

# Hiestand, Brand, Loughran, P.A.

SOC 1 (SSAE No. 16) TYPE 2 REPORT ON CONTROLS  
PLACED IN OPERATION FOR DATA CENTER SERVICES

**DataBank Holdings, Ltd.**

*JUNE 1, 2014 TO MAY 31, 2015*



D A T A B A N K



# DATABANK HOLDINGS, LTD.

## Table of Contents

<b>SECTION 1: INDEPENDENT SERVICE AUDITORS' REPORT .....</b>	<b>1</b>
<b>SECTION 2: MANAGEMENT'S ASSERTION .....</b>	<b>4</b>
<b>SECTION 3: DATABANK'S DESCRIPTION OF CONTROLS .....</b>	<b>6</b>
SCOPE OF REPORT AND DISCLOSURES .....	8
Sub-Service Organizations .....	8
Significant Changes during the Review Period .....	8
Subsequent Events .....	8
Using the Work of the Internal Audit Function .....	8
OVERVIEW OF OPERATIONS AND THE SYSTEM .....	9
Company Overview and Background .....	9
Overview of the Data Center Services System .....	9
OVERVIEW OF RELEVANT INFRASTRUCTURE .....	10
Infrastructure .....	10
Software .....	10
People .....	10
Procedures .....	12
Data .....	12
RELEVANT ASPECTS OF CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATIONS SYSTEMS, MONITORING, POLICIES AND PRACTICES .....	13
Control Environment .....	13
Risk Assessment .....	15
Information and Communication Systems .....	16
Monitoring .....	17
Policies and Practices .....	18
CONTROL OBJECTIVES AND RELATED controls .....	21
USER ENTITY CONTROL CONSIDERATIONS .....	22
<b>SECTION 4: CONTROL DESCRIPTIONS, RELATED CONTROLS AND TESTS OF OPERATING EFFECTIVENESS .....</b>	<b>23</b>
INFORMATION PROVIDED BY THE SERVICE AUDITOR .....	24
Introduction .....	24
Tests of Operating Effectiveness .....	24
Types of Tests Performed .....	25
Sampling Methodology .....	26
TESTING MATRICES .....	27
Physical Security .....	27
Environmental Security .....	37
Customer Provisioning .....	45
Network Monitoring .....	49

---

**SECTION 1:**

**INDEPENDENT SERVICE AUDITORS' REPORT**

# Hiestand, Brand, Loughran, P.A.

## **INDEPENDENT SERVICE AUDITORS' REPORT ON THE DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS**

To DataBank Holdings, Ltd.:

We have examined DataBank Holdings, Ltd.'s ("DataBank") description of its Data Center Services system for the Dallas, Texas, Richardson, Texas, and Edina, Minnesota facilities throughout the period June 1, 2014 to May 31, 2015 and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of DataBank's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Within Section 2 of this report, DataBank has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. DataBank is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period June 1, 2014 to May 31, 2015.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described within DataBank's assertion within Section 2 of this report. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. 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 achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the criteria described in DataBank's assertion in the next section of this report:

- a. the description fairly presents DataBank's Data Center Services system that was designed and implemented throughout the period June 1, 2014 to May 31, 2015;
- b. the controls related to the control objectives of DataBank stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period June 1, 2014 to May 31, 2015, and user entities applied the complementary user entity controls contemplated in the design of DataBank's controls throughout the period June 1, 2014 to May 31, 2015; and
- c. the controls that we tested, which together with the complementary user entity controls referred to in Section 3 of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period June 1, 2014 to May 31, 2015.

The specific controls tested and the nature, timing, and results of those tests are listed within Section 4 of the report.

This report, including the description of tests of controls and results thereof within Section 4, is intended solely for the information and use of DataBank, user entities of DataBank's Data Center Services system during some or all of the period June 1, 2014 to May 31, 2015, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

*Hiestand, Brand, Arghman PA.*

July 30, 2015  
Tampa, Florida

---

**SECTION 2:**

**MANAGEMENT'S ASSERTION**

## MANAGEMENT'S ASSERTION

July 30, 2015

We have prepared the description of DataBank Holdings, Ltd.'s ("DataBank") Data Center Services system for user entities of the system during some or all of the period June 1, 2014 to May 31, 2015 and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that

- a. the description fairly presents the Data Center Services system made available to user entities of the system during some or all of the period June 1, 2014 to May 31, 2015 to support the processing of relevant transactions. The criteria we used in making this assertion were that the description:
  - i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions as they relate to our environment, including when applicable:
    1. the types of services provided;
    2. the procedures, within both automated and manual systems, by which services are provided;
    3. how the system captures and addresses significant events and conditions, other than transactions;
    4. the process used to prepare reports or other information provided to user entities of the system;
    5. the specified control objectives and controls designed to achieve those objectives; and
    6. other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to user entities of the system.
  - ii. does not omit or distort information relevant to the scope of the Data Center Services system, while acknowledging that the description is presented to meet the common needs of a broad range of user entities of the system and their financial statement auditors, and may not, therefore, include every aspect of the Data Center Services system that each individual user entity of the system and its auditor may consider important in its own particular environment.
  - iii. includes relevant details of changes to the service organization's system during the audit period covered by the description.
- b. the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period June 1, 2014 to May 31, 2015 to achieve those control objectives. The criteria we used in making this assertion were that:
  - i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management;
  - ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and
  - iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

/s/ DataBank Holdings, Ltd.

Timothy Moore – CEO

H. Michael Gentry – VP of Operations

---

**SECTION 3:**

**DATABANK'S DESCRIPTION OF CONTROLS**

## SCOPE OF REPORT AND DISCLOSURES

This description of the system of controls provided by DataBank Holdings, Ltd. (“DataBank”) management, as related to Statement on Standards for Attestation Engagements No. 16 ‘Reporting on controls at a Service Organization’ (“SSAE 16” or “SOC 1”), considers the direct and indirect impact of risks and controls that DataBank management has determined are likely to be relevant to its user entities’ internal controls over financial reporting. The scope of management’s description of the system of controls covers the general computer and customer provisioning controls supporting the Data Center Services system, and considers the initiation, authorization, recording, processing and reporting of related transactions. DataBank is responsible for identification of risks associated with the system of controls (defined as control objectives), and for the design and operation of controls intended to mitigate those risks. This includes the applicable information technology infrastructure and the supporting processes related to the Data Center Services system. It does not include any other processes used to initiate, authorize, record, process, or report on the financial transactions of its user entities. Additionally, DataBank does not maintain accountability for any user entity assets, liabilities, or equity.

As part of its overall SOC 1 program, DataBank’s management sets and determines the scope and timing of each report. This report features the Data Center Services system. This description of the system of controls has been prepared by DataBank management to provide information on controls applicable to the Data Center Services system at the headquarters located in Dallas, Texas, as well as the Richardson, Texas, and Edina, Minnesota locations (“data centers” or “facilities”).

### **Sub-Service Organizations**

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

### **Significant Changes during the Review Period**

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

### **Subsequent Events**

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

### **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 managed data center space for colocation services headquartered in the Dallas, Texas. 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 colocation offerings include customized technology solutions designed specifically to help organizations manage their risk and improve their overall business performance.

## Overview of the Data Center Services System

DataBank provides data center facilities and infrastructure to protect customers' systems from physical and environmental security threats. DataBank provides customizable space and power solutions to accommodate unique customer requirements within its data halls located throughout the data centers. The data centers, and data halls within, are protected from unauthorized access through the use of card and biometric security access controls restricted to authorized personnel, as well as video surveillance systems. The data centers and data halls within are further secured from environmental threats such as fire, harmful temperature and humidity levels, and power surges or power failures.

### Functional Areas of Operations

The following groups are responsible for providing services related to the Data Center Services system:

- Executive management – responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives;
- Data center personnel – manages, monitors and supports the data center from unauthorized access and use while maintaining integrity and availability;
- Support operations – monitors the network infrastructure and responds to incidents identified; and
- Accounting and administration – perform reconciliations related to services provided to user entities and provides financial and regulatory reporting and operational quality assurance and compliance.

# OVERVIEW OF RELEVANT INFRASTRUCTURE

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

- Infrastructure (facilities, equipment, and networks);
- Software (systems, applications, and utilities);
- People (developers, operators, users, and managers);
- Procedures (automated and manual); and
- Data (transaction streams, files, databases, and tables).

## Infrastructure

The DataBank data centers offer facilities and infrastructure to provide colocation services for its customers. Each facility is designed with multiple data halls within 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 facilities.

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

System / Application	Description	Infrastructure
Nagios	Network monitoring	GNU / Linux (Nagios Core)
WebCTRL 5.5	Environmental monitoring (Dallas and Richardson)	Automated Logic
TrendPoint	Environmental monitoring (Edina only)	Automated Logic
On Guard	Card access system (Dallas and Richardson)	Lenel / Suprema
System Galaxy	Card access system (Edina only)	Windows 7 / SQL Server 2008

## Software

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

## People

The roles and responsibilities of key functions include the following:

- **Chief Executive Officer (CEO):** Timothy Moore serves as the CEO of DataBank. He provides overall direction for the daily operations as well as the strategic vision of the company. Moore joined DataBank following Avista Capital Partners' acquisition of the company in 2011. He has over 30 years of experience leading large and small companies through significant growth cycles in technology marketplaces. Moore has 12 years of senior management experience in the outsourced data center industry. He has served at the Vice President level for three Fortune 500 companies where he established a successful background in sales, marketing, and business development. He began his career in the computer industry in the 1980's. Moore earned a B.S. in Business Administration from the Fisher Business School at The Ohio State University.

- **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, 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. Ooley holds a Bachelor of Industrial Engineering from the Georgia Institute of Technology.
- **Chief Technology Officer (CTO):** Bryan Porter joined DataBank through the April 2014 acquisition of Arsalon Technologies, where he served as President since he co-founded the company 2001. In his role as DataBank's Chief Technology Officer, Porter is responsible for the direction of the company's overall technology strategies, service philosophy, implementation and management. Porter's experience previous to Arsalon includes management positions at BHA, St. Luke's Shawnee Mission Health System and GeoAccess. He earned his undergraduate degree in Computer Science from Mid-America Nazarene University.
- **Co-Founder & Vice President of Sales:** As Co-Founder, Jerry Blair was instrumental in DataBank's inception in 2005. In his role as Vice President of Sales, Blair is charged with executing the company's sales strategy. With a successful track record spanning more than 20 years in senior sales management, Blair's experience and proven ability to implement results-driven direct and channel-focused sales programs is an asset to the company. Prior to DataBank, 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 Operations:** Michael Gentry joined DataBank management in early 2013, bringing with him a long history of industry success. He provides DataBank with oversight and management on the company's business operations including provisioning, quality assurance, customer service, and new product development. Prior to DataBank, Gentry served as Vice President of Managed Service Operations for SunGard Availability Services where he managed product engineering and the technical support of computer, storage, database and application management services. Before that, he managed VeriCenter's client experience as the Vice President of Customer Service.
- **Vice President of Technical Operations:** Dan Allen joined the DataBank management team in 2011. As the head of technical operations, Allen is responsible for all of DataBank's facility infrastructure and data center operations. With over 28 years of Telecom and management experience, Allen's oversight ensures DataBank customers have the highest levels of security and redundancy in the industry. Prior to DataBank, Allen managed multiple facilities totaling more than 100K square feet of raised floor for Denver-based ViaWest. Before that, he served as the Director of Technical Services for Dallas-based colocation provider Dataside, and spent 16 years with Cable & Wireless managing the company's central US operations. Allen also served in the United States Air Force.
- **Vice President of Marketing:** Aaron Alwell joined the DataBank management team as a consultant in the closing months of 2011. His immediate focus was on enhancing the company's brand image and awareness. Now in his permanent role, Alwell's impact can be felt throughout every facet of DataBank's branding, presence, and messaging. Prior to DataBank, Alwell was the Vice President of Marketing for USAFact, one of the leading corporate background screening agencies. He has also held management-level marketing positions with a number of technology companies, including ViaWest, Dataside, and Internet America.

## Procedures

DataBank has developed, and communicated to its users, procedures to restrict physical access to DataBank's facilities 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;
- Data Center Physical Security;
- Data Center Environmental Security Policy; and
- Incident and Response Policy.

## Data

DataBank does not process customer's data. The scope of management's description of the system of controls covers the physical and environmental security supporting the Data Center Services system. This includes the applicable information technology infrastructure and the supporting processes related to the Data Center Services system. It does not include any other processes used to initiate, authorize, record, process, or report on the financial transactions of its user entities.

# 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 important 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 all 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.

## **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 President is an active participant in day-to-day operations and all 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. Standards for hiring the most qualified individuals with emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior demonstrate DataBank's commitment to competent and trustworthy people. Training policies that communicate prospective roles and responsibilities and include practices such as training schools and seminars illustrate expected levels of performance and behavior. Promotions driven by periodic performance appraisals demonstrate DataBank's commitment to the advancement of qualified personnel to higher levels of responsibility.

## Risk Assessment

DataBank's risk assessment process is designed to identify and consider the implications of external and internal risk factors concurrent with establishing unit-wide objectives and plans. The likelihood of occurrence and potential monetary impact (or publicity risk) has been evaluated to enhance the reliability of management transaction processes. Risks are categorized as tolerable or requiring action, and include the following considerations:

- **Changes in the operating environment** – a change in regulations may necessitate a revision of existing processing. Revisions of existing processing may create the need for additional or revised controls.
- **New personnel** – new personnel who are responsible for overseeing the IT controls may increase the risk that controls will not operate effectively.
- **Rapid growth** – a rapid increase in the number of new customers may affect the operating effectiveness of certain controls.
- **New business models, products, or activities** – the diversion of resources to new activities from existing activities could affect certain controls.
- **Corporate restructuring** – a change in ownership or internal reorganization could affect reporting responsibilities or the resources available for services to user entities.
- **Government and regulatory changes** – the implementation of relevant government and regulatory pronouncements could affect user entities

DataBank's recognition of risks that could affect the organization's ability to provide reliable data center services for its user entities is generally implicit, rather than explicit. Management's involvement in the daily operations allows them to learn about risks related to services provided through direct personal involvement with employees and outside parties. In addition to this, Management undergoes a formal annual risk assessment process to document the risks as well as the mitigating factors for each risk. Residual risk that is determined to be too high, is discussed and an action plan is put in place to ensure the overall risk exposure is reduced to an acceptable level as determined by DataBank Executive Management.

## **Information and Communication Systems**

### **Information System**

DataBank has and maintains 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).

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

## INFRASTRUCTURE MANAGEMENT

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

### Physical Security

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 hand 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 is maintained in separate, secured and locked steel cages and cabinets.

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 employees with badge access have 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 video monitoring 24 hours per day. Video surveillance cameras at each location are supported by systems which retain at minimum 90 days of video activity.

### Environmental Security

#### *Redundancy*

DataBank has many attributes capable of providing complete redundancy in power, cooling, and network infrastructure.

Primary components of the Dallas, Texas data center include:

- Two vaults with Twelve outgoing independent utility feeds;
- 10 generators;
- Seven 500 ton cooling towers;
- Dual closed loop water system;
- 80,000 gallon make-up water tank;
- Dual zero manholes for diverse service provider entry; and
- Utility service built in a 2(N+2) configuration.

Primary components of the Richardson, Texas data center include:

- Dual 10MW feeds in a true 2N configuration;
- Four 2.75MW generators;
- Five 500 ton cooling towers and dual-fed high-efficiency CRAH units;
- 100,000 gallon reserve water tank for cooling on-site; and

- On-site carrier-class redundant Meet-Me-Rooms.

Primary components of the Edina, Minnesota facility's data center include:

- Two 2MW independent utility feed generators;
- Three 240 ton air cooled chillers;
- Dual 2.5MW feeds in a true 2N configuration;
- high-efficiency Computer Room Air Handler (CRAH) units; and
- on-site carrier-class Meet-Me-Room.

#### *Power Capabilities*

The aspects and elements of the power delivery system are configured in a redundant design. Two diverse substation feeds deliver power to the facilities. 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.

The Dallas, Texas facility has a cooling infrastructure comprised of open and closed loop condenser water systems. The system consists of seven 500 ton cooling towers, six 650 ton plate heat exchangers and an 80,000 gallon make-up water tank providing a total of 10.2 MW of cooling.

The Richardson, Texas facility has a cooling infrastructure based on a common header, open loop condenser water, closed loop chilled water system. The system consists of three 500 ton cooling towers, three 500 ton variable speed screw chillers, and four 10,000 gallon make-up water tank providing a total of 3.5 MW of cooling. Cooling is distributed via thirty-seven CRAH units deployed in an N+1 design.

The Edina, Minnesota facility has a cooling infrastructure comprised of open and closed loop condenser water systems. The system consists of three 240 ton air cooled chillers for a total of 480 tons N+1. Cooling is distributed via fourteen CRAH units deployed in an N+1 design.

#### *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 facility to monitor temperature, humidity, and leak detection.

#### Customer Provisioning

DataBank utilizes Master Service Agreements (MSAs) and Service Level Agreements (SLAs) 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 letter and a start of service notification. Each customer provides a list of customer contacts to be notified in the event of a networking incident.

### 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 (primarily Nagios) 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.

## CONTROL OBJECTIVES AND RELATED CONTROLS

The DataBank control objectives and related controls are included in Section 4 of this report, “Control Descriptions, 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 control objectives and related controls are included in Section 4, they are, nevertheless, an integral part of the service organization’s description of controls.

## USER ENTITY CONTROL CONSIDERATIONS

The control activities at DataBank cover only a portion of the overall internal control for each user entity. It is not feasible for the control objectives related to the Data Center Services system to be solely achieved by DataBank. DataBank's controls over the systems and infrastructure supporting the Data Center Services system were designed with the assumption that certain controls would be in place and in operation at user entities. User entity internal controls must be evaluated, taking into consideration DataBank's controls and their own internal controls. DataBank does not represent any responsibility or provide any assurance in regards to the services that it provides in relation to any such internal control or regulatory requirements for which the customer must assess or comply.

This section describes some of the control considerations for user entities, or "complementary user entity controls", which should be in operation at user entities to complement the controls at the service organization. User auditors should determine whether user entities have established controls to ensure that control objectives within this report are met. The "complementary user entity controls" presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities. There may be additional control objectives and related controls that would be appropriate for the processing of user transactions that are not identified in this report.

### 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 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.
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 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 providing and maintaining a list of authorized customer contacts with the ability to initiate changes to subscribed services.

---

**SECTION 4:**

**CONTROL DESCRIPTIONS, RELATED CONTROLS AND TESTS OF  
OPERATING EFFECTIVENESS**

# INFORMATION PROVIDED BY THE SERVICE AUDITOR

## Introduction

This report is intended to provide user entities and user auditors 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. This report, when combined with an understanding of the internal controls in place at user entities, is intended to assist the user auditor in planning the audit of the financial statements of user entities. It may be used in assessing control risk associated with user entity financial statement assertions that could be impacted by the Data Center Services system provided by DataBank.

The scope of our testing of DataBank's controls was limited to the control objectives 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 objectives stated. Our review was not extended to controls in place at any user entities, sub-service organizations or any other third-party vendors.

The examination was performed in accordance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 16 ("SSAE 16"), *"Reporting on controls at a Service Organization"*, as amended. It is each interested party's responsibility to evaluate this information in relation to controls in place at user entities to obtain an overall understanding of internal control and to assess control risk. Controls in place at user entities and DataBank's controls must be evaluated together. A general, but not inclusive, listing of control considerations is provided in Section 3, "User Entity Control Considerations." If an effectively operating user entity 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 control objectives during the period from June 1, 2014 to May 31, 2015. 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 control objectives 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 stated control objectives.

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 or user auditors for the controls specified to achieve the stated objective 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 customers in order to complement the controls of DataBank to attain the stated objectives 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"> <li>➤ Knowledge and additional information regarding the policy or procedure; and</li> <li>➤ Corroborating evidence of the policy or procedure.</li> </ul>
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"> <li>➤ Examination / Inspection of source documentation and authorizations to verify transactions processed;</li> <li>➤ Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures;</li> <li>➤ Examination / Inspection of systems documentation, configurations and settings; and</li> <li>➤ Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.</li> </ul>
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.

## 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.

## TESTING MATRICES

<b>Physical Security</b>			
<b>Control Objective Specified by the Service Organization:</b> Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.			
<b>#</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
1.1	Documented physical security policies and procedures are in place to guide employees' activities for granting, controlling, monitoring, and revoking physical access.	Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN 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 DataBank Data Center 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.
1.2	The data halls do not contain any exterior windows.	Inquired of the Provisioning Manager in Dallas, TX; the Director of Facilities in Richardson, TX; and a Sr. Technician in Edina, MN to verify that the data halls did not contain any exterior windows.	No relevant exceptions noted.
		Observed there were no exterior windows within the data halls at each location to verify that the data halls did not contain any exterior windows.	No relevant exceptions noted.
1.3	The entrances to the facilities containing the data halls are monitored and controlled by third-party security personnel.	Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that the entrances to the facilities containing the data halls were monitored and controlled by third-party security personnel.	No relevant exceptions noted.

## Physical Security

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.4	Visitors, vendors, and contractors are required to: <ul style="list-style-type: none"> <li>➤ Present photo identification;</li> <li>➤ Sign a visitor sign-in log including name, firm represented, onsite personnel authorizing access; and</li> <li>➤ Wear a visitor's tag to gain access into the facilities.</li> </ul>	Observed the monitoring activities at each facility to verify that the entrances to the facilities containing the data halls were monitored and controlled by third-party security personnel.  Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that visitors, vendors, and contractors were required to: <ul style="list-style-type: none"> <li>➤ Present photo identification;</li> <li>➤ Sign a visitor sign-in log including name, firm represented, onsite personnel authorizing access; and</li> <li>➤ Wear a visitor's tag to gain access into the facilities.</li> </ul> Inspected the Visitor sign In Sheets at each location to verify that visitors, vendors, and contractors were required to: <ul style="list-style-type: none"> <li>➤ Present photo identification;</li> <li>➤ Sign a visitor sign-in log including name, firm represented, onsite personnel authorizing access; and</li> <li>➤ Wear a visitor's tag to gain access into the facilities.</li> </ul>	No relevant exceptions noted.  No relevant exceptions noted.  No relevant exceptions noted.
1.5	Visitors are required to be escorted by an authorized employee when accessing the facilities.	Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that visitors were required to be escorted by an authorized employee when accessing the facilities.  Observed visitors at each location to verify that visitors were required to be escorted by an authorized employee when accessing the facilities.	No relevant exceptions noted.  No relevant exceptions noted.

## Physical Security

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.6	A list of authorized customer contacts with the ability to initiate customer modifications to physical access privileges is maintained and reviewed when access requests are received from customers.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that a list of authorized customer contacts with the ability to initiate customer modifications to physical access privileges was maintained and reviewed when access requests were received from customers.</p> <p>Inspected the Authorized Customer Contact listings for a selected sample of new clients to verify that a list of authorized customer contacts with the ability to initiate customer modifications to physical access privileges was maintained and reviewed when access requests were received from customers.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
1.7	Requests for the modification of badge access privileges are made by management, or an authorized client requestor, utilizing a standardized access request form.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that requests for the modification of badge access privileges were made by management, or an authorized client requestor, utilizing a standardized access request form.</p> <p>Inspected Facility Access Request Forms for the selected sample of new clients to verify that requests for the modification of badge access privileges were made by management, or an authorized client requestor, utilizing a standardized access request form.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
1.8	Access to and throughout the facilities is controlled through the use of badge access systems	Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that access to and throughout the facilities was controlled through the use of badge access systems.	No relevant exceptions noted.

## Physical Security

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.9	Access to the data halls is controlled via two-factor authentication systems that require an electronic badge and biometric scan.	<p>Inspected the badge access systems at each location to verify that access to and throughout the facilities was controlled through the use of badge access systems.</p> <p>Observed the access restrictions throughout each facility to verify that access to and throughout the facilities was controlled through the use of badge access systems.</p> <p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that access to the data halls was controlled via two-factor authentication systems that required an electronic badge and biometric scan.</p> <p>Observed the requirement for two factor authentication for each data hall entrance at each facility to verify that access to the data halls was controlled via two-factor authentication systems that required an electronic badge and biometric scan.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
1.10	The doors to the facilities and data halls remain locked at all times.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that the doors to the facilities and data halls remained locked at all times.</p> <p>Observed the doors at each facility to verify that the doors to the facilities and data halls remained locked at all times.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
1.11	The doors to the facilities and data halls are equipped with forced entry sensors and door alarm contact points.	Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that the doors to the facilities and data halls were equipped with forced entry sensors and door alarm contact points.	No relevant exceptions noted.

## Physical Security

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.12	Electronic badges do not contain any markings identifying the data centers or their location.	<p>Observed the forced entry sensors at each location to verify that the doors to the facilities and data halls were equipped with forced entry sensors and door alarm contact points.</p> <p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that electronic badges did not contain any markings identifying the data centers or their location.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
1.13	Predefined physical security zones are utilized to assign role-based access to and throughout the data centers.	<p>Observed a sample of access badges from each location to verify that electronic badges did not contain any markings identifying the data centers or their location.</p> <p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that predefined physical security zones were utilized to assign role-based access to and throughout the data centers.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
1.14	The ability to create, modify, and delete user badge access privileges is restricted to administrative user accounts accessible by security and facilities personnel only.	<p>Inspected the badge access configurations at each location to verify that predefined physical security zones were utilized to assign role-based access to and throughout the data centers.</p> <p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that the ability to create, modify, and delete user badge access privileges was restricted to administrative user accounts accessible by security and facilities personnel only.</p>	<p>No relevant exceptions noted.</p>

## Physical Security

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.15	The badge access system is configured to create and store access logs traceable to specific badge holders.	<p>Inspected the badge access system administrators listing for each facility to verify that the ability to create, modify, and delete user badge access privileges was restricted to administrative user accounts accessible by security and facilities personnel only.</p> <p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that the badge access system was configured to create and store access logs traceable to specific badge holders.</p> <p>Inspected the badge access system logs from each location to verify that the badge access system was configured to create and store access logs traceable to specific badge holders.</p> <p>Observed the badge access system log events while on site at each location to verify that the badge access system was configured to create and store access logs traceable to specific badge holders.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
1.16	Management notifies security personnel of employee terminations. Security personnel are required to revoke badge access privileges assigned to the terminated employee.	Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that management notified security personnel of employee terminations. Security personnel were required to revoke badge access privileges assigned to the terminated employee.	No relevant exceptions noted.

## Physical Security

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.17	Management notifies security personnel of customer employee requests for access removal. Security personnel are required to revoke badge access privileges assigned to the customers.	<p>Inspected the access removal notifications for the selected sample of terminated employees during the audit period to verify that management notified security personnel of employee terminations. Security personnel were required to revoke badge access privileges assigned to the terminated employee.</p> <p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that management notified security personnel of customer employee requests for access removal. Security personnel were required to revoke badge access privileges assigned to the customers.</p> <p>Inspected the access removal notifications for the selected sample of access removal requests during the audit period to verify that management notified security personnel of customer employee requests for access removal. Security personnel were required to revoke badge access privileges assigned to the customers.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>



## Physical Security

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.20	Customer equipment is maintained in separated environments within the data centers and is secured via locked steel cages and / or cabinets depending on contract.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that customer equipment was maintained in separated environments within the data centers and was secured via locked steel cages and / or cabinets depending on contract.</p> <p>Observed the data halls at each location to verify that customer equipment was maintained in separated environments within the data centers and was secured via locked steel cages and / or cabinets depending on contract.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
1.21	Customer areas are not identified in any way to help ensure that the client's equipment is not easily distinguishable.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that customer areas were not identified in any way to help ensure that the client's equipment was not easily distinguishable.</p> <p>Observed the data halls at each location to verify that customer areas were not identified in any way to help ensure that the client's equipment was not easily distinguishable.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
1.22	Data hall walls are continuous from floor to ceiling.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that the data hall walls were continuous from floor to ceiling.</p> <p>Observed the data hall walls at each location to verify that the data hall walls were continuous from floor to ceiling.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

## Physical Security

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.23	Delivery and loading docks are separated from the data halls. DataBank employees are required to be present within the delivery and loading dock areas to open the door and monitor access while the door remains open.	Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that delivery and loading docks were separated from the data halls. DataBank employees were required to be present within the delivery and loading dock areas to open the door and monitor access while the door remains open.  Observed the separation of loading docks and data halls at each location to verify that delivery and loading docks were separated from the data center floors.	No relevant exceptions noted.  No relevant exceptions noted.

## Environmental Security

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that relevant information technology infrastructure is protected from certain environmental threats.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.1	Documented environmental security policies and procedures are in place to govern environmental security practices.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that documented environmental security policies and procedures were in place for each location to govern environmental security practices.</p> <p>Inspected the Emergency Procedures for each location to verify that documented environmental security policies and procedures were in place for each location to govern environmental security practices.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
2.2	<p>Data hall areas are equipped with the following fire detection and suppression systems:</p> <ul style="list-style-type: none"> <li>➤ Audible and visual fire alarms;</li> <li>➤ Dry-pipe water sprinklers;</li> <li>➤ Automated FM200 extinguisher system; (Edina, MN only)</li> <li>➤ Hand-held fire extinguishers; and</li> <li>➤ Fire and smoke detectors.</li> </ul>	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that data hall areas were equipped with the following fire detection and suppression systems:</p> <ul style="list-style-type: none"> <li>➤ Audible and visual fire alarms;</li> <li>➤ Dry-pipe water sprinklers;</li> <li>➤ Automated FM200 extinguisher system; (Edina, MN only)</li> <li>➤ Hand-held fire extinguishers; and</li> <li>➤ Fire and smoke detectors.</li> </ul> <p>Observed the data centers at each location to verify that data hall areas were equipped with the following fire detection and suppression systems:</p> <ul style="list-style-type: none"> <li>➤ Audible and visual fire alarms;</li> <li>➤ Dry-pipe water sprinklers;</li> <li>➤ Automated FM200 extinguisher system; (Edina, MN only)</li> <li>➤ Hand-held fire extinguishers; and</li> <li>➤ Fire and smoke detectors.</li> </ul>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

## Environmental Security

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that relevant information technology infrastructure is protected from certain environmental threats.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.3	On an annual basis, Management contracts third-party vendors to complete fire detection and suppression equipment inspections.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that management contracted third-party vendors to complete fire detection and suppression equipment inspections on an annual basis.</p> <p>Inspected the fire detection and suppression reports for each location to verify that management contracted third-party vendors to complete fire detection and suppression equipment inspections on an annual basis.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
2.4	Data hall areas are equipped with multiple dedicated air handling units.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that data hall areas were equipped with multiple dedicated air handling units.</p> <p>Observed the data centers to verify that data hall areas were equipped with multiple dedicated air handling units.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
2.5	For the Dallas and Richardson locations, the air handling units are supported by multiple cooling towers in a redundant configuration.	<p>Inquired of the Provisioning Manager in Dallas, TX; and Director of Facilities in Richardson, TX to verify that air handling units were supported by multiple cooling towers in a redundant configuration.</p> <p>Observed the air handling units for each location to verify that the air handling units were supported by multiple cooling towers in a redundant configuration.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
2.6	For the Dallas and Richardson locations, secure water tanks provide cooling towers with water in the event external supply lines are unavailable.	Inquired of the Provisioning Manager in Dallas, TX; and the Director of Facilities in Richardson, TX to verify that secure water tanks provide cooling towers with water in the event external supply lines are unavailable.	No relevant exceptions noted.

## Environmental Security

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that relevant information technology infrastructure is protected from certain environmental threats.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.7	On an annual basis, Management contracts third-party vendors to complete inspections on the air handling units.	<p>Observed the cooling tower water tanks at the Dallas and Richardson facilities to verify that secure water tanks provide cooling towers with water in the event external supply lines are unavailable.</p> <p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that management contracted third-party vendors to complete inspections of the air handling units on an annual basis.</p> <p>Inspected the most recent air handling unit inspection reports and invoices for each location to verify that management retained the inspection reports completed by third-party vendors to evidence completion of the air handling units on an annual basis.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
2.8	Data hall 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.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that data hall 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.</p> <p>Observed the water detection devices to verify that data hall 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.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

## Environmental Security

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that relevant information technology infrastructure is protected from certain environmental threats.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.9	Data hall areas are available with raised flooring and/or server racks to elevate equipment and help facilitate cooling.	<p>Inquired of the Facility Directors for each location to verify that data hall areas were available with raised flooring and/or server racks to elevate equipment and help facilitate cooling.</p> <p>Observed the data halls to verify that data hall areas were available with raised flooring and/or server racks to elevate equipment and help facilitate cooling.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
2.10	The data halls have redundant electrical utility feeds.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that the data halls had redundant electrical utility feeds.</p> <p>Observed the data halls at each location to verify that the data centers had redundant electrical utility feeds.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
2.11	PDUs are in place to mitigate the risk of electrical power issues impacting the data center facility's infrastructure.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that PDUs were in place to mitigate the risk of electrical power issues impacting the data center facility's infrastructure.</p> <p>Observed the data centers at each location to verify that PDUs were in place to mitigate the risk of electrical power issues impacting the data center facility's infrastructure.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
2.12	Data center infrastructures are configured to be connected to redundant UPS systems.	Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that data center infrastructures were configured to be connected to redundant UPS systems.	No relevant exceptions noted.

## Environmental Security

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that relevant information technology infrastructure is protected from certain environmental threats.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.13	On an annual basis, Management contracts third-party vendors to complete inspections of the UPS systems.	<p>Observed the data centers at each location to verify that data center infrastructures were configured to be connected to redundant UPS systems.</p> <p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that management contracted third-party vendors to complete inspections of the UPS systems on an annual basis.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
2.14	UPS breakers protect data center infrastructures from potential electrical issues during UPS system maintenance.	<p>Inspected the most recent UPS inspection reports for each location to verify that management contracted third-party vendors to complete inspections of the UPS systems on an annual basis.</p> <p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that UPS breakers protected data center infrastructures from potential electrical issues during UPS system maintenance.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
2.15	The data centers are connected to multiple generators configured to provide electricity in the event of a power outage.	<p>Observed the UPS units at each location to verify that UPS breakers protected data center infrastructures from potential electrical issues during UPS system maintenance.</p> <p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that the data centers were connected to multiple generators configured to provide electricity in the event of a power outage.</p>	<p>No relevant exceptions noted.</p>

## Environmental Security

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that relevant information technology infrastructure is protected from certain environmental threats.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.16	On an annual basis, Management contracts third-party vendors to complete load bank testing of the generators.	<p>Observed the data centers at each location to verify that the data centers were connected to multiple generators configured to provide electricity in the event of a power outage.</p> <p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that management contracted third-party vendors to complete load bank testing of the generators on an annual basis.</p> <p>Inspected the most recent load bank testing reports from each location to verify that management contracted third-party vendors to complete load bank testing of the generators on an annual basis.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
2.17	The data halls' floor tiles are grounded and covered with an anti-static covering to reduce the occurrence of electro-static buildup.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that the data halls' floor tiles were grounded and covered with an anti-static covering to reduce the occurrence of electro-static buildup.</p> <p>Observed the data halls at each location to verify that the data halls' floor tiles were grounded and covered with an anti-static covering to reduce the occurrence of electro-static buildup.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>



## Environmental Security

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that relevant information technology infrastructure is protected from certain environmental threats.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.19	The environmental monitoring system is configured to notify security and data center personnel when predefined thresholds are exceeded on monitored devices.	Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that the environmental monitoring systems were configured to notify security and data center personnel when predefined thresholds were exceeded on monitored devices.  Inspected example email alerts from the environmental monitoring systems of each location to verify that environmental monitoring systems were configured to notify security and data center personnel when predefined thresholds were exceeded on monitored devices.	No relevant exceptions noted.  No relevant exceptions noted.

## Customer Provisioning

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that new client environments are provisioned according to standardized methodologies and to mutually agreed upon criteria and contractual obligations.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	<p>Executed MSAs are maintained with customers to define the terms of services provided including, but not limited to, the following:</p> <ul style="list-style-type: none"> <li>➤ Nature, timing and extent of services provided;</li> <li>➤ Roles and responsibilities;</li> <li>➤ Service warranties; and</li> <li>➤ Intellectual property and confidentiality requirements.</li> </ul>	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that MSAs were maintained with customers to define the terms of services provided including, but not limited to, the following:</p> <ul style="list-style-type: none"> <li>➤ Nature, timing and extent of services provided;</li> <li>➤ Roles and responsibilities;</li> <li>➤ Service warranties; and</li> <li>➤ Intellectual property and confidentiality requirements.</li> </ul> <p>Inspected MSAs for the selected sample of new customers to verify that MSAs were maintained with customers to define the terms of services provided including, but not limited to, the following:</p> <ul style="list-style-type: none"> <li>➤ Nature, timing and extent of services provided;</li> <li>➤ Roles and responsibilities;</li> <li>➤ Service warranties; and</li> <li>➤ Intellectual property and confidentiality requirements.</li> </ul>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
3.2	<p>SLAs are maintained for customers that define specific performance metrics and service level requirements.</p>	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that SLAs were maintained for customers that define specific performance metrics and service level requirements.</p> <p>Inspected the DataBank SLA and customer files for the selected sample of new customers to verify that SLAs were maintained for customers that define specific performance metrics and service level requirements.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

## Customer Provisioning

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that new client environments are provisioned according to standardized methodologies and to mutually agreed upon criteria and contractual obligations.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.3	Customers who purchase network services are required to sign an Acceptable Use Policy (AUP) that outlines the prohibited uses of network services.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that customers who purchased network services were required to sign an AUP that outlined the prohibited uses of network services.</p> <p>Inspected the DataBank AUP and customer files for the selected sample of new customers to verify that customers who purchased network services were required to sign an AUP that outlined the prohibited uses of network services.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
3.4	A completion letter and start of service notification are sent to customers upon installation of new services. The letter and notification include a description of services and contact information for reporting problems.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that a completion letter and start of service notification were sent to customers upon installation of a new service. The letter and notification included a description of services and contact information for reporting problems.</p> <p>Inspected Completion Notice / Start of Service Notifications for the selected sample of new clients and client changes during the audit period to verify that a completion letter and start of service notification were sent to customers upon installation of a new service. The letter and notification included a description of services and contact information for reporting problems.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
3.5	A Customer Information Guide is sent to customers upon installation of a new service.	Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that a Customer Information Guide was sent to customers upon installation of a new service.	No relevant exceptions noted.

## Customer Provisioning

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that new client environments are provisioned according to standardized methodologies and to mutually agreed upon criteria and contractual obligations.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.6	A customer authorized requestor list is maintained for each customer that lists the authorized customer contacts with the ability to initiate changes to subscribed services.	Inspected a New Client Documents email for the sample of new clients to verify that a Customer Information Guide was sent to customers upon installation of a new service.	No relevant exceptions noted.
3.7	DataBank requires all customers to obtain comprehensive general liability insurance coverage.	Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that an authorized requestor list was maintained for each customer that listed the authorized customer contacts with the ability to initiate changes to subscribed services.	No relevant exceptions noted.
3.7	DataBank requires all customers to obtain comprehensive general liability insurance coverage.	Inspected the authorized requestor list for a sample of new customers to verify that an authorized requestor list was maintained for each customer that listed the authorized customer contacts with the ability to initiate changes to subscribed services.	No relevant exceptions noted.
3.8	New client procedures are documented in a new client checklist to guide personnel during the new client process.	Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that DataBank required all customers to obtain comprehensive general liability insurance coverage.	No relevant exceptions noted.
3.8	New client procedures are documented in a new client checklist to guide personnel during the new client process.	Inspected MSAs for the selected sample of new customers to verify that DataBank required customers to obtain comprehensive general liability insurance coverage.	No relevant exceptions noted.
3.8	New client procedures are documented in a new client checklist to guide personnel during the new client process.	Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN 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.

## Customer Provisioning

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that new client environments are provisioned according to standardized methodologies and to mutually agreed upon criteria and contractual obligations.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.9	DataBank notifies clients of entry to client areas due to maintenance needs.	<p>Inspected the new client checklists for the selected sample of new clients to verify that new client procedures were documented in a new client checklist to guide personnel during the new client process.</p> <p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that DataBank notified clients of entry to client areas due to maintenance needs.</p> <p>Inspected a sample of maintenance notifications from each facility to verify that DataBank notified clients of entry to client areas due to maintenance needs.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

## Network Monitoring

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that network service is monitored and problems are tracked, escalated, and resolved in accordance with service level agreements.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.1	Documented incident response procedures are in place to guide personnel in monitoring, documenting, escalating and resolving problems affecting services provided. The procedures include defined severity levels, escalation procedures and response time requirements for service alerts.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating and resolving problems affecting services provided. The procedures included defined severity levels, escalation procedures and response time requirements for service alerts.</p> <p>Inspected the Incident Management Process to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating and resolving problems affecting services provided. The procedures included defined severity levels, escalation procedures and response time requirements for service alerts.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
4.2	Monitoring personnel are available on-site 24 hours a day at the Dallas, Texas and Richardson, Texas facilities. The Edina, Minnesota facility maintains personnel onsite during business hours with remote monitoring from another DataBank location for after hours. Edina personnel are on-call 24 hours per day for resolution of problem.	Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that monitoring personnel were available on-site 24 hours a day at the Dallas, Texas and Richardson, Texas facilities. The Edina, Minnesota facility maintained personnel onsite during business hours with remote monitoring provided by another DataBank location after hours. Edina personnel were on-call 24 hours per day for resolution of problem.	No relevant exceptions noted.

## Network Monitoring

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that network service is monitored and problems are tracked, escalated, and resolved in accordance with service level agreements.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.3	<p>Monitoring applications are utilized to monitor the following performance, availability, and controlled events for data center infrastructure:</p> <ul style="list-style-type: none"> <li>➤ Availability of the network, host services and ports;</li> <li>➤ CPU and hard disk utilization;</li> <li>➤ Temperature and cooling systems; and</li> <li>➤ Power supply and voltage.</li> </ul>	<p>Inspected schedules and on-call schedules and the on-call rotation and monitoring tools to verify that monitoring personnel were available on-site 24 hours a day at the Dallas, Texas and Richardson, Texas facilities. The Edina, Minnesota facility maintained personnel onsite during business hours with remote monitoring provided by another DataBank location after hours. Edina personnel were on-call 24 hours per day for resolution of problem.</p> <p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that monitoring applications were utilized to monitor the following performance, availability, and controlled events for data center infrastructure:</p> <ul style="list-style-type: none"> <li>➤ Availability of the network, host services and ports;</li> <li>➤ CPU and hard disk utilization;</li> <li>➤ Temperature and cooling systems; and</li> <li>➤ Power supply and voltage.</li> </ul> <p>Inspected the monitoring applications and their configurations to verify that monitoring applications were utilized to monitor the following performance, availability, and controlled events for data center infrastructure:</p> <ul style="list-style-type: none"> <li>➤ Availability of the network, host services and ports;</li> <li>➤ CPU and hard disk utilization;</li> <li>➤ Temperature and cooling systems; and</li> <li>➤ Power supply and voltage.</li> </ul>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

## Network Monitoring

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that network service is monitored and problems are tracked, escalated, and resolved in accordance with service level agreements.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.4	In the event predefined thresholds are exceeded, monitoring applications are configured to generate automated onscreen and e-mail alert notifications.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that in the event predefined thresholds were exceeded, monitoring applications were configured to generate automated onscreen and e-mail alert notifications.</p> <p>Inspected examples of Nagios Alert Notifications to verify that in the event predefined thresholds were exceeded, monitoring applications were configured to generate automated onscreen and e-mail alert notifications.</p> <p>Observed the Nagios system and on screen alerts to verify that monitoring applications were configured to generate automated onscreen and e-mail alert notifications in the event predefined thresholds were exceeded.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
4.5	Statistical reports are reviewed on a monthly basis to monitor and gauge the services provided against performance metrics and defined service levels.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that statistical reports were reviewed on a monthly basis to monitor and gauge the services provided against performance metrics and defined service levels.</p> <p>Inspected the recurring Operations Management Meeting calendar invite to verify that statistical reports were reviewed on a monthly basis to monitor and gauge the services provided against performance metrics and defined service levels.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

## Network Monitoring

**Control Objective Specified by the Service Organization:** Control activities provide reasonable assurance that network service is monitored and problems are tracked, escalated, and resolved in accordance with service level agreements.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.6	An incident ticketing system is utilized to document, prioritize, escalate and help resolve problems affecting services provided.	<p>Inquired of the Provisioning Manager in Dallas, TX; Director of Facilities in Richardson, TX; and Sr. Technician in Edina, MN to verify that an incident ticketing system was utilized to document, prioritize, escalate and help resolve problems affecting services provided.</p> <p>Observed the ticketing system to verify that an incident ticketing system was utilized to document, prioritize, escalate and help resolve problems affecting services provided.</p> <p>Inspected incident tickets for the selected sample of incidents during the audit period to verify that an incident ticketing system was utilized to document, prioritize, escalate and help resolve problems affecting services provided.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>