' access to DataBank's ticket system for the purposes of requesting any changes to customer environments and requesting changes to physical access controls.
10. User entities are responsible for providing and maintaining a list of authorized customer contacts with the ability to initiate changes to subscribed services.

System Availability and Monitoring

11. User entities are responsible for maintaining network connectivity between the customer and DataBank's network.
12. User entities are responsible for initiating any requests for DataBank to verify it has met the agreed-upon levels of availability for a given month.

Change Management

13. User entities are responsible for obtaining appropriate approval of customer-requested changes to their environment(s).
14. User entities are responsible for implementing and changing business process software applications.
15. User entities are responsible for providing updated contact information for their designated primary and secondary emergency-level contact personnel.
16. User entities are responsible for providing updated contact information for their designated primary and secondary standard version update contact personnel for Managed Service systems.
17. User entities are responsible for obtaining appropriate approval of security-related emergency changes within Managed Service systems.
18. User entities are responsible for notifying DataBank if it chooses to opt out of standard version updates for Managed Service systems.
19. User entities are responsible for requesting any modifications to the existing access control lists (ACLs) or firewall policies within Managed Service systems.
20. User entities are responsible for providing specific workstation and/or network addresses it authorizes to access system management ports within Managed Service systems.

Information Security

21. User entities are responsible for monitoring user accounts and administrative activity on customer systems at DataBank.
22. User entities are responsible for establishing logical access controls that define authorizations and security profiles within Hosted and Managed Service systems and for ensuring the assignment of users to these profiles.
23. User entities are responsible for creating, maintaining, and disseminating their own Information Security Policy for their environment(s).

Backup Processes

24. User entities are responsible for requesting data restorations through the ticket system for Managed Service systems.
25. User entities are responsible for securing approval of restorations for Managed Service systems.

SECTION 4:

CATEGORIES, CRITERIA, CONTROL DESCRIPTIONS, RELATED CONTROLS AND TESTS OF OPERATING EFFECTIVENESS

INFORMATION PROVIDED BY THE SERVICE AUDITOR

Introduction

This report is intended to provide user entities, prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding with information about controls that may affect the Data Center Services system provided by DataBank and to provide information about the operating effectiveness of controls that were tested.

The scope of our testing of DataBank's controls was limited to the categories, criteria, and the related controls specified by DataBank's management and contained within Section 4 of this report, which management believes to be the relevant key controls for the categories and criteria included in the scope of this report.

The examination was performed in accordance with the American Institute of Certified Public Accountants ("AICPA") Standards for Attestation Engagements No. 18 '*Attestation Standards: Clarification and Recodification*', specifically AT-C Section 105, "*Concepts Common to All Attestation Engagements*' and AT-C Section 205, '*Examination Engagements*.' It is each interested party's responsibility to evaluate this information in relation to controls in place at user entities and sub-service organizations (if applicable) to obtain an overall understanding of internal control and to assess control risk. Controls in place at user entities, sub-service organizations (if applicable), and DataBank's controls must be evaluated together. A general, but not inclusive, listing of control considerations is provided in Section 3, "Complementary Control Considerations." If an effectively operating user entity or sub-service organization (if applicable) internal control is not in place, the controls at DataBank may not sufficiently compensate the deficiency.

Tests of Operating Effectiveness

Our tests of the operating effectiveness of the controls specified by DataBank's management included such tests as we considered necessary in the circumstances to obtain reasonable, but not absolute, assurance that the controls operated in a manner that achieved the specified criteria during the period from October 1, 2018 to September 30, 2019. In selecting particular tests of the operating effectiveness of controls we considered 1) the nature of the controls being tested; 2) the types and completeness of available evidential matter; 3) the nature of the criteria to be achieved; 4) the assessed level of control risk; 5) the expected efficiency and effectiveness of the test; and, 6) the testing of other controls relevant to the criteria.

Testing exceptions, if any, and information about specific tests of the operating effectiveness performed that may be relevant to the interpretation of testing results by user entities, prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding for the controls specified to achieve the criteria are presented in this section under the column heading "Results of Testing." The concept of materiality is not applied when reporting the results of the tests of controls for which exceptions have been identified because the independent service auditor does not have the ability to determine whether an exception will be relevant to a particular user entity. Consequently, 360 Advanced, Inc. reports all exceptions. Exceptions identified herein are not necessarily considered significant deficiencies or material weaknesses in the total system of internal controls of DataBank, as this determination can only be made after consideration of controls in place at user entities. Control considerations that should be exercised by DataBank's clients in order to complement the controls of DataBank to attain the criteria are presented in relation to the nature of services being audited and the controls specified by DataBank management.

Types of Tests Performed

The table below describes the nature of our audit procedures and tests performed to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Test Types	Description of Tests
Inquiry	Inquired of appropriate personnel seeking relevant information or representation to obtain the following information about the control: ➢ Knowledge and additional information regarding the policy or procedure; and ➢ Corroborating evidence of the policy or procedure.
Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: ➢ Examination / Inspection of source documentation and authorizations to verify transactions processed; ➢ Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures; ➢ Examination / Inspection of systems documentation, configurations and settings; and ➢ Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.
Observation	Observed the implementation, application or existence of specific controls as represented
Re-performance	Re-performed the control to verify the design and / or operation of the control activity as performed

Procedures for Assessing Completeness and Accuracy of IPE

For tests of controls requiring the use of Information Provided by the Entity (IPE) (e.g., controls requiring system generated populations for sample-based testing), 360 Advanced, Inc. performed a combination of the following procedures, where possible, based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspected the source of the IPE, (2) inspected the query, script, or parameters used to generate the IPE, (3) tied data between the IPE and the source, and/or (4) inspected the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintained its integrity. In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), the independent service auditor inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Sampling Methodology

The table below describes the sampling methodology utilized in our testing to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Type of Control and Frequency	Minimum Number of Items to Test (Period of Review Six Months or Less)	Minimum Number of Items to Test (Period of Review More than Six Months)
Manual control, many times per day	At least 25	At least 40
Manual control, daily (Note 1)	At least 25	At least 40
Manual control, weekly	At least 5	At least 10
Manual control, monthly	At least 3	At least 4
Manual control, quarterly	At least 2	At least 2
Manual control, annually	Test annually	Test annually
Application controls	Test one operation of each relevant aspect of each application control if supported by effective IT general controls; otherwise test at least 15	Test one operation of each application control if supported by effective IT general controls; otherwise test at least 25
IT general controls	Follow guidance above for manual and automated aspects of IT general controls	Follow guidance above for manual and automated aspects of IT general controls

Notes: 1.) Some controls might be performed frequently, but less than daily. For such controls, the sample size should be interpolated using the above guidance. Generally, for controls where the number of occurrences ranges from 50 to 250 during the year, our minimum sample size using the above table should be approximately 10% of the number of occurrences.

CATEGORIES, CRITERIA, AND RELATED CONTROLS

Security (Common Criteria to All Categories)

Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC1.0 Control Environment			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	Inquired of the Chief Information Security Officer to verify that organizational charts were in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	No exceptions noted.
		Inspected the DataBank Organizational Chart to verify that organizational charts were in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	No exceptions noted.
CC1.1.2	Information security and availability policies and procedures are documented, approved, and maintained by management, and available to guide personnel. The policies include, but are not limited to the following: ➢ Information Sensitivity ➢ Physical Security ➢ Environmental Security ➢ Incident Response	Inquired of the Compliance Engineer, to verify that information security and availability policies and procedures were documented, approved, and maintained by management, and available to guide personnel. The policies include, but were not limited to the following: ➢ Information Sensitivity ➢ Physical Security ➢ Environmental Security ➢ Incident Response	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the information security policy and incident response plan to verify that information security and availability policies and procedures were documented, approved, and maintained by management, and available to guide personnel. The policies include, but were not limited to the following: ➢ Information Sensitivity ➢ Physical Security ➢ Environmental Security ➢ Incident Response	No exceptions noted.
CC1.1.3	Background screenings are performed for employment candidates as a component of the hiring process.	Inquired of the Compliance Engineer to verify that background screenings were performed for employment candidates as a component of the hiring process.	No exceptions noted.
		Inspected background screenings for a sample of employees on-boarded during the examination period to verify that background screenings were performed for employment candidates as a component of the hiring process.	No exceptions noted.
CC1.1.4	Personnel are required to read and accept the physical security policy, information security policy, employee guide and confidentiality agreement as part of the on-boarding process.	Inquired of the Compliance Engineer to verify that personnel were required to read and accept the physical security policy, information security policy, employee guide and confidentiality agreement as part of the on-boarding process.	No exceptions noted.
		Inspected the signed policy acknowledgments and confidentiality agreements for a sample of employees on-boarded during the examination period to verify that personnel were required to read and accept the physical security policy, information security policy, employee guide and confidentiality agreement as part of the on-boarding process.	No exceptions noted.
CC1.1.5	Documented policies and procedures for significant processes are available to personnel on Databank's shared document repository.	Inquired of the Compliance Engineer to verify that documented policies and procedures for significant processes were available to personnel on Databank's shared document repository.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the DataBank Knowledge Base to verify that documented policies and procedures for significant processes were available to personnel on Databank's shared document repository.	No exceptions noted.
CC1.1.6	DataBank maintains a documented Information Security Policy which expresses sanctions that can be applied for non-compliance with the policy.	Inquired of the Compliance Engineer to verify that DataBank maintained a documented Information Security Policy which expressed sanctions that could be applied for non-compliance with the policy.	No exceptions noted.
		Inspected the Information Security Policy and Standards Manual to verify that DataBank maintained a documented Information Security Policy which expressed sanctions that could be applied for non-compliance with the policy.	No exceptions noted.
CC1.1.7	Procedure for reporting threats, incidents and violations is described in the Employee Handbook.	Inquired of the Compliance Engineer to verify that a procedure for reporting threats, incidents and violations was described in the Employee Handbook.	No exceptions noted.
		Inspected the Employee Handbook to verify that a procedure for reporting threats, incidents and violations was described in the Employee Handbook.	No exceptions noted.
CC1.2 COSO Principle 2: The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	Individuals outside of the organization are appointed as members of the Board of Directors to maintain independent oversight of executive responsibilities.	Inquired of the Compliance Engineer to verify that individuals outside of the organization were appointed as members of the Board of Directors to maintain independent oversight of executive responsibilities.	No exceptions noted.
		Inspected the active list of Board of Directors members to verify that individuals outside of the organization were appointed as members of the Board of Directors to maintain independent oversight of executive responsibilities.	No exceptions noted.
CC1.2.2	Quarterly, the Board of Directors meets to discuss business objectives and establish company direction.	Inquired of the Compliance Engineer to verify that, quarterly, the Board of Directors had met to discuss business objectives and establish company direction.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Board of Directors meeting agenda for the sample of quarters during the examination period to verify that quarterly, the Board of Directors had met to discuss business objectives and establish company direction.	No exceptions noted.
CC1.3 COSO Principle 3: Management establishes, with Board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	DataBank maintains policy and procedure manuals for user organization-requested changes to existing systems.	Inquired of the Compliance Engineer to verify that DataBank maintained policy and procedure manuals for user organization-requested changes to existing systems.	No exceptions noted.
		Inspected the Client Requested Changes Procedures and Customer Information Guide to verify that DataBank maintained policy and procedure manuals for user organization-requested changes to existing systems.	No exceptions noted.
CC1.3.2	DataBank maintains a documented Information Security Policy which identifies the Chief Information Security Officer as accountable for the development and implementation of the policies and procedures required by this subpart for the entity or business associate.	Inquired of the Compliance Engineer to verify that DataBank maintained a documented Information Security Policy which identified the Chief Information Security Officer as accountable for the development and implementation of the policies and procedures required by this subpart for the entity or business associate.	No exceptions noted.
		Inspected the Information Security Policy and Standards Manual to verify that DataBank maintained a documented Information Security Policy which identified the Chief Information Security Officer as accountable for the development and implementation of the policies and procedures required by this subpart for the entity or business associate.	No exceptions noted.
CC1.3.3	Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	Inquired of the Chief Information Security Officer to verify that organizational charts were in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the DataBank Organizational Chart to verify that organizational charts were in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	No exceptions noted.
CC1.3.4	Information security and availability policies and procedures are documented, approved, and maintained by management, and available to guide personnel. The policies include, but are not limited to the following: ➢ Information Sensitivity ➢ Physical Security ➢ Environmental Security ➢ Incident Response	Inquired of the Compliance Engineer, to verify that information security and availability policies and procedures were documented, approved, and maintained by management, and available to guide personnel. The policies include, but were not limited to the following: ➢ Information Sensitivity ➢ Physical Security ➢ Environmental Security ➢ Incident Response	No exceptions noted.
		Inspected the information security policy and incident response plan to verify that information security and availability policies and procedures were documented, approved, and maintained by management, and available to guide personnel. The policies include, but were not limited to the following: ➢ Information Sensitivity ➢ Physical Security ➢ Environmental Security ➢ Incident Response	No exceptions noted.
CC1.3.5	Roles and responsibilities are defined in written job descriptions.	Inquired of the Compliance Engineer to verify that roles and responsibilities were defined in written job descriptions.	No exceptions noted.
		Inspected the organizational job descriptions to verify that roles and responsibilities were defined in written job descriptions.	No exceptions noted.
CC1.3.6	Documented policies and procedures for significant processes are available to personnel on Databank's shared document repository.	Inquired of the Compliance Engineer to verify that documented policies and procedures for significant processes were available to personnel on Databank's shared document repository.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the DataBank Knowledge Base to verify that documented policies and procedures for significant processes were available to personnel on Databank's shared document repository.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Personnel are required to attend security, confidentiality, and privacy training upon hire and annually thereafter.	Inquired of the Compliance Engineer to verify that personnel were required to attend security, confidentiality, and privacy training upon hire and annually thereafter.	No exceptions noted.
		Inspected the training completion report for a sample of personnel that were on-boarded and that were employed longer than one year during the examination period to verify that personnel were required to attend security, confidentiality, and privacy training upon hire and annually thereafter.	No exceptions noted.
CC1.4.2	Roles and responsibilities are defined in written job descriptions.	Inquired of the Compliance Engineer to verify that roles and responsibilities were defined in written job descriptions.	No exceptions noted.
		Inspected the organizational job descriptions to verify that roles and responsibilities were defined in written job descriptions.	No exceptions noted.
CC1.4.3	Background screenings are performed for employment candidates as a component of the hiring process.	Inquired of the Compliance Engineer to verify that background screenings were performed for employment candidates as a component of the hiring process.	No exceptions noted.
		Inspected background screenings for a sample of employees on-boarded during the examination period to verify that background screenings were performed for employment candidates as a component of the hiring process.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	DataBank maintains a documented Information Security Policy which identifies the Chief Information Security Officer as accountable for the development and implementation of the policies and procedures required by this subpart for the entity or business associate.	Inquired of the Compliance Engineer to verify that DataBank maintained a documented Information Security Policy which identified the Chief Information Security Officer as accountable for the development and implementation of the policies and procedures required by this subpart for the entity or business associate.	No exceptions noted.
		Inspected the Information Security Policy and Standards Manual to verify that DataBank maintained a documented Information Security Policy which identified the Chief Information Security Officer as accountable for the development and implementation of the policies and procedures required by this subpart for the entity or business associate.	No exceptions noted.
CC1.5.2	Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	Inquired of the Chief Information Security Officer to verify that organizational charts were in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	No exceptions noted.
		Inspected the DataBank Organizational Chart to verify that organizational charts were in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	No exceptions noted.
CC1.5.3	Roles and responsibilities are defined in written job descriptions.	Inquired of the Compliance Engineer to verify that roles and responsibilities were defined in written job descriptions.	No exceptions noted.
		Inspected the organizational job descriptions to verify that roles and responsibilities were defined in written job descriptions.	No exceptions noted.
CC1.5.4	DataBank maintains a documented Information Security Policy which expresses sanctions that can be applied for non-compliance with the policy.	Inquired of the Compliance Engineer to verify that DataBank maintained a documented Information Security Policy which expressed sanctions that could be applied for non-compliance with the policy.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Information Security Policy and Standards Manual to verify that DataBank maintained a documented Information Security Policy which expressed sanctions that could be applied for non-compliance with the policy.	No exceptions noted.
CC2.0 Communication and Information			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	A third-party vendor performs an external vulnerability assessment on an annual basis.	Inquired of the Compliance Engineer to verify that a third-party vendor performed an external vulnerability assessment on an annual basis.	No exceptions noted.
		Inspected the most recent vulnerability assessments to verify that a third-party vendor performed an external vulnerability assessment within the past 12 months.	No exceptions noted.
CC2.1.2	A risk assessment is performed annually and includes identifying and assessing the risks associated with identified threats that may impair system security. Management identifies controls that mitigate the identified risks.	Inquired of the Compliance Engineer to verify that a risk assessment was performed annually and included identifying and assessing the risks associated with identified threats that may have impaired system security. Management identified controls that mitigated the identified risks.	No exceptions noted.
		Inspected the Data Center Risk Assessment to verify that a risk assessment was performed within the past 12 months and included identifying and assessing the risks associated with identified threats that may have impaired system security and management had identified controls that mitigate the identified risks.	No exceptions noted.
CC2.1.3	Databank contracts an independent third-party to perform annual SOC 1® and SOC 2® Type 2 examinations to test the controls and their effectiveness to meet control objectives and criteria identified for the services provided. This includes security and availability commitments and requirements.	Inquired of the Compliance Engineer to verify that Databank contracted an independent third-party to perform annual SOC 1® and SOC 2® Type 2 examinations to test the controls and their effectiveness to meet control objectives and criteria identified for the services provided. This included security and availability commitments and requirements.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the most recent SOC 1® Type 2 report to verify that within the past 12 months, Databank had contracted an independent third-party to perform SOC 1® and SOC 2® Type 2 examinations to test the controls and their effectiveness to meet control objectives and criteria identified for the services provided. This included security and availability commitments and requirements.	No exceptions noted.
CC2.1.4	Quarterly, the Board of Directors meets to discuss business objectives and establish company direction.	Inquired of the Compliance Engineer to verify that, quarterly, the Board of Directors had met to discuss business objectives and establish company direction.	No exceptions noted.
		Inspected the Board of Directors meeting agenda for the sample of quarters during the examination period to verify that quarterly, the Board of Directors had met to discuss business objectives and establish company direction.	No exceptions noted.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Personnel are required to attend security, confidentiality, and privacy training upon hire and annually thereafter.	Inquired of the Compliance Engineer to verify that personnel were required to attend security, confidentiality, and privacy training upon hire and annually thereafter.	No exceptions noted.
		Inspected the training completion report for a sample of personnel that were on-boarded and that were employed longer than one year during the examination period to verify that personnel were required to attend security, confidentiality, and privacy training upon hire and annually thereafter.	No exceptions noted.
CC2.2.2	Documented incident response procedures are in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided. The procedures include defined severity levels, escalation procedures, and response time requirements for service alerts.	Inquired of the Compliance Engineer to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Incident Monitoring and Response procedures to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No exceptions noted.
CC2.2.3	Personnel are required to read and accept the physical security policy, information security policy, employee guide and confidentiality agreement as part of the on-boarding process.	Inquired of the Compliance Engineer to verify that personnel were required to read and accept the physical security policy, information security policy, employee guide and confidentiality agreement as part of the on-boarding process.	No exceptions noted.
		Inspected the signed policy acknowledgments and confidentiality agreements for a sample of employees on-boarded during the examination period to verify that personnel were required to read and accept the physical security policy, information security policy, employee guide and confidentiality agreement as part of the on-boarding process.	No exceptions noted.
CC2.2.4	Documented policies and procedures for significant processes are available to personnel on Databank's shared document repository.	Inquired of the Compliance Engineer to verify that documented policies and procedures for significant processes were available to personnel on Databank's shared document repository.	No exceptions noted.
		Inspected the DataBank Knowledge Base to verify that documented policies and procedures for significant processes were available to personnel on Databank's shared document repository.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Service agreements are executed with customers prior to on-boarding which define the terms of services provided including, but not limited to, the following: ➢ Nature, timing, and extent of services provided ➢ Roles and responsibilities ➢ Service warranties ➢ Confidentiality requirements	Inquired of the Compliance Engineer to verify that service agreements were executed with customers prior to on-boarding which defined the terms of services provided including, but not limited to, the following: ➢ Nature, timing, and extent of services provided ➢ Roles and responsibilities ➢ Service warranties ➢ Confidentiality requirements	No exceptions noted.
		Inspected executed MSAs for a sample of customers on-boarded during the examination period to verify that service agreements were executed with customers prior to on-boarding which defined the terms of services provided including, but not limited to, the following: ➢ Nature, timing, and extent of services provided ➢ Roles and responsibilities ➢ Service warranties ➢ Confidentiality requirements	No exceptions noted.
CC2.3.2	Documented incident response procedures are in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided. The procedures include defined severity levels, escalation procedures, and response time requirements for service alerts.	Inquired of the Compliance Engineer to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No exceptions noted.
		Inspected the Incident Monitoring and Response procedures to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.3.3	Upon closing a ticket, the trouble ticket system automatically emails the primary customer contact person notifying them of the issue and actions taken by DataBank.	Inquired of the Compliance Engineer to verify that upon closing a ticket, the trouble ticket system automatically emailed the primary customer contact person notifying them of the issue and actions taken by DataBank.	No exceptions noted.
		Inspected the ticket configurations to verify that upon closing a ticket, the trouble ticket system automatically emailed the primary customer contact person notifying them of the issue and actions taken by DataBank.	No exceptions noted.
CC2.3.4	DataBank's escalation procedures require notifying customers after making customer-specific firewall configuration changes.	Inquired of the Compliance Engineer to verify that DataBank's escalation procedures required notifying customers after making customer-specific firewall configuration changes.	No exceptions noted.
		Inspected notifications sent to customers for a sample of the firewall configuration changes made during the examination period to verify that DataBank's escalation procedures required notifying customers after making customer-specific firewall configuration changes.	No exceptions noted.
CC2.3.5	Technical Support staff confirms the successful completion of customer-requested restorations.	Inquired of the Compliance Engineer to verify that Technical Support staff confirmed the successful completion of customer-requested restorations.	No exceptions noted.
		Inspected job tickets for a sample of customer-requested restorations during the examination period to verify that Technical Support staff confirmed the successful completion of customer-requested restorations.	No exceptions noted.
CC2.3.6	Information security and availability policies and procedures are documented, approved, and maintained by management, and available to guide personnel. The policies include, but are not limited to the following: ➢ Information Sensitivity ➢ Physical Security ➢ Environmental Security ➢ Incident Response	Inquired of the Compliance Engineer, to verify that information security and availability policies and procedures were documented, approved, and maintained by management, and available to guide personnel. The policies include, but were not limited to the following: ➢ Information Sensitivity ➢ Physical Security ➢ Environmental Security ➢ Incident Response	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the information security policy and incident response plan to verify that information security and availability policies and procedures were documented, approved, and maintained by management, and available to guide personnel. The policies include, but were not limited to the following: ➢ Information Sensitivity ➢ Physical Security ➢ Environmental Security ➢ Incident Response	No exceptions noted.
CC3.0 Risk Assessment			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Documented incident response procedures are in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided. The procedures include defined severity levels, escalation procedures, and response time requirements for service alerts.	Inquired of the Compliance Engineer to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No exceptions noted.
		Inspected the Incident Monitoring and Response procedures to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No exceptions noted.
CC3.1.2	A risk assessment is performed annually and includes identifying and assessing the risks associated with identified threats that may impair system security. Management identifies controls that mitigate the identified risks.	Inquired of the Compliance Engineer to verify that a risk assessment was performed annually and included identifying and assessing the risks associated with identified threats that may have impaired system security. Management identified controls that mitigated the identified risks.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Data Center Risk Assessment to verify that a risk assessment was performed within the past 12 months and included identifying and assessing the risks associated with identified threats that may have impaired system security and management had identified controls that mitigate the identified risks.	No exceptions noted.
CC3.2 COSO Principle 7: 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.			
CC3.2.1	A risk assessment is performed annually and includes identifying and assessing the risks associated with identified threats that may impair system security. Management identifies controls that mitigate the identified risks.	Inquired of the Compliance Engineer to verify that a risk assessment was performed annually and included identifying and assessing the risks associated with identified threats that may have impaired system security. Management identified controls that mitigated the identified risks.	No exceptions noted.
		Inspected the Data Center Risk Assessment to verify that a risk assessment was performed within the past 12 months and included identifying and assessing the risks associated with identified threats that may have impaired system security and management had identified controls that mitigate the identified risks.	No exceptions noted.
CC3.2.2	A third-party vendor performs an external vulnerability assessment on an annual basis.	Inquired of the Compliance Engineer to verify that a third-party vendor performed an external vulnerability assessment on an annual basis.	No exceptions noted.
		Inspected the most recent vulnerability assessments to verify that a third-party vendor performed an external vulnerability assessment within the past 12 months.	No exceptions noted.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Documented incident response procedures are in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided. The procedures include defined severity levels, escalation procedures, and response time requirements for service alerts.	Inquired of the Compliance Engineer to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Incident Monitoring and Response procedures to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No exceptions noted.
CC3.3.2	An incident ticketing system is utilized to document, prioritize, escalate, and help resolve problems affecting services provided.	Inquired of the Compliance Engineer to verify that an incident ticketing system was utilized to document, prioritize, escalate, and help resolve problems that affected services provided.	No exceptions noted.
		Inspected a sample of incident tickets during the examination period to verify that an incident ticketing system was utilized to document, prioritize, escalate, and help resolve problems that affected services provided.	No exceptions noted.
CC3.3.3	A risk assessment is performed annually and includes identifying and assessing the risks associated with identified threats that may impair system security. Management identifies controls that mitigate the identified risks.	Inquired of the Compliance Engineer to verify that a risk assessment was performed annually and included identifying and assessing the risks associated with identified threats that may have impaired system security. Management identified controls that mitigated the identified risks.	No exceptions noted.
		Inspected the Data Center Risk Assessment to verify that a risk assessment was performed within the past 12 months and included identifying and assessing the risks associated with identified threats that may have impaired system security and management had identified controls that mitigate the identified risks.	No exceptions noted.
CC3.3.4	Procedure for reporting threats, incidents and violations is described in the Employee Handbook.	Inquired of the Compliance Engineer to verify that a procedure for reporting threats, incidents and violations was described in the Employee Handbook.	No exceptions noted.
		Inspected the Employee Handbook to verify that a procedure for reporting threats, incidents and violations was described in the Employee Handbook.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	A third-party vendor performs an external vulnerability assessment on an annual basis.	Inquired of the Compliance Engineer to verify that a third-party vendor performed an external vulnerability assessment on an annual basis.	No exceptions noted.
		Inspected the most recent vulnerability assessments to verify that a third-party vendor performed an external vulnerability assessment within the past 12 months.	No exceptions noted.
CC3.4.2	DataBank maintains policy and procedure manuals for implementing changes to existing systems.	Inquired of the Compliance Engineer to verify that DataBank maintained policy and procedure manuals for implementing changes to existing systems.	No exceptions noted.
		Inspected the change management policies and procedures to verify that DataBank maintained policy and procedure manuals for implementing changes to existing systems.	No exceptions noted.
CC3.4.3	Quarterly, the Board of Directors meets to discuss business objectives and establish company direction.	Inquired of the Compliance Engineer to verify that, quarterly, the Board of Directors had met to discuss business objectives and establish company direction.	No exceptions noted.
		Inspected the Board of Directors meeting agenda for the sample of quarters during the examination period to verify that quarterly, the Board of Directors had met to discuss business objectives and establish company direction.	No exceptions noted.
CC3.4.5	A risk assessment is performed annually and includes identifying and assessing the risks associated with identified threats that may impair system security. Management identifies controls that mitigate the identified risks.	Inquired of the Compliance Engineer to verify that a risk assessment was performed annually and included identifying and assessing the risks associated with identified threats that may have impaired system security. Management identified controls that mitigated the identified risks.	No exceptions noted.
		Inspected the Data Center Risk Assessment to verify that a risk assessment was performed within the past 12 months and included identifying and assessing the risks associated with identified threats that may have impaired system security and management had identified controls that mitigate the identified risks.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC3.4.6	Physical access privileges are reviewed for accuracy annually.	Inquired of the Compliance Engineer to verify that physical access privileges were reviewed for accuracy annually.	No exceptions noted.
		Inspected the access review communications for each location from within the examination period to verify that physical access privileges were reviewed for accuracy within the past 12 months.	No exceptions noted.
CC4.0 Monitoring Activities			
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	Physical access privileges are reviewed for accuracy annually.	Inquired of the Compliance Engineer to verify that physical access privileges were reviewed for accuracy annually.	No exceptions noted.
		Inspected the access review communications for each location from within the examination period to verify that physical access privileges were reviewed for accuracy within the past 12 months.	No exceptions noted.
CC4.1.2	A monitoring system is in place to monitor the firewalls for warnings, errors, and alarms.	Inquired of the Compliance Engineer to verify that a monitoring system was in place to monitor the firewalls for warnings, errors, and alarms.	No exceptions noted.
		Inspected the monitoring system log summary to verify that a monitoring system was in place to monitor the firewalls for warnings, errors, and alarms.	No exceptions noted.
CC4.1.3	A risk assessment is performed annually and includes identifying and assessing the risks associated with identified threats that may impair system security. Management identifies controls that mitigate the identified risks.	Inquired of the Compliance Engineer to verify that a risk assessment was performed annually and included identifying and assessing the risks associated with identified threats that may have impaired system security. Management identified controls that mitigated the identified risks.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Data Center Risk Assessment to verify that a risk assessment was performed within the past 12 months and included identifying and assessing the risks associated with identified threats that may have impaired system security and management had identified controls that mitigate the identified risks.	No exceptions noted.
CC4.1.4	A third-party vendor performs an external vulnerability assessment on an annual basis.	Inquired of the Compliance Engineer to verify that a third-party vendor performed an external vulnerability assessment on an annual basis.	No exceptions noted.
		Inspected the most recent vulnerability assessments to verify that a third-party vendor performed an external vulnerability assessment within the past 12 months.	No exceptions noted.
CC4.1.5	Databank contracts an independent third-party to perform annual SOC 1® and SOC 2® Type 2 examinations to test the controls and their effectiveness to meet control objectives and criteria identified for the services provided. This includes security and availability commitments and requirements.	Inquired of the Compliance Engineer to verify that Databank contracted an independent third-party to perform annual SOC 1® and SOC 2® Type 2 examinations to test the controls and their effectiveness to meet control objectives and criteria identified for the services provided. This included security and availability commitments and requirements.	No exceptions noted.
		Inspected the most recent SOC 1® Type 2 report to verify that within the past 12 months, Databank had contracted an independent third-party to perform SOC 1® and SOC 2® Type 2 examinations to test the controls and their effectiveness to meet control objectives and criteria identified for the services provided. This included security and availability commitments and requirements.	No exceptions noted.
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	Quarterly, the Board of Directors meets to discuss business objectives and establish company direction.	Inquired of the Compliance Engineer to verify that, quarterly, the Board of Directors had met to discuss business objectives and establish company direction.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Board of Directors meeting agenda for the sample of quarters during the examination period to verify that quarterly, the Board of Directors had met to discuss business objectives and establish company direction.	No exceptions noted.
CC4.2.2	Procedure for reporting threats, incidents and violations is described in the Employee Handbook.	Inquired of the Compliance Engineer to verify that a procedure for reporting threats, incidents and violations was described in the Employee Handbook.	No exceptions noted.
		Inspected the Employee Handbook to verify that a procedure for reporting threats, incidents and violations was described in the Employee Handbook.	No exceptions noted.
CC4.2.3	An incident ticketing system is utilized to document, prioritize, escalate, and help resolve problems affecting services provided.	Inquired of the Compliance Engineer to verify that an incident ticketing system was utilized to document, prioritize, escalate, and help resolve problems that affected services provided.	No exceptions noted.
		Inspected a sample of incident tickets during the examination period to verify that an incident ticketing system was utilized to document, prioritize, escalate, and help resolve problems that affected services provided.	No exceptions noted.
CC4.2.4	The environmental monitoring system is configured to notify security and data center personnel when predefined thresholds are exceeded on monitored devices.	Inquired of the Compliance Engineer to verify that the environmental monitoring systems were configured to notify security and data center personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
		Inspected monitoring system alert configurations for each location and examples of alert notifications to verify that the environmental monitoring systems were configured to notify security and data center personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
CC4.2.5	Upon closing a ticket, the trouble ticket system automatically emails the primary customer contact person notifying them of the issue and actions taken by DataBank.	Inquired of the Compliance Engineer to verify that upon closing a ticket, the trouble ticket system automatically emailed the primary customer contact person notifying them of the issue and actions taken by DataBank.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the ticket configurations to verify that upon closing a ticket, the trouble ticket system automatically emailed the primary customer contact person notifying them of the issue and actions taken by DataBank.	No exceptions noted.
CC4.2.6	DataBank's escalation procedures require notifying customers after making customer-specific firewall configuration changes.	Inquired of the Compliance Engineer to verify that DataBank's escalation procedures required notifying customers after making customer-specific firewall configuration changes.	No exceptions noted.
		Inspected notifications sent to customers for a sample of the firewall configuration changes made during the examination period to verify that DataBank's escalation procedures required notifying customers after making customer-specific firewall configuration changes.	No exceptions noted.
CC4.2.7	In the event predefined thresholds within the Managed Services monitoring systems are exceeded, the systems are configured to generate onscreen alerts and e-mail notifications.	Inquired of the Compliance Engineer to verify that in the event predefined thresholds within the managed services monitoring systems were exceeded, the systems were configured to generate onscreen alerts and e-mail notifications.	No exceptions noted.
		Inspected the monitoring event dashboard, threshold alert configurations, and an example alert to verify that in the event predefined thresholds within the managed services monitoring systems were exceeded, the systems were configured to generate onscreen alerts and e-mail notifications.	No exceptions noted.
CC4.2.8	Databank contracts an independent third-party to perform annual SOC 1® and SOC 2® Type 2 examinations to test the controls and their effectiveness to meet control objectives and criteria identified for the services provided. This includes security and availability commitments and requirements.	Inquired of the Compliance Engineer to verify that Databank contracted an independent third-party to perform annual SOC 1® and SOC 2® Type 2 examinations to test the controls and their effectiveness to meet control objectives and criteria identified for the services provided. This included security and availability commitments and requirements.	No exceptions noted.
		Inspected the most recent SOC 1® Type 2 report to verify that within the past 12 months, Databank had contracted an independent third-party to perform SOC 1® and SOC 2® Type 2 examinations to test the controls and their effectiveness to meet control objectives and criteria identified for the services provided. This included security and availability commitments and requirements.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.0 Control Activities			
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	A risk assessment is performed annually and includes identifying and assessing the risks associated with identified threats that may impair system security. Management identifies controls that mitigate the identified risks.	Inquired of the Compliance Engineer to verify that a risk assessment was performed annually and included identifying and assessing the risks associated with identified threats that may have impaired system security. Management identified controls that mitigated the identified risks.	No exceptions noted.
		Inspected the Data Center Risk Assessment to verify that a risk assessment was performed within the past 12 months and included identifying and assessing the risks associated with identified threats that may have impaired system security and management had identified controls that mitigate the identified risks.	No exceptions noted.
CC5.1.2	A third-party vendor performs an external vulnerability assessment on an annual basis.	Inquired of the Compliance Engineer to verify that a third-party vendor performed an external vulnerability assessment on an annual basis.	No exceptions noted.
		Inspected the most recent vulnerability assessments to verify that a third-party vendor performed an external vulnerability assessment within the past 12 months.	No exceptions noted.
CC5.1.3	Quarterly, the Board of Directors meets to discuss business objectives and establish company direction.	Inquired of the Compliance Engineer to verify that, quarterly, the Board of Directors had met to discuss business objectives and establish company direction.	No exceptions noted.
		Inspected the Board of Directors meeting agenda for the sample of quarters during the examination period to verify that quarterly, the Board of Directors had met to discuss business objectives and establish company direction.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Information security and availability policies and procedures are documented, approved, and maintained by management, and available to guide personnel. The policies include, but are not limited to the following: ➢ Information Sensitivity ➢ Physical Security ➢ Environmental Security ➢ Incident Response	Inquired of the Compliance Engineer, to verify that information security and availability policies and procedures were documented, approved, and maintained by management, and available to guide personnel. The policies include, but were not limited to the following: ➢ Information Sensitivity ➢ Physical Security ➢ Environmental Security ➢ Incident Response	No exceptions noted.
		Inspected the information security policy and incident response plan to verify that information security and availability policies and procedures were documented, approved, and maintained by management, and available to guide personnel. The policies include, but were not limited to the following: ➢ Information Sensitivity ➢ Physical Security ➢ Environmental Security ➢ Incident Response	No exceptions noted.
CC5.2.2	A risk assessment is performed annually and includes identifying and assessing the risks associated with identified threats that may impair system security. Management identifies controls that mitigate the identified risks.	Inquired of the Compliance Engineer to verify that a risk assessment was performed annually and included identifying and assessing the risks associated with identified threats that may have impaired system security. Management identified controls that mitigated the identified risks.	No exceptions noted.
		Inspected the Data Center Risk Assessment to verify that a risk assessment was performed within the past 12 months and included identifying and assessing the risks associated with identified threats that may have impaired system security and management had identified controls that mitigate the identified risks.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.2.3	Management reviews the DR Plan on an annual basis to ensure that it meets DataBank's availability business requirements.	Inquired of the Compliance Engineer to verify that management reviewed the DR Plan on an annual basis to ensure that it had met DataBank's availability business requirements.	No exceptions noted.
		Inspected the Incident Response Plan and the Information System Contingency Plan to verify that management reviewed the DR Plan within the past 12 months to ensure that it had met DataBank's availability business requirements.	No exceptions noted.
CC5.2.4	Management ensures that testing of the DR Plan is completed on an annual basis.	Inquired of the Compliance Engineer to verify that management ensured that testing of the DR Plan was completed on an annual basis.	No exceptions noted.
		Inspected the Business Continuity Plan Exercise to verify that management ensured that testing of the DR Plan was completed on an annual basis.	No exceptions noted.
CC5.2.5	CISO responsibilities include developing and overseeing technology teams that strategically align with and support business objectives.	Inquired of the Compliance Engineer to verify that CISO responsibilities included developing and overseeing technology teams that strategically aligned with and supported business objectives.	No exceptions noted.
		Inspected the CISO Job Description to verify that CISO responsibilities included developing and overseeing technology teams that strategically aligned with and supported business objectives.	No exceptions noted.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Documented policies and procedures for significant processes are available to personnel on Databank's shared document repository.	Inquired of the Compliance Engineer to verify that documented policies and procedures for significant processes were available to personnel on Databank's shared document repository.	No exceptions noted.
		Inspected the DataBank Knowledge Base to verify that documented policies and procedures for significant processes were available to personnel on Databank's shared document repository.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.3.2	Documented physical security policies and procedures are in place to guide employees' activities for granting, controlling, monitoring, and revoking physical access.	Inquired of the Compliance Engineer to verify that documented physical security policies and procedures were in place to guide employees' activities for granting, controlling, monitoring, and revoking physical access.	No exceptions noted.
		Inspected the Information Security and Standards Manual and the Documentation Book to verify that documented physical security policies and procedures were in place to guide employees' activities for granting, controlling, monitoring, and revoking physical access.	No exceptions noted.
CC5.3.3	Documented environmental security policies and procedures are in place to govern environmental security practices.	Inquired of the Compliance Engineer to verify that documented environmental security policies and procedures were in place to govern environmental security practices.	No exceptions noted.
		Inspected the Information Security and Standards Manual, the Documentation Book, and the Incident Monitoring and Response Procedure to verify that documented environmental security policies and procedures were in place to govern environmental security practices.	No exceptions noted.
CC5.3.4	DataBank maintains policy and procedure manuals for user organization-requested changes to existing systems.	Inquired of the Compliance Engineer to verify that DataBank maintained policy and procedure manuals for user organization-requested changes to existing systems.	No exceptions noted.
		Inspected the Client Requested Changes Procedures and Customer Information Guide to verify that DataBank maintained policy and procedure manuals for user organization-requested changes to existing systems.	No exceptions noted.
CC5.3.5	DataBank maintains policy and procedure manuals for internal network infrastructure and user organization system availability and monitoring.	Inquired of the Compliance Engineer to verify that DataBank maintained policy and procedure manuals for internal network infrastructure and user organization system availability and monitoring.	No exceptions noted.
		Inspected the Information Security Policy and Standards Manual and the Documentation Book to verify that DataBank maintained policy and procedure manuals for internal network infrastructure and user organization system availability and monitoring.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.3.6	DataBank maintains a documented Information Security Policy which identifies the Chief Information Security Officer as accountable for the development and implementation of the policies and procedures required by this subpart for the entity or business associate.	Inquired of the Compliance Engineer to verify that DataBank maintained a documented Information Security Policy which identified the Chief Information Security Officer as accountable for the development and implementation of the policies and procedures required by this subpart for the entity or business associate.	No exceptions noted.
		Inspected the Information Security Policy and Standards Manual to verify that DataBank maintained a documented Information Security Policy which identified the Chief Information Security Officer as accountable for the development and implementation of the policies and procedures required by this subpart for the entity or business associate.	No exceptions noted.
CC5.3.7	DataBank maintains policy and procedure manuals for firewall event logging, review, and escalation.	Inquired of the Compliance Engineer to verify that DataBank maintained policy and procedure manuals for firewall event logging, review, and escalation.	No exceptions noted.
		Inspected the Information Security Policy and Standards Manual and the Monitoring and Escalation Procedures to verify that DataBank maintained policy and procedure manuals for firewall event logging, review, and escalation.	No exceptions noted.
CC5.3.8	DataBank maintains policy and procedure manuals for backup, storage, and restoration procedures.	Inquired of the Compliance Engineer to verify that DataBank maintained policy and procedure manuals for backup, storage, and restoration procedures.	No exceptions noted.
		Inspected the Information System Contingency Plan to verify that DataBank maintained policy and procedure manuals for backup, storage, and restoration procedures.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.3.9	Information security and availability policies and procedures are documented, approved, and maintained by management, and available to guide personnel. The policies include, but are not limited to the following: ➢ Information Sensitivity ➢ Physical Security ➢ Environmental Security ➢ Incident Response	Inquired of the Compliance Engineer, to verify that information security and availability policies and procedures were documented, approved, and maintained by management, and available to guide personnel. The policies include, but were not limited to the following: ➢ Information Sensitivity ➢ Physical Security ➢ Environmental Security ➢ Incident Response	No exceptions noted.
		Inspected the information security policy and incident response plan to verify that information security and availability policies and procedures were documented, approved, and maintained by management, and available to guide personnel. The policies include, but were not limited to the following: ➢ Information Sensitivity ➢ Physical Security ➢ Environmental Security ➢ Incident Response	No exceptions noted.
CC5.3.10	DataBank maintains policy and procedure manuals for implementing changes to existing systems.	Inquired of the Compliance Engineer to verify that DataBank maintained policy and procedure manuals for implementing changes to existing systems.	No exceptions noted.
		Inspected the change management policies and procedures to verify that DataBank maintained policy and procedure manuals for implementing changes to existing systems.	No exceptions noted.
CC5.3.11	DataBank maintains a documented Information Security Policy which expresses sanctions that can be applied for non-compliance with the policy.	Inquired of the Compliance Engineer to verify that DataBank maintained a documented Information Security Policy which expressed sanctions that could be applied for non-compliance with the policy.	No exceptions noted.
		Inspected the Information Security Policy and Standards Manual to verify that DataBank maintained a documented Information Security Policy which expressed sanctions that could be applied for non-compliance with the policy.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC6.0 Logical and Physical Access Controls			
CC6.1 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.			
CC6.1.1	Administration of the access control system is restricted to IT, Management, and Operations personnel.	Inquired of the Compliance Engineer to verify that administration of the access control system and facility physical access was restricted to IT, Management, and Operations personnel.	No exceptions noted.
		Inspected the badge access system administrators for each location to verify that administration of the access control system and facility physical access was restricted to IT, Management, and Operations personnel.	No exceptions noted.
CC6.1.2	The access control system logs ingress activity by each user and secured point. Logs are retained for a minimum of 90 days.	Inquired of the Compliance Engineer to verify that the access control system logged ingress activity by each user and secured point and logs were retained for a minimum of 90 days.	No exceptions noted.
		Inspected badge access system logs from each location to verify that the access control system logged ingress activity by each user and secured point and logs were retained for a minimum of 90 days.	No exceptions noted.
CC6.1.3	Workstations are restricted to authorized employees via unique usernames and passwords.	Inquired of the Compliance Engineer to verify that workstations were restricted to authorized employees via unique usernames and passwords.	No exceptions noted.
		Inspected the AD Lockout Settings and the AD Password Requirements to verify that workstations were restricted to authorized employees via unique usernames and passwords.	No exceptions noted.
CC6.1.4	Employee access to customer networking devices is logically restricted to specific workstations.	Inquired of the Compliance Engineer to verify that employee access to customer networking devices was logically restricted to specific workstations.	No exceptions noted.
		Inspected the firewall configurations to verify that employee access to customer networking devices was logically restricted to specific workstations.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC6.1.5	Logical access to technical workstations is restricted by the following password requirements: ➢ Minimum length ➢ Password expiration ➢ Complexity enabled	Inquired of the Compliance Engineer to verify that logical access to technical workstations was restricted by the following password requirements: ➢ Minimum length ➢ Password expiration ➢ Complexity enabled	No exceptions noted.
		Inspected the Default Domain Policy to verify that logical access to technical workstations was restricted by the following password requirements: ➢ Minimum length ➢ Password expiration ➢ Complexity enabled	No exceptions noted.
CC6.1.6	Employee system administrator access to customer operating systems is limited by IP address to specific technical workstations.	Inquired of the Compliance Engineer to verify that employee system administrator access to customer operating systems was limited by IP address to specific technical workstations.	No exceptions noted.
		Inspected the firewall configurations to verify that employee system administrator access to customer operating systems was limited by IP address to specific technical workstations.	No exceptions noted.
CC6.1.7	Remote access to technical workstations that enable the ability for DataBank to provide remote support to customer systems is restricted by secure VPN connectivity.	Inquired of the Compliance Engineer to verify that remote access to technical workstations that enabled the ability for DataBank to provide remote support to customer systems was restricted by secure VPN connectivity.	No exceptions noted.
		Inspected the VPN configurations and authentication to verify that remote access to technical workstations that enabled the ability for DataBank to provide remote support to customer systems was restricted by secure VPN connectivity.	No exceptions noted.
CC6.1.8	VPN sessions require unique usernames and password authentication.	Inquired of the Compliance Engineer to verify that VPN sessions required unique usernames and password authentication.	No exceptions noted.
		Inspected the VPN client to verify that VPN sessions required unique usernames and password authentication.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC6.1.9	Network policies are configured to lock workstations after a predefined amount of inactivity.	Inquired of the Compliance Engineer to verify that network policies were configured to lock workstations after a predefined amount of inactivity.	No exceptions noted.
		Inspected the Default Domain Policy to verify that network policies were configured to lock workstations after a predefined amount of inactivity.	No exceptions noted.
CC6.1.10	Access to the DataBank Customer Center system is restricted through a unique username and password logins.	Inquired of the Compliance Engineer to verify that access to the DataBank Customer Care system was restricted through a unique username and password logins.	No exceptions noted.
		Inspected the Databank portal login screen to verify that access to the DataBank Customer Care system was restricted through a unique username and password logins.	No exceptions noted.
CC6.1.11	Stateful inspection firewalls are in place and are configured to filter unauthorized inbound network traffic from the Internet.	Inquired of the Compliance Engineer to verify that stateful inspection firewalls were in place and were configured to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		Inspected the network diagrams to verify that stateful inspection firewalls were in place and were configured to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
CC6.1.12	Remote access to technical workstations that enable the ability for DataBank to provide remote support to customer systems is restricted by secure VPN connectivity.	Inquired of the Compliance Engineer to verify that remote access to technical workstations that enabled the ability for DataBank to provide remote support to customer systems was restricted by secure VPN connectivity.	No exceptions noted.
		Inspected the VPN configurations and authentication to verify that remote access to technical workstations that enabled the ability for DataBank to provide remote support to customer systems was restricted by secure VPN connectivity.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC6.2 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.			
CC6.2.1	Requests for the modification of badge access privileges are made by management, or an authorized customer requestor.	Inquired of the Compliance Engineer to verify that requests for the modification of badge access privileges were made by management, or an authorized customer requestor.	No exceptions noted.
		Inspected the customer access change request communications for a sample of customer badge access changes during the examination period to verify that requests for the modification of badge access privileges were made by management, or an authorized customer requestor.	No exceptions noted.
CC6.2.2	A list of authorized customer contacts with the ability to initiate customer modifications to physical access privileges is maintained and reviewed when access requests are received from customers.	Inquired of the Compliance Engineer to verify that a list of authorized customer contacts with the ability to initiate customer modifications to physical access privileges was maintained and reviewed when access requests were received from customers.	No exceptions noted.
		Inspected the authorized customer contact listing to verify that a list of authorized customer contacts with the ability to initiate customer modifications to physical access privileges was maintained and reviewed when access requests were received from customers.	No exceptions noted.
CC6.2.3	Physical access privileges are reviewed for accuracy annually.	Inquired of the Compliance Engineer to verify that physical access privileges were reviewed for accuracy annually.	No exceptions noted.
		Inspected the access review communications for each location from within the examination period to verify that physical access privileges were reviewed for accuracy within the past 12 months.	No exceptions noted.
CC6.2.4	Management / HR notify access administrators of employee terminations via the ticketing system as part of the off-boarding process. On duty access administrators revoke access privileges for the terminated employee and confirm to management.	Inquired of the Compliance Engineer to verify that management / HR notified access administrators of employee terminations via the ticketing system as part of the off-boarding process and on duty access administrators revoked access privileges for the terminated employee and confirmed to management.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the access removal communications for a sample of employees terminated during the examination period to verify that management / HR notified access administrators of employee terminations via the ticketing system as part of the off-boarding process and on duty access administrators revoked access privileges for the terminated employee and confirmed to management.	No exceptions noted.
CC6.2.5	Service agreements are executed with customers prior to on-boarding which define the terms of services provided including, but not limited to, the following: ➢ Nature, timing, and extent of services provided ➢ Roles and responsibilities ➢ Service warranties ➢ Confidentiality requirements	Inquired of the Compliance Engineer to verify that service agreements were executed with customers prior to on-boarding which defined the terms of services provided including, but not limited to, the following: ➢ Nature, timing, and extent of services provided ➢ Roles and responsibilities ➢ Service warranties ➢ Confidentiality requirements	No exceptions noted.
		Inspected executed MSAs for a sample of customers on-boarded during the examination period to verify that service agreements were executed with customers prior to on-boarding which defined the terms of services provided including, but not limited to, the following: ➢ Nature, timing, and extent of services provided ➢ Roles and responsibilities ➢ Service warranties ➢ Confidentiality requirements	No exceptions noted.
CC6.2.6	Senior management verifies the receipt of a signed services agreement prior to the creation of a provisioning form.	Inquired of the Compliance Engineer to verify that senior management verified the receipt of a signed services agreement prior to the creation of a provisioning form.	No exceptions noted.
		Inspected signed Service Agreements and the Completion Letters for a sample of customers on-board during the examination period to verify that Senior Management verified the receipt of a signed services agreement prior to the creation of a provisioning form.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC6.2.7	New customers are tracked and managed in PowerBI to guide personnel during the new customer process.	Inquired of the Compliance Engineer to verify that new customers were tracked and managed in PowerBI to guide personnel during the new customer process.	No exceptions noted.
		Inspected the PowerBI Billing Audit Report to verify that new customers were tracked and managed in PowerBI to guide personnel during the new customer process.	No exceptions noted.
CC6.2.8	A customer authorized requestor list is maintained for each customer that lists the authorized customer contacts with the ability to initiate changes to subscribed services.	Inquired of the Compliance Engineer to verify that a customer authorized requestor list was maintained for each customer that listed the authorized customer contacts with the ability to initiate changes to subscribed services.	No exceptions noted.
		Inspected the authorized customer contact listing to verify that a customer authorized requestor list was maintained for each customer that listed the authorized customer contacts with the ability to initiate changes to subscribed services.	No exceptions noted.
CC6.3 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.			
CC6.3.1	Administration of the access control system is restricted to IT, Management, and Operations personnel.	Inquired of the Compliance Engineer to verify that administration of the access control system and facility physical access was restricted to IT, Management, and Operations personnel.	No exceptions noted.
		Inspected the badge access system administrators for each location to verify that administration of the access control system and facility physical access was restricted to IT, Management, and Operations personnel.	No exceptions noted.
CC6.3.2	Requests for the modification of badge access privileges are made by management, or an authorized customer requestor.	Inquired of the Compliance Engineer to verify that requests for the modification of badge access privileges were made by management, or an authorized customer requestor.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the customer access change request communications for a sample of customer badge access changes during the examination period to verify that requests for the modification of badge access privileges were made by management, or an authorized customer requestor.	No exceptions noted.
CC6.3.3	A list of authorized customer contacts with the ability to initiate customer modifications to physical access privileges is maintained and reviewed when access requests are received from customers.	Inquired of the Compliance Engineer to verify that a list of authorized customer contacts with the ability to initiate customer modifications to physical access privileges was maintained and reviewed when access requests were received from customers.	No exceptions noted.
		Inspected the authorized customer contact listing to verify that a list of authorized customer contacts with the ability to initiate customer modifications to physical access privileges was maintained and reviewed when access requests were received from customers.	No exceptions noted.
CC6.3.4	Physical access privileges are reviewed for accuracy annually.	Inquired of the Compliance Engineer to verify that physical access privileges were reviewed for accuracy annually.	No exceptions noted.
		Inspected the access review communications for each location from within the examination period to verify that physical access privileges were reviewed for accuracy within the past 12 months.	No exceptions noted.
CC6.3.5	Senior management verifies the receipt of a signed services agreement prior to the creation of a provisioning form.	Inquired of the Compliance Engineer to verify that senior management verified the receipt of a signed services agreement prior to the creation of a provisioning form.	No exceptions noted.
		Inspected signed Service Agreements and the Completion Letters for a sample of customers on-board during the examination period to verify that Senior Management verified the receipt of a signed services agreement prior to the creation of a provisioning form.	No exceptions noted.
CC6.3.6	A customer authorized requestor list is maintained for each customer that lists the authorized customer contacts with the ability to initiate changes to subscribed services.	Inquired of the Compliance Engineer to verify that a customer authorized requestor list was maintained for each customer that listed the authorized customer contacts with the ability to initiate changes to subscribed services.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the authorized customer contact listing to verify that a customer authorized requestor list was maintained for each customer that listed the authorized customer contacts with the ability to initiate changes to subscribed services.	No exceptions noted.
CC6.3.7	Workstations are restricted to authorized employees via unique usernames and passwords.	Inquired of the Compliance Engineer to verify that workstations were restricted to authorized employees via unique usernames and passwords.	No exceptions noted.
		Inspected the AD Lockout Settings and the AD Password Requirements to verify that workstations were restricted to authorized employees via unique usernames and passwords.	No exceptions noted.
CC6.3.8	Employee access to customer networking devices is logically restricted to specific workstations.	Inquired of the Compliance Engineer to verify that employee access to customer networking devices was logically restricted to specific workstations.	No exceptions noted.
		Inspected the firewall configurations to verify that employee access to customer networking devices was logically restricted to specific workstations.	No exceptions noted.
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive location(s) to authorized personnel to meet the entity's objectives.			
CC6.4.1	Documented physical security policies and procedures are in place to guide employees' activities for granting, controlling, monitoring, and revoking physical access.	Inquired of the Compliance Engineer to verify that documented physical security policies and procedures were in place to guide employees' activities for granting, controlling, monitoring, and revoking physical access.	No exceptions noted.
		Inspected the Information Security and Standards Manual and the Documentation Book to verify that documented physical security policies and procedures were in place to guide employees' activities for granting, controlling, monitoring, and revoking physical access.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC6.4.2	Visitors, vendors, and contractors are required to: ➢ Present photo identification ➢ Sign a visitor sign-in log including name, firm represented, onsite personnel authorizing access ➢ Wear a visitor's tag to gain access into the facilities	Inquired of the onsite personnel for a sample of sites visited to verify that visitors, vendors, and contractors were required to: ➢ Present photo identification ➢ Sign a visitor sign-in log including name, firm represented, onsite personnel authorizing access ➢ Wear a visitor's tag to gain access into the facilities	No exceptions noted.
		Inspected visitor sign-in logs to verify that visitors, vendors, and contractors were required to: ➢ Present photo identification ➢ Sign a visitor sign-in log including name, firm represented, onsite personnel authorizing access ➢ Wear a visitor's tag to gain access into the facilities	No exceptions noted.
		Observed visitors enter the data centers for a sample of sites visited during onsite activities to verify that visitors, vendors, and contractors were required to: ➢ Present photo identification ➢ Sign a visitor sign-in log including name, firm represented, onsite personnel authorizing access ➢ Wear a visitor's tag to gain access into the facilities	No exceptions noted.
CC6.4.3	Visitors are required to be escorted by an authorized employee when accessing the facilities.	Inquired of the onsite personnel for a sample of sites visited to verify that visitors were required to be escorted by an authorized employee when accessing the facilities.	No exceptions noted.
		Observed visitors during onsite activities for a sample of sites visited to verify that visitors were required to be escorted by an authorized employee when accessing the facilities.	No exceptions noted.
CC6.4.4	Visitors leaving the facilities are required to surrender their badge upon departure.	Inquired of the onsite personnel for a sample of sites visited to verify that visitors leaving the facilities were required to surrender their badge upon departure.	No exceptions noted.
		Observed visitors during onsite activities for a sample of sites visited to verify that visitors leaving the facilities were required to surrender their badge upon departure.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC6.4.5	Doors controlling access to facilities and restricted areas remain secured at all times.	Inquired of the onsite personnel for a sample of sites visited to verify that the doors to the facilities and data centers remained locked at all times.	No exceptions noted.
		Observed access to the data centers during onsite activities for a sample of sites visited to verify that the doors to the facilities and data centers remained locked at all times.	No exceptions noted.
CC6.4.6	Doors controlling access to facilities and restricted areas are equipped with alarm contacts and alert on forced entry.	Inquired of the onsite personnel for a sample of sites visited to verify that the doors to the facilities and data centers were equipped with forced entry sensors and door alarm contact points.	No exceptions noted.
		Observed the data centers during onsite activities for a sample of sites visited to verify that the doors to the facilities and data centers were equipped with forced entry sensors and door alarm contact points.	No exceptions noted.
CC6.4.7	An access control system is in place at each facility to prevent ingress by unauthorized users and restrict authorized users to appropriate areas.	Inquired of the onsite personnel for a sample of sites visited to verify that an access control system was in place at each facility to prevent ingress by unauthorized users and restrict authorized users to appropriate areas.	No exceptions noted.
		Inspected the badge access systems for each location to verify that an access control system was in place at each facility to prevent ingress by unauthorized users and restrict authorized users to appropriate areas.	No exceptions noted.
		Observed the data centers during onsite activities for a sample of sites visited to verify that access to and throughout the facilities was controlled using badge access systems.	No exceptions noted.
CC6.4.8	Predefined physical security zones are utilized to assign role-based access to and throughout the data centers.	Inquired of the onsite personnel for a sample of sites visited to verify that predefined physical security zones were utilized to assign role-based access to and throughout the data centers.	No exceptions noted.
		Inspected the badge access system at each location to verify that predefined physical security zones were utilized to assign role-based access to and throughout the data centers.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Observed the use and configurations of predefined security zones within the data centers during onsite activities for a sample of sites visited to verify that predefined physical security zones were utilized to assign role-based access to and throughout the data centers.	No exceptions noted.
CC6.4.9	Surveillance cameras are utilized to record activity at the facility and data hall entrances.	Inquired of the onsite personnel for a sample of sites visited to verify that surveillance cameras were utilized to record activity at the facility and data hall entrances.	No exceptions noted.
		Observed the security cameras within the facilities during onsite activities for a sample of sites visited to verify that surveillance cameras were utilized to record activity at the facility and data hall entrances.	No exceptions noted.
CC6.4.10	Surveillance video is retained for a minimum of 90 days.	Inquired of the onsite personnel to verify that surveillance video was retained for a minimum of 90 days.	No exceptions noted.
		Inspected the surveillance video systems for each location to verify that surveillance video was retained for a minimum of 90 days.	No exceptions noted.
CC6.4.11	Customer equipment is housed in locked, segregated environments within the data centers.	Inquired of the onsite personnel to verify that customer equipment was housed in locked, segregated environments within the data centers.	No exceptions noted.
		Observed the locked customer equipment cages and server racks during onsite activities for a sample of sites visited to verify that customer equipment was housed in locked, segregated environments within the data centers.	No exceptions noted.
CC6.4.12	Physical access privileges are reviewed for accuracy annually.	Inquired of the Compliance Engineer to verify that physical access privileges were reviewed for accuracy annually.	No exceptions noted.
		Inspected the access review communications for each location from within the examination period to verify that physical access privileges were reviewed for accuracy within the past 12 months.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC6.4.13	The data centers data halls do not contain any exterior windows.	Inquired of the onsite personnel for a sample of sites visited to verify that the data centers did not contain any exterior windows.	No exceptions noted.
		Observed the data center halls during onsite activities for a sample of sites visited to verify that the data centers did not contain any exterior windows.	No exceptions noted.
CC6.5 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.			
CC6.5.1	Management / HR notify access administrators of employee terminations via the ticketing system as part of the off-boarding process. On duty access administrators revoke access privileges for the terminated employee and confirm to management.	Inquired of the Compliance Engineer to verify that management / HR notified access administrators of employee terminations via the ticketing system as part of the off-boarding process and on duty access administrators revoked access privileges for the terminated employee and confirmed to management.	No exceptions noted.
		Inspected the access removal communications for a sample of employees terminated during the examination period to verify that management / HR notified access administrators of employee terminations via the ticketing system as part of the off-boarding process and on duty access administrators revoked access privileges for the terminated employee and confirmed to management.	No exceptions noted.
CC6.5.2	Physical access privileges are reviewed for accuracy annually.	Inquired of the Compliance Engineer to verify that physical access privileges were reviewed for accuracy annually.	No exceptions noted.
		Inspected the access review communications for each location from within the examination period to verify that physical access privileges were reviewed for accuracy within the past 12 months.	No exceptions noted.
CC6.5.3	Requests for the modification of badge access privileges are made by management, or an authorized customer requestor.	Inquired of the Compliance Engineer to verify that requests for the modification of badge access privileges were made by management, or an authorized customer requestor.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the customer access change request communications for a sample of customer badge access changes during the examination period to verify that requests for the modification of badge access privileges were made by management, or an authorized customer requestor.	No exceptions noted.
CC6.5.4	A list of authorized customer contacts with the ability to initiate customer modifications to physical access privileges is maintained and reviewed when access requests are received from customers.	Inquired of the Compliance Engineer to verify that a list of authorized customer contacts with the ability to initiate customer modifications to physical access privileges was maintained and reviewed when access requests were received from customers.	No exceptions noted.
		Inspected the authorized customer contact listing to verify that a list of authorized customer contacts with the ability to initiate customer modifications to physical access privileges was maintained and reviewed when access requests were received from customers.	No exceptions noted.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	A third-party vendor performs an external vulnerability assessment on an annual basis.	Inquired of the Compliance Engineer to verify that a third-party vendor performed an external vulnerability assessment on an annual basis.	No exceptions noted.
		Inspected the most recent vulnerability assessments to verify that a third-party vendor performed an external vulnerability assessment within the past 12 months.	No exceptions noted.
CC6.6.2	Antivirus software is configured to monitor traffic within the internal network, as well as communications with external networks, and detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inquired of the Compliance Engineer to verify that antivirus software was configured to monitor traffic within the internal network, as well as communications with external networks, and detected and prevented the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	No exceptions noted.
		Inspected the antivirus configurations to verify that antivirus software was configured to monitor traffic within the internal network, as well as communications with external networks, and detected and prevented the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC6.6.3	Antivirus software is automatically updated with current virus signatures. A central server is utilized to push updates to production servers daily.	Inquired of the Compliance Engineer to verify that antivirus software was automatically updated with current virus signatures and a central server was utilized to push updates to production servers daily.	No exceptions noted.
		Inspected the antivirus configurations to verify that antivirus software was automatically updated with current virus signatures and a central server was utilized to push updates to production servers daily.	No exceptions noted.
CC6.6.4	A monitoring system is in place to monitor the firewalls for warnings, errors, and alarms.	Inquired of the Compliance Engineer to verify that a monitoring system was in place to monitor the firewalls for warnings, errors, and alarms.	No exceptions noted.
		Inspected the monitoring system log summary to verify that a monitoring system was in place to monitor the firewalls for warnings, errors, and alarms.	No exceptions noted.
CC6.6.5	Stateful inspection firewalls are in place and are configured to filter unauthorized inbound network traffic from the Internet.	Inquired of the Compliance Engineer to verify that stateful inspection firewalls were in place and were configured to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		Inspected the network diagrams to verify that stateful inspection firewalls were in place and were configured to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
CC6.6.6	Remote access to technical workstations that enable the ability for DataBank to provide remote support to customer systems is restricted by secure VPN connectivity.	Inquired of the Compliance Engineer to verify that remote access to technical workstations that enabled the ability for DataBank to provide remote support to customer systems was restricted by secure VPN connectivity.	No exceptions noted.
		Inspected the VPN configurations and authentication to verify that remote access to technical workstations that enabled the ability for DataBank to provide remote support to customer systems was restricted by secure VPN connectivity.	No exceptions noted.
CC6.6.7	VPN sessions require unique usernames and password authentication.	Inquired of the Compliance Engineer to verify that VPN sessions required unique usernames and password authentication.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the VPN client to verify that VPN sessions required unique usernames and password authentication.	No exceptions noted.
CC6.7 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.			
CC6.7.1	Remote access to technical workstations that enable the ability for DataBank to provide remote support to customer systems is restricted by secure VPN connectivity.	Inquired of the Compliance Engineer to verify that remote access to technical workstations that enabled the ability for DataBank to provide remote support to customer systems was restricted by secure VPN connectivity.	No exceptions noted.
		Inspected the VPN configurations and authentication to verify that remote access to technical workstations that enabled the ability for DataBank to provide remote support to customer systems was restricted by secure VPN connectivity.	No exceptions noted.
CC6.7.2	Antivirus software is configured to monitor traffic within the internal network, as well as communications with external networks, and detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inquired of the Compliance Engineer to verify that antivirus software was configured to monitor traffic within the internal network, as well as communications with external networks, and detected and prevented the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	No exceptions noted.
		Inspected the antivirus configurations to verify that antivirus software was configured to monitor traffic within the internal network, as well as communications with external networks, and detected and prevented the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	No exceptions noted.
CC6.7.3	Antivirus software is automatically updated with current virus signatures. A central server is utilized to push updates to production servers daily.	Inquired of the Compliance Engineer to verify that antivirus software was automatically updated with current virus signatures and a central server was utilized to push updates to production servers daily.	No exceptions noted.
		Inspected the antivirus configurations to verify that antivirus software was automatically updated with current virus signatures and a central server was utilized to push updates to production servers daily.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC6.7.4	Stateful inspection firewalls are in place and are configured to filter unauthorized inbound network traffic from the Internet.	Inquired of the Compliance Engineer to verify that stateful inspection firewalls were in place and were configured to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		Inspected the network diagrams to verify that stateful inspection firewalls were in place and were configured to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
CC6.7.5	Remote access to technical workstations that enable the ability for DataBank to provide remote support to customer systems is restricted by secure VPN connectivity.	Inquired of the Compliance Engineer to verify that remote access to technical workstations that enabled the ability for DataBank to provide remote support to customer systems was restricted by secure VPN connectivity.	No exceptions noted.
		Inspected the VPN configurations and authentication to verify that remote access to technical workstations that enabled the ability for DataBank to provide remote support to customer systems was restricted by secure VPN connectivity.	No exceptions noted.
CC6.7.6	VPN sessions require unique usernames and password authentication.	Inquired of the Compliance Engineer to verify that VPN sessions required unique usernames and password authentication.	No exceptions noted.
		Inspected the VPN client to verify that VPN sessions required unique usernames and password authentication.	No exceptions noted.
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	Customers who purchase network services are required to sign an agreement that outlines the prohibited uses of network services.	Inquired of the Compliance Engineer to verify that customers who purchased network services were required to sign an agreement that outlined the prohibited uses of network services.	No exceptions noted.
		Inspected executed MSAs for a sample of customers on-boarded during the examination period to verify that customers who purchased network services were required to sign an agreement that outlined the prohibited uses of network services.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC6.8.2	Antivirus software is configured to monitor traffic within the internal network, as well as communications with external networks, and detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inquired of the Compliance Engineer to verify that antivirus software was configured to monitor traffic within the internal network, as well as communications with external networks, and detected and prevented the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	No exceptions noted.
		Inspected the antivirus configurations to verify that antivirus software was configured to monitor traffic within the internal network, as well as communications with external networks, and detected and prevented the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	No exceptions noted.
CC6.8.3	Antivirus software is automatically updated with current virus signatures. A central server is utilized to push updates to production servers daily.	Inquired of the Compliance Engineer to verify that antivirus software was automatically updated with current virus signatures and a central server was utilized to push updates to production servers daily.	No exceptions noted.
		Inspected the antivirus configurations to verify that antivirus software was automatically updated with current virus signatures and a central server was utilized to push updates to production servers daily.	No exceptions noted.
CC6.8.4	Technical support staff are available 24 X 365 to manage data center monitoring systems which include power, temperature, humidity, video surveillance, and access control.	Inquired of the Compliance Engineer to verify that technical support staff were available 24 X 365 to manage data center monitoring systems which included power, temperature, humidity, video surveillance, and access control.	No exceptions noted.
		Inspected the on-call schedule to verify that technical support staff were available 24 X 365 to manage data center monitoring systems which included power, temperature, humidity, video surveillance, and access control.	No exceptions noted.
		Observed the technical support staff during on-site activities for a sample of sites visited to verify that they monitored the physical environment on a 24 x 365 basis, including power, temperature, humidity, video surveillance, and access control.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC6.8.5	Applications are utilized to monitor the following performance, availability, and controlled events for managed services infrastructure: ➢ Availability of the network ➢ Host services and ports ➢ CPU and hard disk utilization	Inquired of the onsite personnel for a sample of sites visited to verify that applications were utilized to monitor the following performance, availability, and controlled events for managed services infrastructure: ➢ Availability of the network ➢ Host services and ports ➢ CPU and hard disk utilization	No exceptions noted.
		Observed the monitoring systems during on-site activities for a sample of sites visited to verify that applications were utilized to monitor the following performance, availability, and controlled events for managed services infrastructure: ➢ Availability of the network ➢ Host services and ports ➢ CPU and hard disk utilization	No exceptions noted.
CC6.8.6	Environmental monitoring systems are utilized to monitor the environmental conditions and devices within the data centers including, but not limited to, the following: ➢ Water leakage ➢ Air handling units ➢ UPS systems ➢ Generators	Inquired of the onsite personnel for a sample of sites visited to verify that environmental monitoring systems were utilized to monitor the environmental conditions and devices within the data centers including, but not limited to, the following: ➢ Water leakage ➢ Air handling units ➢ UPS systems ➢ Generators	No exceptions noted.
		Inspected the environmental monitoring Data Center Infrastructure Management systems for a sample of sites visited to verify that environmental monitoring systems were utilized to monitor the environmental conditions and devices within the data centers including, but not limited to, the following: ➢ Water leakage ➢ Air handling units ➢ UPS systems ➢ Generators	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Observed the environmental monitoring systems during onsite activities for a sample of sites visited to verify that environmental monitoring systems were utilized to monitor the environmental conditions and devices within the data centers including, but not limited to, the following: ➢ Water leakage ➢ Air handling units ➢ UPS systems ➢ Generators	No exceptions noted.
CC6.8.7	The environmental monitoring system is configured to notify security and data center personnel when predefined thresholds are exceeded on monitored devices.	Inquired of the Compliance Engineer to verify that the environmental monitoring systems were configured to notify security and data center personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
		Inspected monitoring system alert configurations for each location and examples of alert notifications to verify that the environmental monitoring systems were configured to notify security and data center personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
CC7.0 System Operations			
CC7.1 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.			
CC7.1.1	Environmental monitoring systems are utilized to monitor the environmental conditions and devices within the data centers including, but not limited to, the following: ➢ Water leakage ➢ Air handling units ➢ UPS systems ➢ Generators	Inquired of the onsite personnel for a sample of sites visited to verify that environmental monitoring systems were utilized to monitor the environmental conditions and devices within the data centers including, but not limited to, the following: ➢ Water leakage ➢ Air handling units ➢ UPS systems ➢ Generators	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the environmental monitoring Data Center Infrastructure Management systems for a sample of sites visited to verify that environmental monitoring systems were utilized to monitor the environmental conditions and devices within the data centers including, but not limited to, the following: ➢ Water leakage ➢ Air handling units ➢ UPS systems ➢ Generators	No exceptions noted.
		Observed the environmental monitoring systems during onsite activities for a sample of sites visited to verify that environmental monitoring systems were utilized to monitor the environmental conditions and devices within the data centers including, but not limited to, the following: ➢ Water leakage ➢ Air handling units ➢ UPS systems ➢ Generators	No exceptions noted.
CC7.1.2	The environmental monitoring system is configured to notify security and data center personnel when predefined thresholds are exceeded on monitored devices.	Inquired of the Compliance Engineer to verify that the environmental monitoring systems were configured to notify security and data center personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
		Inspected monitoring system alert configurations for each location and examples of alert notifications to verify that the environmental monitoring systems were configured to notify security and data center personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
CC7.1.3	In the event predefined thresholds within the Managed Services monitoring systems are exceeded, the systems are configured to generate onscreen alerts and e-mail notifications.	Inquired of the Compliance Engineer to verify that in the event predefined thresholds within the managed services monitoring systems were exceeded, the systems were configured to generate onscreen alerts and e-mail notifications.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the monitoring event dashboard, threshold alert configurations, and an example alert to verify that in the event predefined thresholds within the managed services monitoring systems were exceeded, the systems were configured to generate onscreen alerts and e-mail notifications.	No exceptions noted.
CC7.1.4	A monitoring system is in place to monitor the firewalls for warnings, errors, and alarms.	Inquired of the Compliance Engineer to verify that a monitoring system was in place to monitor the firewalls for warnings, errors, and alarms.	No exceptions noted.
		Inspected the monitoring system log summary to verify that a monitoring system was in place to monitor the firewalls for warnings, errors, and alarms.	No exceptions noted.
CC7.1.5	The engineering staff reviews and monitors the backup job error notifications to ensure successful completion.	Inquired of onsite personnel for a sample of sites visited to verify that the engineering staff reviewed and monitored the backup job error notifications to ensure successful completion.	No exceptions noted.
		Observed the engineering staff monitor backup notifications during onsite activities for a sample of sites visited to verify that the engineering staff reviewed and monitored the backup job error notifications to ensure successful completion.	No exceptions noted.
CC7.1.6	A third-party vendor performs an external vulnerability assessment on an annual basis.	Inquired of the Compliance Engineer to verify that a third-party vendor performed an external vulnerability assessment on an annual basis.	No exceptions noted.
		Inspected the most recent vulnerability assessments to verify that a third-party vendor performed an external vulnerability assessment within the past 12 months.	No exceptions noted.
CC7.1.7	Antivirus software is configured to monitor traffic within the internal network, as well as communications with external networks, and detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inquired of the Compliance Engineer to verify that antivirus software was configured to monitor traffic within the internal network, as well as communications with external networks, and detected and prevented the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the antivirus configurations to verify that antivirus software was configured to monitor traffic within the internal network, as well as communications with external networks, and detected and prevented the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	No exceptions noted.
CC7.1.8	Antivirus software is automatically updated with current virus signatures. A central server is utilized to push updates to production servers daily.	Inquired of the Compliance Engineer to verify that antivirus software was automatically updated with current virus signatures and a central server was utilized to push updates to production servers daily.	No exceptions noted.
		Inspected the antivirus configurations to verify that antivirus software was automatically updated with current virus signatures and a central server was utilized to push updates to production servers daily.	No exceptions noted.
CC7.2 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.			
CC7.2.1	The environmental monitoring system is configured to notify security and data center personnel when predefined thresholds are exceeded on monitored devices.	Inquired of the Compliance Engineer to verify that the environmental monitoring systems were configured to notify security and data center personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
		Inspected monitoring system alert configurations for each location and examples of alert notifications to verify that the environmental monitoring systems were configured to notify security and data center personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
CC7.2.2	Applications are utilized to monitor the following performance, availability, and controlled events for managed services infrastructure: ➢ Availability of the network ➢ Host services and ports ➢ CPU and hard disk utilization	Inquired of the onsite personnel for a sample of sites visited to verify that applications were utilized to monitor the following performance, availability, and controlled events for managed services infrastructure: ➢ Availability of the network ➢ Host services and ports ➢ CPU and hard disk utilization	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Observed the monitoring systems during on-site activities to verify that applications were utilized to monitor the following performance, availability, and controlled events for managed services infrastructure: ➢ Availability of the network ➢ Host services and ports ➢ CPU and hard disk utilization	No exceptions noted.
CC7.2.3	In the event predefined thresholds within the Managed Services monitoring systems are exceeded, the systems are configured to generate onscreen alerts and e-mail notifications.	Inquired of the Compliance Engineer to verify that in the event predefined thresholds within the managed services monitoring systems were exceeded, the systems were configured to generate onscreen alerts and e-mail notifications.	No exceptions noted.
		Inspected the monitoring event dashboard, threshold alert configurations, and an example alert to verify that in the event predefined thresholds within the managed services monitoring systems were exceeded, the systems were configured to generate onscreen alerts and e-mail notifications.	No exceptions noted.
CC7.2.4	A monitoring system is in place to monitor the firewalls for warnings, errors, and alarms.	Inquired of the Compliance Engineer to verify that a monitoring system was in place to monitor the firewalls for warnings, errors, and alarms.	No exceptions noted.
		Inspected the monitoring system log summary to verify that a monitoring system was in place to monitor the firewalls for warnings, errors, and alarms.	No exceptions noted.
CC7.2.5	Documented incident response procedures are in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided. The procedures include defined severity levels, escalation procedures, and response time requirements for service alerts.	Inquired of the Compliance Engineer to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Incident Monitoring and Response procedures to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No exceptions noted.
CC7.2.6	Technical support staff are available 24 X 365 to manage data center monitoring systems which include power, temperature, humidity, video surveillance, and access control.	Inquired of the Compliance Engineer to verify that technical support staff were available 24 X 365 to manage data center monitoring systems which included power, temperature, humidity, video surveillance, and access control.	No exceptions noted.
		Inspected the on-call schedule to verify that technical support staff were available 24 X 365 to manage data center monitoring systems which included power, temperature, humidity, video surveillance, and access control.	No exceptions noted.
		Observed the technical support staff during on-site activities for a sample of sites visited to verify that they monitored the physical environment on a 24 x 365 basis, including power, temperature, humidity, video surveillance, and access control.	No exceptions noted.
CC7.3 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.			
CC7.3.1	Documented incident response procedures are in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided. The procedures include defined severity levels, escalation procedures, and response time requirements for service alerts.	Inquired of the Compliance Engineer to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No exceptions noted.
		Inspected the Incident Monitoring and Response procedures to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC7.3.2	An incident ticketing system is utilized to document, prioritize, escalate, and help resolve problems affecting services provided.	Inquired of the Compliance Engineer to verify that an incident ticketing system was utilized to document, prioritize, escalate, and help resolve problems that affected services provided.	No exceptions noted.
		Inspected a sample of incident tickets during the examination period to verify that an incident ticketing system was utilized to document, prioritize, escalate, and help resolve problems that affected services provided.	No exceptions noted.
CC7.3.3	Applications are utilized to monitor the following performance, availability, and controlled events for managed services infrastructure: ➢ Availability of the network ➢ Host services and ports ➢ CPU and hard disk utilization	Inquired of the onsite personnel for a sample of sites visited to verify that applications were utilized to monitor the following performance, availability, and controlled events for managed services infrastructure: ➢ Availability of the network ➢ Host services and ports ➢ CPU and hard disk utilization	No exceptions noted.
		Observed the monitoring systems during on-site activities to verify that applications were utilized to monitor the following performance, availability, and controlled events for managed services infrastructure: ➢ Availability of the network ➢ Host services and ports ➢ CPU and hard disk utilization	No exceptions noted.
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	Documented incident response procedures are in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided. The procedures include defined severity levels, escalation procedures, and response time requirements for service alerts.	Inquired of the Compliance Engineer to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Incident Monitoring and Response procedures to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No exceptions noted.
CC7.4.2	Technical support staff are available 24 X 365 to manage data center monitoring systems which include power, temperature, humidity, video surveillance, and access control.	Inquired of the Compliance Engineer to verify that technical support staff were available 24 X 365 to manage data center monitoring systems which included power, temperature, humidity, video surveillance, and access control.	No exceptions noted.
		Inspected the on-call schedule to verify that technical support staff were available 24 X 365 to manage data center monitoring systems which included power, temperature, humidity, video surveillance, and access control.	No exceptions noted.
		Observed the technical support staff during on-site activities for a sample of sites visited to verify that they monitored the physical environment on a 24 x 365 basis, including power, temperature, humidity, video surveillance, and access control.	No exceptions noted.
CC7.4.3	A ticketing system is used to document and track to resolution, customer requests.	Inquired of the Compliance Engineer to verify that a ticketing system was used to document and track to resolution, customer requests.	No exceptions noted.
		Inspected the customer change ticket systems and notifications to verify that a ticketing system was used to document and track to resolution, customer requests.	No exceptions noted.
CC7.4.4	Upon closing a ticket, the trouble ticket system automatically emails the primary customer contact person notifying them of the issue and actions taken by DataBank.	Inquired of the Compliance Engineer to verify that upon closing a ticket, the trouble ticket system automatically emailed the primary customer contact person notifying them of the issue and actions taken by DataBank.	No exceptions noted.
		Inspected the ticket configurations to verify that upon closing a ticket, the trouble ticket system automatically emailed the primary customer contact person notifying them of the issue and actions taken by DataBank.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Documented incident response procedures are in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided. The procedures include defined severity levels, escalation procedures, and response time requirements for service alerts.	Inquired of the Compliance Engineer to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No exceptions noted.
		Inspected the Incident Monitoring and Response procedures to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No exceptions noted.
CC7.5.2	DataBank maintains policy and procedure manuals for backup, storage, and restoration procedures.	Inquired of the Compliance Engineer to verify that DataBank maintained policy and procedure manuals for backup, storage, and restoration procedures.	No exceptions noted.
		Inspected the Information System Contingency Plan to verify that DataBank maintained policy and procedure manuals for backup, storage, and restoration procedures.	No exceptions noted.
CC7.5.3	DataBank standard backup configuration is set to automatically perform daily backups of customer systems.	Inquired of the Compliance Engineer to verify that DataBank standard backup configurations were set to automatically perform daily backups of customer systems.	No exceptions noted.
		Inspected the backup configurations to verify that DataBank standard backup configurations were set to automatically perform daily backups of customer systems.	No exceptions noted.
CC7.5.4	Management reviews the DR Plan on an annual basis to ensure that it meets DataBank's availability business requirements.	Inquired of the Compliance Engineer to verify that management reviewed the DR Plan on an annual basis to ensure that it had met DataBank's availability business requirements.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Incident Response Plan and the Information System Contingency Plan to verify that management reviewed the DR Plan within the past 12 months to ensure that it had met DataBank's availability business requirements.	No exceptions noted.
CC7.5.5	Management ensures that testing of the DR Plan is completed on an annual basis.	Inquired of the Compliance Engineer to verify that management ensured that testing of the DR Plan was completed on an annual basis.	No exceptions noted.
		Inspected the Business Continuity Plan Exercise to verify that management ensured that testing of the DR Plan was completed on an annual basis.	No exceptions noted.
CC8.0 Change Management			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Modifications to existing user organization firewall rule sets are performed by DataBank only after receiving a modification request from authorized user organization personnel.	Inquired of the Compliance Engineer to verify that modifications to existing user organization firewall rule sets were performed by DataBank only after receiving a modification request from authorized user organization personnel.	No exceptions noted.
		Inspected the firewall change tickets for a sample of customer firewall changes during the examination period to verify that modifications to existing user organization firewall rule sets were performed by DataBank only after receiving a modification request from authorized user organization personnel.	No exceptions noted.
CC8.1.2	Technical Support staff confirms the successful completion of customer-requested restorations.	Inquired of the Compliance Engineer to verify that Technical Support staff confirmed the successful completion of customer-requested restorations.	No exceptions noted.
		Inspected job tickets for a sample of customer-requested restorations during the examination period to verify that Technical Support staff confirmed the successful completion of customer-requested restorations.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC8.1.3	DataBank maintains policy and procedure manuals for implementing changes to existing systems.	Inquired of the Compliance Engineer to verify that DataBank maintained policy and procedure manuals for implementing changes to existing systems.	No exceptions noted.
		Inspected the change management policies and procedures to verify that DataBank maintained policy and procedure manuals for implementing changes to existing systems.	No exceptions noted.
CC9.0 Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	DataBank maintains policy and procedure manuals for backup, storage, and restoration procedures.	Inquired of the Compliance Engineer to verify that DataBank maintained policy and procedure manuals for backup, storage, and restoration procedures.	No exceptions noted.
		Inspected the Information System Contingency Plan to verify that DataBank maintained policy and procedure manuals for backup, storage, and restoration procedures.	No exceptions noted.
CC9.1.2	DataBank standard backup configuration is set to automatically perform daily backups of customer systems.	Inquired of the Compliance Engineer to verify that DataBank standard backup configurations were set to automatically perform daily backups of customer systems.	No exceptions noted.
		Inspected the backup configurations to verify that DataBank standard backup configurations were set to automatically perform daily backups of customer systems.	No exceptions noted.
CC9.1.3	The backup software configurations are configured to send notification to the technical support staff in the event of a job error.	Inquired of the Compliance Engineer to verify that the backup software configurations were configured to send notification to the technical support staff in the event of a job error.	No exceptions noted.
		Inspected the backup alert configurations and example alert notifications to verify that the backup software configurations were configured to send notification to the technical support staff in the event of a job error.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC9.1.4	A risk assessment is performed annually and includes identifying and assessing the risks associated with identified threats that may impair system security. Management identifies controls that mitigate the identified risks.	Inquired of the Compliance Engineer to verify that a risk assessment was performed annually and included identifying and assessing the risks associated with identified threats that may have impaired system security. Management identified controls that mitigated the identified risks.	No exceptions noted.
		Inspected the Data Center Risk Assessment to verify that a risk assessment was performed within the past 12 months and included identifying and assessing the risks associated with identified threats that may have impaired system security and management had identified controls that mitigate the identified risks.	No exceptions noted.
CC9.1.5	Management reviews the DR Plan on an annual basis to ensure that it meets DataBank's availability business requirements.	Inquired of the Compliance Engineer to verify that management reviewed the DR Plan on an annual basis to ensure that it had met DataBank's availability business requirements.	No exceptions noted.
		Inspected the Incident Response Plan and the Information System Contingency Plan to verify that management reviewed the DR Plan within the past 12 months to ensure that it had met DataBank's availability business requirements.	No exceptions noted.
CC9.1.6	Management ensures that testing of the DR Plan is completed on an annual basis.	Inquired of the Compliance Engineer to verify that management ensured that testing of the DR Plan was completed on an annual basis.	No exceptions noted.
		Inspected the Business Continuity Plan Exercise to verify that management ensured that testing of the DR Plan was completed on an annual basis.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Service agreements are executed with customers prior to on-boarding which define the terms of services provided including, but not limited to, the following: ➢ Nature, timing, and extent of services provided ➢ Roles and responsibilities ➢ Service warranties ➢ Confidentiality requirements	Inquired of the Compliance Engineer to verify that service agreements were executed with customers prior to on-boarding which defined the terms of services provided including, but not limited to, the following: ➢ Nature, timing, and extent of services provided ➢ Roles and responsibilities ➢ Service warranties ➢ Confidentiality requirements	No exceptions noted.
		Inspected executed MSAs for a sample of customers on-boarded during the examination period to verify that service agreements were executed with customers prior to on-boarding which defined the terms of services provided including, but not limited to, the following: ➢ Nature, timing, and extent of services provided ➢ Roles and responsibilities ➢ Service warranties ➢ Confidentiality requirements	No exceptions noted.
CC9.2.2	Customers who purchase network services are required to sign an agreement that outlines the prohibited uses of network services.	Inquired of the Compliance Engineer to verify that customers who purchased network services were required to sign an agreement that outlined the prohibited uses of network services.	No exceptions noted.
		Inspected executed MSAs for a sample of customers on-boarded during the examination period to verify that customers who purchased network services were required to sign an agreement that outlined the prohibited uses of network services.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC9.2.3	Databank contracts an independent third-party to perform annual SOC 1® and SOC 2® Type 2 examinations to test the controls and their effectiveness to meet control objectives and criteria identified for the services provided. This includes security and availability commitments and requirements.	Inquired of the Compliance Engineer to verify that Databank contracted an independent third-party to perform annual SOC 1® and SOC 2® Type 2 examinations to test the controls and their effectiveness to meet control objectives and criteria identified for the services provided. This included security and availability commitments and requirements.	No exceptions noted.
		Inspected the most recent SOC 1® Type 2 report to verify that within the past 12 months, Databank had contracted an independent third-party to perform SOC 1® and SOC 2® Type 2 examinations to test the controls and their effectiveness to meet control objectives and criteria identified for the services provided. This included security and availability commitments and requirements.	No exceptions noted.

Availability Category and Criteria

Information and systems are available for operation and use to meet the entity's objectives.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	Documented environmental security policies and procedures are in place to govern environmental security practices.	Inquired of the Compliance Engineer to verify that documented environmental security policies and procedures were in place to govern environmental security practices.	No exceptions noted.
		Inspected the Information Security and Standards Manual, the Documentation Book, and the Incident Monitoring and Response Procedure to verify that documented environmental security policies and procedures were in place to govern environmental security practices.	No exceptions noted.
A1.1.2	Environmental monitoring systems are utilized to monitor the environmental conditions and devices within the data centers including, but not limited to, the following: ➢ Water leakage ➢ Air handling units ➢ UPS systems ➢ Generators	Inquired of the onsite personnel for a sample of sites visited to verify that environmental monitoring systems were utilized to monitor the environmental conditions and devices within the data centers including, but not limited to, the following: ➢ Water leakage ➢ Air handling units ➢ UPS systems ➢ Generators	No exceptions noted.
		Inspected the environmental monitoring Data Center Infrastructure Management systems for a sample of sites visited to verify that environmental monitoring systems were utilized to monitor the environmental conditions and devices within the data centers including, but not limited to, the following: ➢ Water leakage ➢ Air handling units ➢ UPS systems ➢ Generators	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Observed the environmental monitoring systems during onsite activities for a sample of sites visited to verify that environmental monitoring systems were utilized to monitor the environmental conditions and devices within the data centers including, but not limited to, the following: ➢ Water leakage ➢ Air handling units ➢ UPS systems ➢ Generators	No exceptions noted.
A1.1.3	The environmental monitoring system is configured to notify security and data center personnel when predefined thresholds are exceeded on monitored devices.	Inquired of the Compliance Engineer to verify that the environmental monitoring systems were configured to notify security and data center personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
		Inspected monitoring system alert configurations for each location and examples of alert notifications to verify that the environmental monitoring systems were configured to notify security and data center personnel when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
A1.1.4	Applications are utilized to monitor the following performance, availability, and controlled events for managed services infrastructure: ➢ Availability of the network ➢ Host services and ports ➢ CPU and hard disk utilization	Inquired of the onsite personnel for a sample of sites visited to verify that applications were utilized to monitor the following performance, availability, and controlled events for managed services infrastructure: ➢ Availability of the network ➢ Host services and ports ➢ CPU and hard disk utilization	No exceptions noted.
		Observed the monitoring systems during on-site activities for a sample of sites visited to verify that applications were utilized to monitor the following performance, availability, and controlled events for managed services infrastructure: ➢ Availability of the network ➢ Host services and ports ➢ CPU and hard disk utilization	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
A1.1.5	Technical support staff are available 24 X 365 to manage data center monitoring systems which include power, temperature, humidity, video surveillance, and access control.	Inquired of the Compliance Engineer to verify that technical support staff were available 24 X 365 to manage data center monitoring systems which included power, temperature, humidity, video surveillance, and access control.	No exceptions noted.
		Inspected the on-call schedule to verify that technical support staff were available 24 X 365 to manage data center monitoring systems which included power, temperature, humidity, video surveillance, and access control.	No exceptions noted.
		Observed the technical support staff during on-site activities for a sample of sites visited to verify that they monitored the physical environment on a 24 x 365 basis, including power, temperature, humidity, video surveillance, and access control.	No exceptions noted.
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data, backup processes, and recovery infrastructure to meet its objectives.			
A1.2.1	Data center areas are equipped with fire detection and suppression systems including: ➢ Smoke detectors ➢ Audible and visual fire alarms ➢ Automated extinguisher system ➢ Hand-held fire extinguishers	Inquired of the onsite personnel for a sample of sites visited to verify that data center areas were equipped with fire detection and suppression systems including: ➢ Smoke detectors ➢ Audible and visual fire alarms ➢ Automated extinguisher system ➢ Hand-held fire extinguishers	No exceptions noted.
		Observed the fire detection and suppression equipment during onsite activities for a sample of sites visited to verify that data center areas were equipped with fire detection and suppression systems including: ➢ Smoke detectors ➢ Audible and visual fire alarms ➢ Automated extinguisher system ➢ Hand-held fire extinguishers	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
A1.2.2	On an annual basis, management contracts third-party vendors to complete fire detection and suppression equipment inspections.	Inquired of the Compliance Engineer to verify that on an annual basis, management contracted third-party vendors to complete fire detection and suppression equipment inspections.	No exceptions noted.
		Inspected the fire detection and suppression inspection reports for each location to verify that management contracted third-party vendors to complete fire detection and suppression equipment inspections within the past 12 months.	No exceptions noted.
		Observed fire extinguisher service dates during onsite activities to verify that management contracted third-party vendors to complete fire detection and suppression equipment inspections within the past 12 months.	No exceptions noted.
A1.2.3	Data center areas are equipped with multiple dedicated air handling units.	Inquired of the onsite personnel for a sample of sites visited to verify that data center areas were equipped with multiple dedicated air handling units.	No exceptions noted.
		Observed the air handling units during on-site activities for a sample of sites visited to verify that data center areas were equipped with multiple dedicated air handling units.	No exceptions noted.
A1.2.4	On an annual basis, management contracts third-party vendors to complete inspections on the air handling units.	Inquired of the Compliance Engineer to verify that on an annual basis, management contracted third-party vendors to complete inspections on the air handling units.	No exceptions noted.
		Inspected the most recent air handling unit inspection reports for each location to verify that within the past 12 months, management contracted third-party vendors to complete inspections on the air handling units.	No exceptions noted.
A1.2.5	Data center areas are equipped with water detection devices to detect and mitigate the risk of water damage in the event of a flood or water leak.	Inquired of the onsite personnel for a sample of sites visited to verify that data center areas were equipped with water detection devices to detect and mitigate the risk of water damage in the event of a flood or water leak.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Observed the water detection devices during onsite activities for a sample of sites visited to verify that data center areas were equipped with water detection devices to detect and mitigate the risk of water damage in the event of a flood or water leak.	No exceptions noted.
A1.2.6	Data center areas are available with raised flooring and/or server racks to elevate equipment and help facilitate cooling.	Inquired of the onsite personnel for a sample of sites visited to verify that data center areas were available with raised flooring and/or server racks to elevate equipment and help facilitate cooling.	No exceptions noted.
		Observed the flooring and server racks during onsite activities for a sample of sites visited to verify that data center areas were available with raised flooring and/or server racks to elevate equipment and help facilitate cooling.	No exceptions noted.
A1.2.7	For data centers with raised floors, floor tiles are grounded and covered with an anti-static covering to reduce the occurrence of electro-static buildup.	Inquired of the onsite personnel for a sample of sites visited to verify that for data centers with raised floors, floor tiles were grounded and covered with an anti-static covering to reduce the occurrence of electro-static buildup.	No exceptions noted.
		Observed the data center floors during onsite activities for a sample of sites visited to verify that for data centers with raised floors, floor tiles were grounded and covered with an anti-static covering to reduce the occurrence of electro-static buildup.	No exceptions noted.
A1.2.8	Power infrastructure is designed and constructed redundantly to mitigate risk to customer systems and services.	Inquired of the onsite personnel for a sample of sites visited to verify that power infrastructure was designed and constructed redundantly to mitigate risk to customer systems and services.	No exceptions noted.
		Observed the utility feeds and power distribution units during onsite activities for a sample of sites visited to verify that power infrastructure was designed and constructed redundantly to mitigate risk to customer systems and services.	No exceptions noted.
A1.2.9	The data centers have redundant electrical utility feeds.	Inquired of the onsite personnel for a sample of sites visited to verify that the data centers had redundant electrical utility feeds.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Observed the data centers during onsite activities for a sample of sites visited to verify that they had redundant electrical utility feeds.	No exceptions noted.
A1.2.10	Data center power systems are constructed with redundant UPS units.	Inquired of onsite personnel for a sample of sites visited to verify that data center power systems were constructed with redundant UPS units.	No exceptions noted.
		Observed the UPS units at during onsite activities for a sample of sites visited that data center power systems were constructed with redundant UPS units.	No exceptions noted.
A1.2.11	UPS systems are equipped with maintenance bypass or "wrap around" breakers and can be isolated from the protected load during UPS maintenance.	Inquired of the onsite personnel for a sample of sites visited to verify that UPS systems were equipped with maintenance bypass or "wrap around" breakers and could be isolated from the protected load during UPS maintenance.	No exceptions noted.
		Observed the UPS units during onsite activities for a sample of sites visited to verify that they were equipped with maintenance bypass or "wrap around" breakers and could be isolated from the protected load during UPS maintenance.	No exceptions noted.
A1.2.12	On an annual basis, management contracts third-party vendors to complete inspections of the UPS systems.	Inquired of the Compliance Engineer to verify that on an annual basis, management contracted third-party vendors to complete inspections of the UPS systems.	No exceptions noted.
		Inspected the most recent UPS inspection reports for each location to verify that management had contracted third-party vendors to complete inspections of the UPS systems within the past 12 months.	No exceptions noted.
A1.2.13	On an annual basis, management contracts third-party vendors to perform scheduled service and load bank testing of the generators.	Inquired of the Compliance Engineer to verify that, on an annual basis, management contracted third-party vendors to perform scheduled service and load bank testing of the generators.	No exceptions noted.
		Inspected the most recent load bank testing reports from each location to verify that management contracted third-party vendors to perform scheduled service and load bank testing of the generators within the past 12 months.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
A1.2.14	An incident ticketing system is utilized to document, prioritize, escalate, and help resolve problems affecting services provided.	Inquired of the Compliance Engineer to verify that an incident ticketing system was utilized to document, prioritize, escalate, and help resolve problems that affected services provided.	No exceptions noted.
		Inspected incident tickets for a sample of identified incidents during the examination period to verify that an incident ticketing system was utilized to document, prioritize, escalate, and help resolve problems that affected services provided.	No exceptions noted.
A1.2.15	DataBank maintains policy and procedure manuals for backup, storage, and restoration procedures.	Inquired of the Compliance Engineer to verify that DataBank maintained policy and procedure manuals for backup, storage, and restoration procedures.	No exceptions noted.
		Inspected the Information System Contingency Plan to verify that DataBank maintained policy and procedure manuals for backup, storage, and restoration procedures.	No exceptions noted.
A1.2.16	DataBank standard backup configuration is set to automatically perform daily backups of customer systems.	Inquired of the Compliance Engineer to verify that DataBank standard backup configurations were set to automatically perform daily backups of customer systems.	No exceptions noted.
		Inspected the backup configurations to verify that DataBank standard backup configurations were set to automatically perform daily backups of customer systems.	No exceptions noted.
A1.2.17	Management reviews the DR Plan on an annual basis to ensure that it meets DataBank's availability business requirements.	Inquired of the Compliance Engineer to verify that management reviewed the DR Plan on an annual basis to ensure that it had met DataBank's availability business requirements.	No exceptions noted.
		Inspected the Incident Response Plan and the Information System Contingency Plan to verify that management reviewed the DR Plan within the past 12 months to ensure that it had met DataBank's availability business requirements.	No exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Management reviews the DR Plan on an annual basis to ensure that it meets DataBank's availability business requirements.	Inquired of the Compliance Engineer to verify that management reviewed the DR Plan on an annual basis to ensure that it had met DataBank's availability business requirements.	No exceptions noted.
		Inspected the Incident Response Plan and the Information System Contingency Plan to verify that management reviewed the DR Plan within the past 12 months to ensure that it had met DataBank's availability business requirements.	No exceptions noted.
A1.3.2	Management ensures that testing of the DR Plan is completed on an annual basis.	Inquired of the Compliance Engineer to verify that management ensured that testing of the DR Plan was completed on an annual basis.	No exceptions noted.
		Inspected the Business Continuity Plan Exercise to verify that management ensured that testing of the DR Plan was completed on an annual basis.	No exceptions noted.