

Hiestand, Brand, Loughran, P.A.

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

DATABANK HOLDINGS, LTD.

OCTOBER 1, 2017 TO SEPTEMBER 30, 2018



D A T A B A N K



An Affiliate Company of
360[°] ADVANCED

DATABANK HOLDINGS, LTD.

Table of Contents

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2: MANAGEMENT'S ASSERTION	5
SECTION 3: DATABANK'S DESCRIPTION OF CONTROLS	8
SCOPE OF REPORT AND DISCLOSURES	9
Overview	9
Principles and Related Criteria	9
Significant Changes during the Examination Period	12
Subsequent Events	12
Using the Work of the Internal Audit Function	12
OVERVIEW OF OPERATIONS AND THE SYSTEM	13
Company Overview and Background	13
Overview of Data Center Services System	13
Infrastructure	14
Software	14
People	15
Procedures	17
Data	17
RELEVANT ASPECTS OF CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATIONS SYSTEMS, MONITORING, POLICIES AND PRACTICES	18
Control Environment	18
Risk Assessment	20
Information and Communication Systems	21
Monitoring	22
Policies and Practices	23
PRINCIPLES, CRITERIA, AND RELATED CONTROLS	27
COMPLEMENTARY CONTROL CONSIDERATIONS	28
SECTION 4: PRINCIPLES, CRITERIA, CONTROL DESCRIPTIONS, RELATED CONTROLS AND TESTS OF OPERATING EFFECTIVENESS	30
INFORMATION PROVIDED BY THE SERVICE AUDITOR	31
Introduction	31
Tests of Operating Effectiveness	31
Types of Tests Performed	32
Data Centers Physically Inspected through Onsite Procedures	32
Sampling Methodology	33
PRINCIPLES, CRITERIA, AND RELATED CONTROLS	34
Security Principle and Criteria (Common Criteria to All Principles)	34
Availability Principle and Criteria	78

SECTION 1:

INDEPENDENT SERVICE AUDITOR'S REPORT

Hiestand, Brand, Loughran, P.A.

INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION OF A SERVICE ORGANIZATION'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS RELEVANT TO SECURITY AND AVAILABILITY

To DataBank Holdings, Ltd.:

Scope

We have examined the description of DataBank Holdings, Ltd.'s ("DataBank") Data Center Services system based on the criteria set forth in paragraph 1.26 of the AICPA Guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the Security and Availability principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria), throughout the period October 1, 2017 to September 30, 2018.

The description indicates that certain applicable trust services criteria specified in the description can be met only if complementary user entity controls assumed in the design of DataBank's controls are suitably designed and operating effectively, along with the related controls of the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls. The controls included in the description are those that management of DataBank believes are likely to be relevant to meeting the applicable trust services criteria, and the description does not include those aspects of the Data Center Services system that are not likely to be relevant to meeting the applicable trust services criteria.

Service Organization's Responsibilities

Within Section 2 of this report, DataBank has provided an assertion about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. DataBank is responsible for (1) preparing the description and assertion; (2) including the completeness, accuracy, and method of presentation of the description and assertion; (3) providing the services covered by the description; (4) identifying the risks that would prevent the applicable trust services criteria from being met; (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria; and (6) specifying the controls that meet the applicable trust services criteria and stating them in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period October 1, 2017 to September 30, 2018.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria involves:

- evaluating and performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period October 1, 2017 to September 30, 2018;
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively;

- testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met; and
- evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization in its assertion.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the description criteria identified in DataBank's assertion and the applicable trust services criteria:

- a. the description fairly presents the system that was designed and implemented throughout the period October 1, 2017 to September 30, 2018;
- b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period October 1, 2017 to September 30, 2018, and user entities applied the complementary user entity controls assumed in the design of DataBank's controls throughout the period October 1, 2017 to September 30, 2018; and
- c. the controls tested operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period October 1, 2017 to September 30, 2018 if the user entities applied the complementary user entity controls assumed in the design of DataBank's controls, and those controls operated effectively throughout the period October 1, 2017 to September 30, 2018.

Description of Tests of Controls

The specific controls we tested, the tests we performed, and the results of our tests are presented in Section 4 of this report.

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 and user entities of DataBank's Data Center Services system during some or all of the period October 1, 2017 to September 30, 2018; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, and other parties;
- Internal control and its limitations;
- The nature of user entity controls and responsibilities, and their role in the user entities internal control as they relate to, and how they interact with, related controls at the service organization to meet the applicable trust services criteria;
- The applicable trust services criteria; and

- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

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

Hiestand, Brand, Hughes PA.

November 27, 2018
St. Petersburg, Florida

SECTION 2:

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

November 27, 2018

We have prepared the description of DataBank Holdings, Ltd.'s ("DataBank") Data Center Services system based on the criteria for a description of a service organization's system identified in paragraph 1.26 of the AICPA Guide, *Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria). The description is intended to provide users with information about the Data Center Services, particularly system controls intended to meet the criteria for the Security and Availability principles set forth in TSP Section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services principles), throughout the period October 1, 2017 to September 30, 2018. We confirm, to the best of our knowledge and belief, that

- 1) The description fairly presents the Data Center Services system throughout the period October 1, 2017 to September 30, 2018. Our assertion is based on the following description criteria:
 - a) The description contains the following information:
 1. the types of services provided;
 2. the components of the system used to provide the services, which are the following:
 - *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; and
 - *Data* – transaction streams, files, databases, tables, and output used or processed by the system.
 3. the boundaries or aspects of the system covered by the description;
 4. for information provided to, or received from, sub-service organizations, and other parties:
 - a. how such information is provided or received and the role of the sub-service organization and other parties; and
 - b. the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.
 5. the applicable trust services criteria and related controls designed to meet those criteria, including, as applicable, the following:
 - a. complementary user entity controls contemplated in the design of the service organization's system; and
 - b. when the inclusive method is used to present a sub-service organization, controls at the sub-service organization.
 6. if the service organization presents the sub-service organization using the carve-out method:
 - a. the nature of the services provided by the sub-service organization; and

- b. each of the applicable trust services criteria that are intended to be met by controls at the sub-service organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out sub-service organizations to meet those criteria.
 - 7. any applicable trust services criteria that are not addressed by a control at the service organization or a sub-service organization and the reasons; and
 - 8. relevant details of changes to the service organization's system during the period covered by the description.
- b) The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.
- 2) The controls in the description were suitably designed throughout the period October 1, 2017 to September 30, 2018, to meet the applicable trust services criteria.
- 3) The controls stated in the description operated effectively throughout the period October 1, 2017 to September 30, 2018, to meet the applicable trust services criteria.

/s/ DataBank Holdings, Ltd.

Mark A. Houpt – Chief Information Security Officer

Kevin Ooley – President

SECTION 3:

DATABANK'S DESCRIPTION OF CONTROLS

SCOPE OF REPORT AND DISCLOSURES

Overview

This description of the system of controls provided by DataBank Holdings, 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.

Principles and Related Criteria

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

- **Security:** The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements. The *security principle* refers to the protection of the system resources through logical and physical access control measures in order to enable the entity to meet its commitments and system requirements related to security, availability, processing integrity, confidentiality, and privacy. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of data or system resources, misuse of software, and improper access to, or use of, alteration, destruction, or disclosure of information.
- **Availability:** The system is available for operation and use to meet the entity's commitments and system requirements. The *availability principle* refers to the accessibility of the system, products, or services as committed by contract, service-level agreement, or other agreements. This principle does not, in itself, set a minimum acceptable performance level for system availability. The *availability principle* does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to the performance of specific tasks or problems), but does address whether the system includes controls to support system accessibility for operation, monitoring, and maintenance.
- **Processing Integrity:** System processing is complete, valid, accurate, timely, and authorized to meet the entity's commitments and system requirements. The *processing integrity principle* refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether the system achieves its aim or the purpose for which it exists, and whether it performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation. Processing integrity does not automatically imply that the information received and stored by the system is complete, valid, accurate, current, and authorized. The risk that data contains errors introduced prior to its input in the system often cannot be addressed by system controls and detecting such errors is not usually the responsibility of the entity. Similarly, users outside the boundary of the system may be responsible for initiating processing. In these instances, the data may become invalid, inaccurate, or otherwise inappropriate even though the system is processing with integrity.
- **Confidentiality:** Information designated as confidential is protected to meet the entity's commitments and system requirements. The *confidentiality principle* addresses the system's ability to protect information designated as confidential, including, its final disposition and removal from the system in accordance with management's commitments and system requirements. 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. Such requirements may be contained in laws or regulations, or commitments in user contracts. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy only applies to personal information, while the confidentiality principle applies to various types of sensitive information. In addition, the privacy principle 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 commitments and system requirements.

Many of the criteria used to evaluate a system are shared amongst all of the principles; for example, the criteria related to risk management apply to the security, availability, processing integrity, confidentiality, and privacy principles. As a result, the trust services criteria of (1) criteria common to all five principles (common criteria) and (2) additional principle specific criteria for the availability, processing integrity, confidentiality, and privacy principles. For the security principle, the common criteria constitute the complete set of criteria. For the principles of availability, processing integrity, confidentiality, and privacy, a complete set of criteria consists of the common criteria and the criteria applicable to the principles addressed by the engagement. The criteria for a principle addressed by the engagement are considered to be complete only if all of the criteria associated with that principle are addressed by the engagement.

The common criteria are organized into seven categories:

- a. *Organization and management.* The criteria relevant to how the organization is structured and the processes the entity has implemented to manage and support people within its operating units to meet the criteria for the principles addressed by the engagement. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.
- b. *Communications.* The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and system requirements to authorized users and other parties of the system to meet the criteria for the principles addressed by the engagement.
- c. *Risk management and design and implementation of controls.* The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process to meet the criteria for the principles addressed by the engagement.
- d. *Monitoring of controls.* The criteria relevant to how the entity monitors the system, including the suitability of the design and operating effectiveness of the controls, and takes action to address deficiencies identified to meet the criteria for the principles addressed by the engagement.
- e. *Logical and physical access controls.* The criteria relevant to how the entity restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principles addressed in the engagement.
- f. *System operations.* The criteria relevant to how the entity manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the criteria for the principles addressed in the engagement.
- g. *Change management.* The criteria relevant to how the entity identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principles addressed in the engagement.

Although the confidentiality principle applies to various types of sensitive information, the privacy principle applies only to personal information. If the entity is directly responsible for providing services to data subjects covering all of the categories noted as follows, then the privacy principle may be appropriate. If the entity is not directly responsible for significant aspects of the following categories but retains responsibility for protecting personal information, the confidentiality principle may be more applicable.

The privacy criteria are organized into eight categories:

- a. *Notice and communication of commitments and system requirements.* The entity provides notice to data subjects about its privacy practices, its privacy commitments, and system requirements.
- b. *Choice and consent.* The entity communicates choice 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 privacy commitments and system requirements.
- d. *Use, retention, and disposal.* The entity limits use, retention, and disposal of personal information to meet its privacy commitments and system requirements.
- e. *Access.* The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its privacy commitments and system requirements.
- f. *Disclosure and notifications.* The entity discloses personal information, with the consent of the data subjects, to meet its privacy commitments and system requirements. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its privacy commitments and system requirements.
- g. *Quality.* The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its privacy commitments and system requirements.
- h. *Monitoring and enforcement.* The entity monitors compliance to meet its privacy commitments and system requirements including procedures to address privacy-related inquiries, complaints, and disputes.

The scope management has determined appropriate for the Data Center Services system includes the controls to meet the criteria for the Security and Availability principles. DataBank is responsible for identification of risks associated with the system of controls (defined as Principles), 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 13 Databank data center locations listed below:

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 (2) MCI1, and MCI2;
- Eagan, Minnesota (1) MSP2; and
- 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 (2) SLC2, and SLC3;
- Pittsburgh, Pennsylvania (1) PIT1; and
- Cleveland, Ohio (1) CLE1.

Sub-Service Organizations

DataBank Holdings, Ltd. 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

Management is not aware of any significant changes that occurred during the examination period.

Subsequent Events

Subsequent to the period of this examination, and on November 15, 2018, DataBank's Kansas City #3 (MCI3) data center went live. This location was not included within the scope 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 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.

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; and
- 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 Martyněk 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. Martyněk 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. Martyněk 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. Martyněk 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. Martyněk earned a Bachelor of Arts in Political Science from Binghamton University and received a Master 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. 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.
- **Vice President of Marketing:** Stacey Levas joined DataBank in September of 2017. Previously, Mrs. Levas served as Vice President of Marketing at Edge Hosting. There she led marketing strategy, product marketing, and demand generation. She brings over 20 years of experience in creating market value for healthcare-related and IT service companies. Before joining Edge, Mrs. Levas consulted for several data analytics start-ups and a financial software application company. Throughout her career, Mrs. Levas has approached marketing with a sense of pragmatism and a persistent focus on customer experience. As Vice President of Marketing for Health Market Science (HMS), Mrs. Levas led commercial efforts to drive product messaging and differentiation, contributing to an average of 30% year-over-year growth and a successful exit to LexisNexis Risk Solutions. Mrs. Levas held a variety of marketing management roles at Gene Logic, Cambrex Bio Science (now Lonza), RWD Technologies (now GP Strategies) and CSC. Mrs. Levas holds a Bachelor's degree in Art History and Psychology from New York University and a Master of Science in Marketing from The Johns Hopkins University Carey School of Business.

Procedures

DataBank has developed, and communicated to its users, procedures to restrict physical and logical access to DataBank's facilities, systems, and its data halls and critical areas within, as well as procedures to protect the facilities from certain environmental threats. Policies include the following:

- DataBank Data Center Security Policy;
- Information Security Policy (which encompasses all eighteen (18) families of NIST SP800-53R4).;
- Data Center Physical Security;
- Data Center Environmental Security Policy; and
- Incident and Response Policy.

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.

Management Committee

DataBank's control consciousness is influenced significantly by its 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 SP800-37. 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; and
- 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.

Policies and Practices

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.

INFRASTRUCTURE MANAGEMENT

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 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 notice 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 to 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, 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.

PRINCIPLES, CRITERIA, AND RELATED CONTROLS

The principles, criteria, and related controls are included in Section 4 of this report, “Principles, 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 principles 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 the principles and criteria 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 controls and their own internal controls. DataBank management does not make any representations regarding responsibility related to or provide any assurance in regard 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 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 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 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:

PRINCIPLES, 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 principles, criteria, and the related controls specified by DataBank and contained within Section 4 of this report, which management believes to be the relevant key controls for the principles and criteria included in the scope of this report. Our review was not extended to controls in place at any user entities or any other third-party vendors.

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 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 principle during the period from October 1, 2017 to September 30, 2018. 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 principle 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 principle.

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 principle are presented in this section under the column heading "Results of Testing". 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 principles are presented in relation to the nature of services being audited and the controls specified by DataBank.

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: <ul style="list-style-type: none">➤ 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: <ul style="list-style-type: none">➤ 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

Data Centers Physically Inspected through Onsite Procedures

Below is the listing of DataBank data centers physically inspected by 360 Advanced examiners through onsite procedures during the period.

- DFW3;
- MCI1;
- MCI2;
- MSP2;
- BW11;
- SLC2; and
- SLC3.

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.

PRINCIPLES, CRITERIA, AND RELATED CONTROLS

Security Principle and Criteria (Common Criteria to All Principles)

The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC1.0 Organization and Management: The criteria relevant to how the organization is structured and the processes the entity has implemented to manage and support people within its operating units to meet the criteria for the principle(s) addressed by the engagement. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.			
CC1.1 The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, maintenance operation, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to Security and Availability			
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 relevant 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 relevant 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: <ul style="list-style-type: none"> ➤ 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: <ul style="list-style-type: none"> ➤ Information Sensitivity ➤ Physical Security ➤ Environmental Security ➤ Incident Response 	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		<p>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:</p> <ul style="list-style-type: none"> ➤ Information Sensitivity ➤ Physical Security ➤ Environmental Security ➤ Incident Response 	No relevant exceptions noted.
CC1.1.3	New client procedures are documented in a new client checklist to guide personnel during the new client process.	Inquired of the Compliance Engineer to verify that new client procedures were documented in a new client checklist to guide personnel during the new client process.	No relevant exceptions noted.
		Inspected the new client checklists for a sample of customers on-boarded during the examination period to verify that new client procedures were documented in a new client checklist to guide personnel during the new client process.	No relevant exceptions noted.
CC1.1.4	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 relevant exceptions noted.
		Inspected the job descriptions to verify that roles and responsibilities were defined in written job descriptions.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC1.2 Responsibility and accountability for designing, developing, implementing, operating, maintaining monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to Security and Availability			
CC1.2.1	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 relevant exceptions noted.
		Inspected the job descriptions to verify that roles and responsibilities were defined in written job descriptions.	No relevant exceptions noted.
CC1.2.2	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 relevant 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 relevant exceptions noted.
CC1.3 The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting Security and Availability and provides resources necessary for personnel to fulfill their responsibilities.			
CC1.3.1	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 relevant exceptions noted.
		Inspected the job descriptions to verify that roles and responsibilities were defined in written job descriptions.	No relevant exceptions noted.
CC1.3.2	Personnel are required to attend annual security, confidentiality, and privacy training.	Inquired of the Compliance Engineer to verify that personnel were required to attend annual security, confidentiality, and privacy training.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the training completion report for a sample of personnel employed during the examination period to verify that personnel were required to attend annual security, confidentiality, and privacy training.	No relevant exceptions noted.
CC1.3.3	Background screenings are performed for employment candidates as a component of the hiring process.	Inquired of the onsite personnel to verify that background screenings were performed for employment candidates as a component of the hiring process.	No relevant 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 relevant exceptions noted.
CC1.4 The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to Security and Availability			
CC1.4.1	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 relevant 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 relevant exceptions noted.
CC1.4.2	Background screenings are performed for employment candidates as a component of the hiring process.	Inquired of the onsite personnel to verify that background screenings were performed for employment candidates as a component of the hiring process.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		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 relevant exceptions noted.
CC2.0 Communications: The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and uses to the effective operation of the system.			
CC2.1 Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users to permit users to understand their role in the system and the results of system operation.			
CC2.1.1	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: <ul style="list-style-type: none"> ➤ 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: <ul style="list-style-type: none"> ➤ Information Sensitivity ➤ Physical Security ➤ Environmental Security ➤ Incident Response 	No relevant 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: <ul style="list-style-type: none"> ➤ Information Sensitivity ➤ Physical Security ➤ Environmental Security ➤ Incident Response 	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.1.2	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 relevant exceptions noted.
		Inspected the DataBank documentation repository on company intranet to verify that documented policies and procedures for significant processes were available to personnel on Databank's shared document repository.	No relevant exceptions noted.
CC2.1.3	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 relevant exceptions noted.
		Inspected the Information System Contingency Plan to verify that DataBank maintained policy and procedure manuals for backup, storage, and restoration procedures.	No relevant exceptions noted.
CC2.1.4	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 relevant exceptions noted.
		Inspected the Information Security Policy and Standards Manual to verify that DataBank maintained policy and procedure manuals for internal network infrastructure and user organization system availability and monitoring.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.1.5	<p>Service agreements are executed with customers prior to on-boarding which define the terms of services provided including, but not limited to, the following:</p> <ul style="list-style-type: none"> ➤ Nature, timing, and extent of services provided ➤ Roles and responsibilities ➤ Service warranties ➤ Confidentiality requirements 	<p>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:</p> <ul style="list-style-type: none"> ➤ Nature, timing, and extent of services provided ➤ Roles and responsibilities ➤ Service warranties ➤ Confidentiality requirements 	No relevant exceptions noted.
		<p>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:</p> <ul style="list-style-type: none"> ➤ Nature, timing, and extent of services provided ➤ Roles and responsibilities ➤ Service warranties ➤ Confidentiality requirements 	No relevant exceptions noted.
CC2.1.6	<p>Customers who purchase network services are required to sign an agreement that outlines the prohibited uses of network services.</p>	<p>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.</p>	No relevant exceptions noted.
		<p>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.</p>	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.2 The entity's Security and Availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.			
CC2.2.1	<p>Service agreements are executed with customers prior to on-boarding which define the terms of services provided including, but not limited to, the following:</p> <ul style="list-style-type: none"> ➤ Nature, timing, and extent of services provided ➤ Roles and responsibilities ➤ Service warranties ➤ Confidentiality requirements 	<p>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:</p> <ul style="list-style-type: none"> ➤ Nature, timing, and extent of services provided ➤ Roles and responsibilities ➤ Service warranties ➤ Confidentiality requirements 	No relevant exceptions noted.
		<p>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:</p> <ul style="list-style-type: none"> ➤ Nature, timing, and extent of services provided ➤ Roles and responsibilities ➤ Service warranties ➤ Confidentiality requirements 	No relevant exceptions noted.
CC2.2.2	<p>Customers who purchase network services are required to sign an agreement that outlines the prohibited uses of network services.</p>	<p>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.</p>	No relevant exceptions noted.
		<p>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.</p>	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.2.3	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 relevant exceptions noted.
		Inspected the DataBank Share Drive on company intranet to verify that documented policies and procedures for significant processes were available to personnel on Databank's shared document repository.	No relevant exceptions noted.
CC2.2.4	Personnel are required to attend annual security, confidentiality, and privacy training.	Inquired of the Compliance Engineer to verify that personnel were required to attend annual security, confidentiality, and privacy training.	No relevant exceptions noted.
		Inspected the training completion report for a sample of personnel employed during the examination period to verify that personnel were required to attend annual security, confidentiality, and privacy training.	No relevant exceptions noted.
CC2.3 The responsibility of internal and external users and other whose roles affect system operation are communicated to those parties.			
CC2.3.1	<p>Service agreements are executed with customers prior to on-boarding which define the terms of services provided including, but not limited to, the following:</p> <ul style="list-style-type: none"> ➤ Nature, timing, and extent of services provided ➤ Roles and responsibilities ➤ Service warranties ➤ Confidentiality requirements 	<p>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:</p> <ul style="list-style-type: none"> ➤ Nature, timing, and extent of services provided ➤ Roles and responsibilities ➤ Service warranties ➤ Confidentiality requirements 	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		<p>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:</p> <ul style="list-style-type: none"> ➤ Nature, timing, and extent of services provided ➤ Roles and responsibilities ➤ Service warranties ➤ Confidentiality requirements 	No relevant exceptions noted.
CC2.3.2	Personnel are required to attend annual security, confidentiality, and privacy training.	Inquired of the Compliance Engineer to verify that personnel were required to attend annual security, confidentiality, and privacy training.	No relevant exceptions noted.
		Inspected the training completion report for a sample of personnel employed during the examination period to verify that personnel were required to attend annual security, confidentiality, and privacy training.	No relevant exceptions noted.
CC2.3.3	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 relevant 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 relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.4 Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the Security and Availability of the system, is provided to personnel to carry out their responsibilities.			
CC2.4.1	<p>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:</p> <ul style="list-style-type: none"> ➤ Information Sensitivity ➤ Physical Security ➤ Environmental Security ➤ Incident Response 	<p>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:</p> <ul style="list-style-type: none"> ➤ Information Sensitivity ➤ Physical Security ➤ Environmental Security ➤ Incident Response 	No relevant exceptions noted.
		<p>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:</p> <ul style="list-style-type: none"> ➤ Information Sensitivity ➤ Physical Security ➤ Environmental Security ➤ Incident Response 	No relevant exceptions noted.
CC2.4.2	<p>Service agreements are executed with customers prior to on-boarding which define the terms of services provided including, but not limited to, the following:</p> <ul style="list-style-type: none"> ➤ Nature, timing, and extent of services provided ➤ Roles and responsibilities ➤ Service warranties ➤ Confidentiality requirements 	<p>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:</p> <ul style="list-style-type: none"> ➤ Nature, timing, and extent of services provided ➤ Roles and responsibilities ➤ Service warranties ➤ Confidentiality requirements 	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		<p>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:</p> <ul style="list-style-type: none"> ➤ Nature, timing, and extent of services provided ➤ Roles and responsibilities ➤ Service warranties ➤ Confidentiality requirements 	No relevant exceptions noted.
CC2.4.3	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 relevant exceptions noted.
		Inspected the job descriptions to verify that roles and responsibilities were defined in written job descriptions.	No relevant exceptions noted.
CC2.5 Internal and external users have been provided with information on how to report Security and Availability failures, incidents, concerns, and other complaints to appropriate personnel.			
CC2.5.1	<p>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:</p> <ul style="list-style-type: none"> ➤ Information Sensitivity ➤ Physical Security ➤ Environmental Security ➤ Incident Response 	<p>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:</p> <ul style="list-style-type: none"> ➤ Information Sensitivity ➤ Physical Security ➤ Environmental Security ➤ Incident Response 	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		<p>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:</p> <ul style="list-style-type: none"> ➤ Information Sensitivity ➤ Physical Security ➤ Environmental Security ➤ Incident Response 	No relevant exceptions noted.
CC2.6 System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to Security and Availability are communicated to those users in a timely manner.			
CC2.6.1	<p>Service agreements are executed with customers prior to on-boarding which define the terms of services provided including, but not limited to, the following:</p> <ul style="list-style-type: none"> ➤ Nature, timing, and extent of services provided ➤ Roles and responsibilities ➤ Service warranties ➤ Confidentiality requirements 	<p>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:</p> <ul style="list-style-type: none"> ➤ Nature, timing, and extent of services provided ➤ Roles and responsibilities ➤ Service warranties ➤ Confidentiality requirements 	No relevant exceptions noted.
		<p>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:</p> <ul style="list-style-type: none"> ➤ Nature, timing, and extent of services provided ➤ Roles and responsibilities ➤ Service warranties ➤ Confidentiality requirements 	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.6.2	<p>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:</p> <ul style="list-style-type: none"> ➤ Information Sensitivity ➤ Physical Security ➤ Environmental Security ➤ Incident Response 	<p>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:</p> <ul style="list-style-type: none"> ➤ Information Sensitivity ➤ Physical Security ➤ Environmental Security ➤ Incident Response 	No relevant exceptions noted.
		<p>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:</p> <ul style="list-style-type: none"> ➤ Information Sensitivity ➤ Physical Security ➤ Environmental Security ➤ Incident Response 	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC3.0 Risk Management and Design and Implementation of Controls: The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.			
CC3.1 The entity (1) identifies potential threats that could impair system Security and Availability commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and other with access to the system), (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods and services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.			
CC3.1.1	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 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 relevant 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 relevant exceptions noted.
CC3.1.2	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 within the past 12 months.	No relevant 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 relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC3.1.3	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 relevant exceptions noted.
		Inspected the incident 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 relevant exceptions noted.
CC3.2 The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy, reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities, and updates the controls, as necessary.			
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 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 relevant 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 relevant 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 within the past 12 months.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the most recent vulnerability assessments to verify that a third-party vendor performed an external vulnerability assessment within the past 12 months.	No relevant exceptions noted.
CC4.0 Monitoring Controls: The criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.			
CC4.1 The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to Security and Availability, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.			
CC4.1.1	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 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 relevant 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 relevant exceptions noted.
CC4.1.2	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 within the past 12 months.	No relevant 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 relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC4.1.3	<p>Environmental monitoring systems are utilized to monitor the environmental conditions and devices within the data centers including, but not limited to, the following:</p> <ul style="list-style-type: none"> ➤ Water leakage ➤ Air handling units ➤ UPS systems ➤ Generators 	<p>Inquired of the onsite personnel 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:</p> <ul style="list-style-type: none"> ➤ Water leakage ➤ Air handling units ➤ UPS systems ➤ Generators 	No relevant exceptions noted.
		<p>Inspected the environmental monitoring Data Center Infrastructure Management systems at each location 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:</p> <ul style="list-style-type: none"> ➤ Water leakage ➤ Air handling units ➤ UPS systems ➤ Generators 	No relevant exceptions noted.
		<p>Observed the environmental monitoring systems during onsite activities 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:</p> <ul style="list-style-type: none"> ➤ Water leakage ➤ Air handling units ➤ UPS systems ➤ Generators 	No relevant exceptions noted.
CC4.1.4	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 relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		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 relevant exceptions noted.
CC5.0 Logical and Physical Access Controls: The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.			
CC5.1 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to Security and Availability			
(1) identification and authentication of internal and external users;			
CC5.1.1	Workstations are restricted to authorized employees via unique user names and passwords.	Inquired of the Compliance Engineer to verify that workstations were restricted to authorized employees via unique user names and passwords.	No relevant exceptions noted.
		Inspected the Default Domain Policy to verify that workstations were restricted to authorized employees via unique user names and passwords.	No relevant exceptions noted.
CC5.1.2	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 relevant 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 relevant exceptions noted.
CC5.1.3	A client authorized requestor list is maintained for each client that lists the authorized client contacts with the ability to initiate changes to subscribed services.	Inquired of the Compliance Engineer to verify that a client authorized requestor list was maintained for each client that listed the authorized client contacts with the ability to initiate changes to subscribed services.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the authorized client contact listing to verify that a client authorized requestor list was maintained for each client that listed the authorized client contacts with the ability to initiate changes to subscribed services.	No relevant exceptions noted.
CC5.1.4	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 relevant exceptions noted.
		Inspected customer access change request communications for a sample of customer badge access change requests 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 relevant exceptions noted.
(2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements;			
CC5.1.5	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 relevant 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 relevant exceptions noted.
CC5.1.6	VPN sessions require unique user names and password authentication.	Inquired of the Compliance Engineer to verify that VPN sessions required unique user names and password authentication.	No relevant 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 user names and password authentication.	No relevant exceptions noted.
CC5.1.7	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 relevant 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 relevant exceptions noted.
CC5.1.8	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 relevant exceptions noted.
		Inspected the firewall change tickets for a sample of client firewall changes requested 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 relevant exceptions noted.
(3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to Security and Availability			
CC5.1.9	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 within the past 12 months.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the most recent vulnerability assessments to verify that a third-party vendor performed an external vulnerability assessment within the past 12 months.	No relevant exceptions noted.
CC5.1.10	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 relevant 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 relevant exceptions noted.
CC5.1.11	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 relevant 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 relevant exceptions noted.
CC5.1.12	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 relevant 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 relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.2 New internal and external users, whose access is administered by the entity, are registered, and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC5.2.1	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 relevant 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 relevant exceptions noted.
CC5.2.2	Workstations are restricted to authorized employees via unique user names and passwords.	Inquired of the Compliance Engineer to verify that workstations were restricted to authorized employees via unique user names and passwords.	No relevant exceptions noted.
		Inspected the Default Domain Policy to verify that workstations were restricted to authorized employees via unique user names and passwords.	No relevant exceptions noted.
CC5.2.3	A client authorized requestor list is maintained for each client that lists the authorized client contacts with the ability to initiate changes to subscribed services.	Inquired of the Compliance Engineer to verify that a client authorized requestor list was maintained for each client that listed the authorized client contacts with the ability to initiate changes to subscribed services.	No relevant exceptions noted.
		Inspected the authorized client contact listing to verify that a client authorized requestor list was maintained for each client that listed the authorized client contacts with the ability to initiate changes to subscribed services.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.2.4	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 relevant exceptions noted.
		Inspected customer access change request communications for a sample of customer badge access change requests 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 relevant exceptions noted.
CC5.2.5	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 relevant 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 relevant exceptions noted.
CC5.3 Internal and external users are identified and authenticated when accessing the system components (that is, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to Security and Availability			
CC5.3.1	Workstations are restricted to authorized employees via unique user names and passwords.	Inquired of the Compliance Engineer to verify that workstations were restricted to authorized employees via unique user names and passwords.	No relevant exceptions noted.
		Inspected the Default Domain Policy to verify that workstations were restricted to authorized employees via unique user names and passwords.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.3.2	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 relevant 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 relevant exceptions noted.
CC5.4 Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to Security and Availability			
CC5.4.1	Workstations are restricted to authorized employees via unique user names and passwords.	Inquired of the Compliance Engineer to verify that workstations were restricted to authorized employees via unique user names and passwords.	No relevant exceptions noted.
		Inspected the Default Domain Policy to verify that workstations were restricted to authorized employees via unique user names and passwords.	No relevant exceptions noted.
CC5.4.2	A client authorized requestor list is maintained for each client that lists the authorized client contacts with the ability to initiate changes to subscribed services.	Inquired of the Compliance Engineer to verify that a client authorized requestor list was maintained for each client that listed the authorized client contacts with the ability to initiate changes to subscribed services.	No relevant exceptions noted.
		Inspected the authorized client contact listing to verify that a client authorized requestor list was maintained for each client that listed the authorized client contacts with the ability to initiate changes to subscribed services.	No relevant exceptions noted.
CC5.4.3	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 relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected customer access change request communications for a sample of customer badge access change requests 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 relevant exceptions noted.
CC5.4.4	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 relevant 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 relevant exceptions noted.
CC5.5 Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to Security and Availability			
CC5.5.1	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 relevant exceptions noted.
		Inspected the security policy 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 relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.5.2	Predefined physical security zones are utilized to assign role-based access to and throughout the data centers.	Inquired of the onsite personnel for the 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 relevant 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 relevant exceptions noted.
		Observed the use and configurations of predefined security zones within the data centers during onsite activities for the 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 relevant exceptions noted.
CC5.5.3	Doors controlling access to facilities and restricted areas remain secured at all times.	Inquired of the onsite personnel for the sample of sites visited to verify that the doors to the facilities and data centers remained locked at all times.	No relevant exceptions noted.
		Observed access to the data centers during onsite activities for the sample of sites visited to verify that the doors to the facilities and data centers remained locked at all times.	No relevant exceptions noted.
CC5.5.4	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 the 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 relevant 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 relevant 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 the sample of sites visited to verify that access to and throughout the facilities was controlled using badge access systems.	No relevant exceptions noted.
CC5.5.5	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 relevant 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 relevant exceptions noted.
CC5.5.6	Background screenings are performed for employment candidates as a component of the hiring process.	Inquired of the onsite personnel to verify that background screenings were performed for employment candidates as a component of the hiring process.	No relevant 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 relevant exceptions noted.
CC5.5.7	Visitors, vendors, and contractors are required to: <ul style="list-style-type: none"> ➤ 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 to verify that visitors, vendors, and contractors were required to: <ul style="list-style-type: none"> ➤ 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 relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		<p>Observed visitors enter the data centers during onsite activities to verify that visitors, vendors, and contractors were required to:</p> <ul style="list-style-type: none"> ➤ 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 relevant exceptions noted.
		<p>Inspected visitor sign-in log to verify that visitors, vendors, and contractors were required to:</p> <ul style="list-style-type: none"> ➤ 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 relevant exceptions noted.
CC5.5.8	Visitors are required to be escorted by an authorized employee when accessing the facilities.	Inquired of the onsite personnel for the sample of sites visited to verify that visitors were required to be escorted by an authorized employee when accessing the facilities.	No relevant exceptions noted.
		Observed visitors during onsite activities for the sample of sites visited to verify that visitors were required to be escorted by an authorized employee when accessing the facilities.	No relevant exceptions noted.
CC5.5.9	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 relevant 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 change requests 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 relevant exceptions noted.
CC5.5.10	The data centers data halls do not contain any exterior windows.	Inquired of the onsite personnel for the sample of sites visited to verify that the data centers did not contain any exterior windows.	No relevant exceptions noted.
		Observed the data center halls during onsite activities for the sample of sites visited to verify that the data centers did not contain any exterior windows.	No relevant exceptions noted.
CC5.5.11	Visitors leaving the facilities are required to surrender their badge upon departure.	Inquired of the onsite personnel for the sample of sites visited to verify that visitors leaving the facilities were required to surrender their badge upon departure.	No relevant exceptions noted.
		Observed visitors during onsite activities for the sample of sites visited to verify that visitors leaving the facilities were required to surrender their badge upon departure.	No relevant exceptions noted.
CC5.5.12	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 relevant exceptions noted.
		Observed the locked customer equipment cages and server racks during onsite activities for the sample of sites visited to verify that customer equipment was housed in locked, segregated environments within the data centers.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.5.13	The data centers' walls are continuous from floor to ceiling.	Inquired of the onsite personnel for the sample of sites visited to verify that the data centers' walls were continuous from floor to ceiling.	No relevant exceptions noted.
		Observed the data center walls during onsite activities for the sample of sites visited to verify that the data centers' walls were continuous from floor to ceiling.	No relevant exceptions noted.
CC5.6 Logical access security measures have been implemented to protect against Security and Availability threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.			
CC5.6.1	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 relevant 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 relevant exceptions noted.
CC5.6.2	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 within the past 12 months.	No relevant 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 relevant exceptions noted.
CC5.6.3	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 Network Administrator 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 relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the VPN configurations and the VPN Client 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 relevant exceptions noted.
CC5.6.4	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 relevant exceptions noted.
		Inspected the firewall change tickets for a sample of client firewall changes requested 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 relevant exceptions noted.
CC5.6.5	VPN sessions require unique user names and password authentication.	Inquired of the Compliance Engineer to verify that VPN sessions required unique user names and password authentication.	No relevant exceptions noted.
		Inspected the VPN client to verify that VPN sessions required unique user names and password authentication.	No relevant exceptions noted.
CC5.6.6	<p>Logical access to technical workstations is restricted by the following password requirements:</p> <ul style="list-style-type: none"> ➤ Minimum of 12 characters in length ➤ Expire after 60 days ➤ Mix of alpha numeric, upper, and lower-case characters 	<p>Inquired of the Compliance Engineer to verify that logical access to technical workstations was restricted by the following password requirements:</p> <ul style="list-style-type: none"> ➤ Minimum of 12 characters in length ➤ Expire after 60 days ➤ Mix of alpha numeric, upper, and lower-case characters 	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		<p>Inspected the Default Domain Policy to verify that logical access to technical workstations was restricted by the following password requirements:</p> <ul style="list-style-type: none"> ➤ Minimum of 12 characters in length ➤ Expire after 60 days ➤ Mix of alpha numeric, upper, and lower-case characters 	No relevant exceptions noted.
CC5.6.7	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 relevant 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 relevant exceptions noted.
CC5.7 The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to Security and Availability			
CC5.7.1	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 relevant 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 relevant exceptions noted.
CC5.7.2	VPN sessions require unique user names and password authentication.	Inquired of the Compliance Engineer to verify that VPN sessions required unique user names and password authentication.	No relevant 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 user names and password authentication.	No relevant exceptions noted.
CC5.7.3	Network policies are configured to lock workstations after 15 minutes of inactivity.	Inquired of the Compliance Engineer to verify that network policies were configured to lock workstations after 15 minutes of inactivity.	No relevant exceptions noted.
		Inspected the Default Domain Policy to verify that network policies were configured to lock workstations after 15 minutes of inactivity.	No relevant exceptions noted.
CC5.7.4	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 relevant 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 relevant exceptions noted.
CC5.8 controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to Security and Availability			
CC5.8.1	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 relevant 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 relevant exceptions noted.
CC5.8.2	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 relevant 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 relevant exceptions noted.
CC6.0 System Operations: The criteria relevant to how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objective(s) of the principle(s) addressed in the engagement.			
CC6.1 Vulnerabilities of system components to Security and Availability breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to Security and Availability			
CC6.1.1	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 relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the incident 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 relevant exceptions noted.
CC6.1.2	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 Mark Houpt, Chief Information Security Officer, 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 relevant 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 relevant exceptions noted.
		Observed the technical support staff during on-site activities to verify that they monitored the physical environment on a 24 x 365 basis, including power, temperature, humidity, video surveillance, and access control.	No relevant exceptions noted.
CC6.1.3	Management reviews the Disaster Recovery (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 within the past 12 months to ensure that it meets DataBank's availability business requirements.	No relevant exceptions noted.
		Inspected the Disaster Recovery Plan to verify that management reviewed the DR Plan within the past 12 months to ensure that it meets DataBank's availability business requirements.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC6.1.4	Management ensures that training on the DR Plan is completed on an annual basis.	Inquired of the Compliance Engineer to verify that management ensured that training on the DR Plan was completed within the past 12 months.	No relevant exceptions noted.
		Inspected the Business Continuity Plan Exercise to verify that management ensured that training on the DR Plan was completed within the past 12 months.	No relevant exceptions noted.
CC6.1.5	<p>Applications are utilized to monitor the following performance, availability, and controlled events for managed services infrastructure:</p> <ul style="list-style-type: none"> ➤ Availability of the network ➤ Host services and ports ➤ CPU and hard disk utilization 	<p>Inquired of the onsite personnel to verify that applications were utilized to monitor the following performance, availability, and controlled events for managed services infrastructure:</p> <ul style="list-style-type: none"> ➤ Availability of the network ➤ Host services and ports ➤ CPU and hard disk utilization 	No relevant exceptions noted.
		<p>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:</p> <ul style="list-style-type: none"> ➤ Availability of the network ➤ Host services and ports ➤ CPU and hard disk utilization 	No relevant exceptions noted.
CC6.1.6	<p>Environmental monitoring systems are utilized to monitor the environmental conditions and devices within the data centers including, but not limited to, the following:</p> <ul style="list-style-type: none"> ➤ Water leakage ➤ Air handling units ➤ UPS systems ➤ Generators 	<p>Inquired of the onsite personnel 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:</p> <ul style="list-style-type: none"> ➤ Water leakage ➤ Air handling units ➤ UPS systems ➤ Generators 	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		<p>Inspected the environmental monitoring Data Center Infrastructure Management systems at each location 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:</p> <ul style="list-style-type: none"> ➤ Water leakage ➤ Air handling units ➤ UPS systems ➤ Generators 	No relevant exceptions noted.
		<p>Observed the environmental monitoring systems during onsite activities 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:</p> <ul style="list-style-type: none"> ➤ Water leakage ➤ Air handling units ➤ UPS systems ➤ Generators 	No relevant exceptions noted.
CC6.1.7	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 relevant 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 relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC6.1.8	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 relevant exceptions noted.
		Inspected the incident tickets to verify that an incident ticketing system was utilized to document, prioritize, escalate, and help resolve problems that affected services provided.	No relevant exceptions noted.
CC6.2 Security and Availability incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.			
CC6.2.1	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 relevant exceptions noted.
		Inspected the incident 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 relevant exceptions noted.
CC6.2.2	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 relevant exceptions noted.
		Inspected the incident tickets to verify that an incident ticketing system was utilized to document, prioritize, escalate, and help resolve problems that affected services provided.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC7.0 Change Management: The criteria relevant to how the entity identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.			
CC7.1 The entity's commitments and system requirements, as they relate to Security and Availability, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.			
CC7.1.1	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 relevant exceptions noted.
		Inspected the DataBank policies and procedures to verify that DataBank maintained policy and procedure manuals for user organization-requested changes to existing systems.	No relevant exceptions noted.
CC7.1.2	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 relevant 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 relevant exceptions noted.
CC7.1.3	Upon closing a ticket, the ticket system automatically emails the primary client 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 ticket system automatically emailed the primary client contact person notifying them of the issue and actions taken by DataBank.	No relevant exceptions noted.
		Inspected the ticket configurations to verify that upon closing a ticket, the ticket system automatically emailed the primary client contact person notifying them of the issue and actions taken by DataBank.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC7.1.4	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 relevant exceptions noted.
		Inspected customer access change request communications for a sample of customer badge access change requests 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 relevant exceptions noted.
CC7.2 Infrastructure, data, software, and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to Security and Availability			
CC7.2.1	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 relevant exceptions noted.
		Inspected the DataBank policies and procedures to verify that DataBank maintained policy and procedure manuals for user organization-requested changes to existing systems.	No relevant exceptions noted.
CC7.2.2	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 relevant 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 relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC7.3 Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to Security and Availability			
CC7.3.1	A ticketing system is used to document and track to resolution, client requests.	Inquired of the Compliance Engineer to verify that a ticketing system was used to document and track to resolution, client requests.	No relevant exceptions noted.
		Inspected the client change tickets to verify that a ticketing system was used to document and track to resolution, client requests.	No relevant exceptions noted.
CC7.3.2	Upon closing a ticket, the ticket system automatically emails the primary client 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 ticket system automatically emailed the primary client contact person notifying them of the issue and actions taken by DataBank.	No relevant exceptions noted.
		Inspected the ticket configurations to verify that upon closing a ticket, the ticket system automatically emailed the primary client contact person notifying them of the issue and actions taken by DataBank.	No relevant exceptions noted.
CC7.4 Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's Security and Availability commitments and system requirements.			
CC7.4.1	A ticketing system is used to document and track to resolution, client requests.	Inquired of the Compliance Engineer to verify that a ticketing system was used to document and track to resolution, client requests.	No relevant exceptions noted.
		Inspected the client change tickets to verify that a ticketing system was used to document and track to resolution, client requests.	No relevant exceptions noted.
CC7.4.2	Upon closing a ticket, the ticket system automatically emails the primary client 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 ticket system automatically emailed the primary client contact person notifying them of the issue and actions taken by DataBank.	No relevant 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 ticket system automatically emailed the primary client contact person notifying them of the issue and actions taken by DataBank.	No relevant exceptions noted.
CC7.4.3	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 relevant exceptions noted.
		Inspected the firewall change tickets for a sample of client firewall changes requested 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 relevant exceptions noted.
CC7.4.4	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 relevant 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 relevant exceptions noted.
CC7.4.5	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 relevant exceptions noted.
		Inspected notifications sent to customers for 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 relevant exceptions noted.

Availability Principle and Criteria

The system is available for operation and use to meet the entity's commitments and system requirements.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
A1.1 Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.			
A1.1.1	<p>Applications are utilized to monitor the following performance, availability, and controlled events for managed services infrastructure:</p> <ul style="list-style-type: none"> ➤ Availability of the network ➤ Host services and ports ➤ CPU and hard disk utilization 	<p>Inquired of the onsite personnel to verify that applications were utilized to monitor the following performance, availability, and controlled events for managed services infrastructure:</p> <ul style="list-style-type: none"> ➤ Availability of the network ➤ Host services and ports ➤ CPU and hard disk utilization 	No relevant exceptions noted.
		<p>Observed the monitoring systems during onsite activities to verify that applications were utilized to monitor the following performance, availability, and controlled events for managed services infrastructure:</p> <ul style="list-style-type: none"> ➤ Availability of the network ➤ Host services and ports ➤ CPU and hard disk utilization 	No relevant exceptions noted.
A1.1.2	<p>Technical support staff are available 24 X 365 to manage data center monitoring systems which include power, temperature, humidity, video surveillance, and access control.</p>	<p>Inquired of Mark Houpt, Chief Information Security Officer, 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.</p>	No relevant exceptions noted.
		<p>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.</p>	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Observed the technical support staff during on-site activities to verify that they monitored the physical environment on a 24 x 365 basis, including power, temperature, humidity, video surveillance, and access control.	No relevant exceptions noted.
A1.1.3	<p>Environmental monitoring systems are utilized to monitor the environmental conditions and devices within the data centers including, but not limited to, the following:</p> <ul style="list-style-type: none"> ➤ Water leakage ➤ Air handling units ➤ UPS systems ➤ Generators 	<p>Inquired of the onsite personnel 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:</p> <ul style="list-style-type: none"> ➤ Water leakage ➤ Air handling units ➤ UPS systems ➤ Generators 	No relevant exceptions noted.
		<p>Inspected the environmental monitoring Data Center Infrastructure Management systems at each location 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:</p> <ul style="list-style-type: none"> ➤ Water leakage ➤ Air handling units ➤ UPS systems ➤ Generators 	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		<p>Observed the environmental monitoring systems during onsite activities 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:</p> <ul style="list-style-type: none"> ➤ Water leakage ➤ Air handling units ➤ UPS systems ➤ Generators 	No relevant exceptions noted.
A1.1.4	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 relevant exceptions noted.
		Inspected the information security policy and incident response plan to verify that documented environmental security policies and procedures were in place to govern environmental security practices.	No relevant exceptions noted.
A1.2 Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.			
A1.2.1	<p>Data center areas are equipped with fire detection and suppression systems including:</p> <ul style="list-style-type: none"> ➤ Smoke detectors ➤ Audible and visual fire alarms ➤ Automated extinguisher system ➤ Hand-held fire extinguishers 	<p>Inquired of the onsite personnel for the sample of sites visited to verify that data center areas were equipped with fire detection and suppression systems including:</p> <ul style="list-style-type: none"> ➤ Smoke detectors ➤ Audible and visual fire alarms ➤ Automated extinguisher system ➤ Hand-held fire extinguishers 	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		<p>Observed the fire detection and suppression equipment during onsite activities for the sample of sites visited to verify that data center areas were equipped with fire detection and suppression systems including:</p> <ul style="list-style-type: none"> ➤ Smoke detectors ➤ Audible and visual fire alarms ➤ Automated extinguisher system ➤ Hand-held fire extinguishers 	No relevant exceptions noted.
A1.2.2	Data center areas are equipped with multiple dedicated air handling units.	Inquired of the onsite personnel to verify that data center areas were equipped with multiple dedicated air handling units.	No relevant exceptions noted.
		Observed the air handling units during on-site activities to verify that data center areas were equipped with multiple dedicated air handling units.	No relevant exceptions noted.
A1.2.3	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 within the past 12 months, management contracted third-party vendors to complete inspections on the air handling units.	No relevant 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 relevant exceptions noted.
A1.2.4	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 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 relevant 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 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 relevant exceptions noted.
A1.2.5	Data center areas are available with raised flooring and/or server racks to elevate equipment and help facilitate cooling.	Inquired of the onsite personnel to verify that data center areas were available with raised flooring and/or server racks to elevate equipment and help facilitate cooling.	No relevant exceptions noted.
		Observed the flooring and server racks during onsite activities to verify that data center areas were available with raised flooring and/or server racks to elevate equipment and help facilitate cooling.	No relevant exceptions noted.
A1.2.6	Data center power systems are constructed with redundant UPS units.	Inquired of onsite personnel to verify that data center power systems were constructed with redundant UPS units.	No relevant exceptions noted.
		Observed the UPS units at during onsite activities that data center power systems were constructed with redundant UPS units.	No relevant exceptions noted.
A1.2.7	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 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 relevant exceptions noted.
		Observed the UPS units during onsite activities 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 relevant exceptions noted.
A1.2.8	The data centers have redundant electrical utility feeds.	Inquired of the onsite personnel to verify that the data centers had redundant electrical utility feeds.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Observed the data centers during onsite activities to verify that they had redundant electrical utility feeds.	No relevant exceptions noted.
A1.2.9	Power infrastructure is designed and constructed redundantly to mitigate risk to customer systems and services.	Inquired of the Facilities Manager to verify that power infrastructure was designed and constructed redundantly to mitigate risk to customer systems and services.	No relevant exceptions noted.
		Observed the utility feeds and power distribution units during onsite activities to verify that power infrastructure was designed and constructed redundantly to mitigate risk to customer systems and services.	No relevant exceptions noted.
A1.2.10	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 management contracted third-party vendors to perform scheduled service and load bank testing of the generators within the past 12 months.	No relevant 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 relevant exceptions noted.
A1.2.11	On an annual basis, management contracts third-party vendors to complete inspections of the UPS systems.	Inquired of the Compliance Engineer to verify that management had contracted third-party vendors to complete inspections of the UPS systems within the past 12 months.	No relevant 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 relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
A1.2.12	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 relevant exceptions noted.
		Inspected the Information System Contingency Plan to verify that DataBank maintained policy and procedure manuals for backup, storage, and restoration procedures.	No relevant exceptions noted.
A1.2.13	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 relevant exceptions noted.
		Inspected the backup configurations to verify that DataBank standard backup configurations were set to automatically perform daily backups of customer systems.	No relevant exceptions noted.
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 relevant exceptions noted.
		Inspected the incident tickets to verify that an incident ticketing system was utilized to document, prioritize, escalate, and help resolve problems that affected services provided.	No relevant exceptions noted.
A1.2.15	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 management contracted third-party vendors to complete fire detection and suppression equipment inspections within the past 12 months.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		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 relevant exceptions noted.
A1.2.16	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 management contracted third-party vendors to perform scheduled service and load bank testing of the generators within the past 12 months.	No relevant 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 relevant 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 within the past 12 months to ensure that it meets DataBank's availability business requirements.	No relevant exceptions noted.
		Inspected the Disaster Recovery Plan to verify that management reviewed the DR Plan within the past 12 months to ensure that it meets DataBank's availability business requirements.	No relevant exceptions noted.
A1.3 Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.			
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 within the past 12 months to ensure that it meets DataBank's availability business requirements.	No relevant exceptions noted.
		Inspected the Disaster Recovery Plan to verify that management reviewed the DR Plan within the past 12 months to ensure that it meets DataBank's availability business requirements.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
A1.3.2	Management ensures that training on the DR Plan is completed on an annual basis.	Inquired of the Compliance Engineer to verify that management ensured that training on the DR Plan was completed within the past 12 months.	No relevant exceptions noted.
		Inspected the Business Continuity Plan Exercise to verify that management ensured that training on the DR Plan was completed within the past 12 months.	No relevant exceptions noted.