Insite Data Services, Inc.
Lincoln, Nebraska

System and Organization Controls Report on the Description and Tests of Operating Effectiveness

Controls Placed in Operation Relevant to Security and Availability

SOC 2® Type 2 Report

August 1, 2017 to July 31, 2018

CPAs and Consultants

Insite Data Services, Inc.

System and Organization Controls Report on the Description and Tests of Operating Effectiveness
August 1, 2017 to July 31, 2018

TABLE OF CONTENTS

Section 1
Insite Data Services, Inc.’s Assertion on Controls

INSITE DATA SERVICES

Insite Data Services, Inc.'s Assertion on Controls

We have prepared the attached description in Section 3 titled "Description of the Insite Core Banking Platform-as-a-Service System Provided by Insite Data Services, Inc." (the "description") throughout the period August 1, 2017 to July 31, 2018, based on the criteria in item #1 below, which are the criteria for a description of a service organization's system set forth in paragraphs 1.26-1.27 of the American Institute of Certified Public Accountants (AICPA) guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (*SOC 2®*)* (the "description criteria") *.* The description is intended to provide users with information about Insite Data Services, Inc.'s (the "Company") Insite Core Banking Platform-as-a-Service System, (the "system"), particularly system controls intended to meet the criteria for the Security and Availability principles set forth in TSP Section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*the "*AICPA *Trust Services Principles and Criteria"*) (the "applicable trust services criteria").

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

1. The description fairly presents the Insite Core Banking Platform-as-a-Service System made available to user entities of the system throughout the period August 1, 2017 to July 31, 2018. The Company uses multiple third-party organizations to support the Insite Core Banking Platform-as-a-Service System. The description in Section 3 of this report includes only the criteria and related controls of the Company and excludes the criteria and related controls of the aforementioned third-party organizations. Our assertion is based on the following description criteria:

    a. The description contains the following information:

        1. The types of services provided.
        2. The components of the system used to provide the services, which are the following:
            a) *Infrastructure* - The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).
            b) *Software* - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
            c) *People* - The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
            d) *Procedures* - The automated and manual procedures involved in the operation of a system.
            e) *Data* - Transaction streams, files, databases, tables, and output used or processed by the system.
        3. The boundaries or aspects of the system covered by the description.
        4. For information provided to, or received from, third-party organizations or other parties:
            a) How such information is provided or received and the role of the third-party organization and other parties.
            b) The procedures the Company performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

Insite Data Services' Assertion on Controls (Continued)

5. The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:
   a) Complementary user entity controls contemplated in the design of the Insite Core Banking Platform-as-a-Service System.
   b) When the inclusive method is used to present a third-party organization, controls at the third-party organization.
6. For third-party organizations presented using the carve-out method:
   a) The nature of the services provided by the third-party organization.
   b) Each of the applicable trust services criteria that are intended to be met by controls at the third-party organization, alone or in combination with controls at the Company, and the types of controls expected to be implemented at carved-out third-party organizations to meet those criteria.
7. Any applicable trust services criteria that are not addressed by a control at the Company or a third-party organization and the reasons.
8. In the case of a Type 2 report, the relevant details of changes to the Company's system throughout the period covered by the description.

b. The description does not omit or distort information relevant to the Company's Insite Core Banking Platform-as-a-Service System, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities and may not, therefore, include every aspect of the Insite Core Banking Platform-as-a-Service System that individual user entities may consider important to their own particular needs.

2. The controls stated in the description were suitably designed throughout the period August 1, 2017 to July 31, 2018, to meet the applicable trust services criteria.

3. The controls stated in the description operated effectively throughout the period August 1, 2017 to July 31, 2018, to meet the applicable trust services criteria.

Section 2
Independent Service Auditor's Report

WIPFLi

Independent Service Auditor's Report

Management of Insite Data Services, Inc.
Lincoln, Nebraska

Scope

We have examined the accompanying description in Section 3 titled "Description of the Insite Core Banking Platform-as-a-Service System Provided by Insite Data Services, Inc." (the description) based on the criteria set forth in paragraphs 1.26 – 1.27 of the American Institute of Certified Public Accountants (AICPA) Guide "*Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy" (*SOC 2®) (the description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the Security and Availability principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* ("AICPA, *Trust Services Principles and Criteria"*) (the applicable trust services criteria), throughout the period August 1, 2017 to July 31, 2018.

The description indicates that certain applicable trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of the Insite Data Services, Inc.'s (IDS) controls are suitably designed and operating effectively, along with related controls at the Company. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

As indicated in the description, IDS utilizes multiple third-party organizations to operate and manage various aspects of its Insite Core Banking Platform-as-a-Service System. The description indicates that certain applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at the third-party organizations are suitably designed and operating effectively. The description presents IDS' system, its controls relevant to the applicable trust services criteria, and the types of controls that the service organization expects to be suitably designed, implemented, and operating effectively at the third-party organizations to meet certain applicable trust services criteria. The description does not include any of the controls expected to be implemented at the third-party organizations. Our examination did not extend to the services provided by the third-party organizations, and we have not evaluated whether the controls management expects to be implemented at the third-party organizations have been suitably designed, implemented, and operating effectively throughout the period August 1, 2017 to July 31, 2018.

The information included in Section 5 titled "Other Information Provided by Insite Data Services" is presented by management of IDS to provide additional information and is not a part of the description. Information about IDS' management responses has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, and accordingly we express no opinion on it.

Service Organization's Responsibilities

IDS has provided its attached assertion in Section 1 titled "Insite Data Services, Inc.'s Assertion on Controls" about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria.

Independent Service Auditor's Report (Continued)

The Company is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting the controls to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust service criteria and stating them in the description.

Service Auditor's Responsibilities

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

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period August 1, 2017 to July 31, 2018.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of the controls involves:

- Evaluating and performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria and the controls were suitability designed and operating effectively, to meet the applicable trust services criteria throughout the period August 1, 2017 to July 31, 2018.
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively.
- Testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- Evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the Company in their assertion.

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

Inherent Limitations

Due to their nature and inherent limitations, controls at a service organization may not prevent or detect and correct all errors or omissions in providing services. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Independent Service Auditor's Report (Continued)

Opinion
In our opinion, in all material respects, based on the description and the applicable trust services criteria:

a. The description fairly presents the system that was designed and implemented throughout the period August 1, 2017 to July 31, 2018.
b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period August 1, 2017 to July 31, 2018, and user entities applied the complementary user entity controls contemplated in the design of IDS' controls throughout the period August 1, 2017 to July 31, 2018, and the third-party organizations applied the types of controls expected to be implemented at the third-party organizations throughout the period August 1, 2017 to July 31, 2018.
c. The controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period August 1, 2017 to July 31, 2018, if user entities applied the complementary user entity controls contemplated in the design of IDS's controls, and those controls operated effectively throughout the period August 1, 2017 to July 31, 2018, and if the controls expected to be implemented at the third-party organizations were also operating effectively throughout the period August 1, 2017 to July 31, 2018.

Description of Tests of Controls
The specific controls we tested and the nature, timing, and results of those tests are presented in Section 4 titled "Trust Services Principles, Criteria, and Related Controls and Independent Service Auditor's Tests of Controls and Results."

Intended Use
This report, including the description of the tests of controls and results thereof in Section 4, are intended solely for the information and use of IDS; user entities of IDS' Insite Core Banking Platform-as-a-Service System during some or all of the period August 1, 2017 to July 31, 2018; and prospective user entities, independent auditors, practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the services provided by IDS
- How IDS' system interacts with user entities, third-party organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and how they interact with related controls at IDS and third-party organizations to meet the applicable trust services criteria
- The nature of third-party organizations and how their services to a service organization may affect user entities
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

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

Wipfli LLP

Wipfli LLP

Minneapolis, Minnesota
September 26, 2018

Section 3
Description of the Insite Core Banking Platform-as-a-Service System Provided by Insite Data Services, Inc.

Description of the Insite Core Banking Platform-as-a-Service System Provided by Insite Data Services

Overview of Operations

Background

Insite Data Services, Inc. (“IDS” or the “Company”), located in Lincoln, Nebraska, provides hosting solutions to community banks. IDS offers three main solutions: application hosting, data protection, and secure email. By partnering with industry technology providers, IDS offers quality products with personal service.

Typical IDS clients are:

- Community banks using the lnsite Core Banking Platform-as a-Service (PaaS) system
- Community banks with limited IT resources

IDS was founded in 2008 and is a wholly owned subsidiary of Automated Systems, Inc. (ASI), a software development and business consulting services company. Although ASI is the parent company, IDS has separate management who operate and are responsible for the hosted platform and remote backup services. IDS employs approximately 12 people, based in the Lincoln, Nebraska, headquarters.

Overview of Services

IDS provides cloud computing services for the financial institutions industry, with a specific focus on serving the community bank sector. The cloud computing services are designed to host applications, data, email, and/or platforms on behalf of community banks with limited IT resources. User entities contract with ASI to license the lnsite Core Banking system and other applications developed and maintained by ASI. These customers may also contract with IDS to provide a hosted platform to access the lnsite Core Banking system and other applications. This hosted platform is known as the lnsite Core Banking System Platform as a Service (PaaS). Development and maintenance of the applications used by the user entities is the responsibility of ASI (or other application provider). IDS is responsible only for maintaining the hosted platform that is used to access those applications.

Application Hosting

Application hosting services allow community banks to leverage the infrastructure of an existing data center with the technical expertise offered by the IDS team of certified network engineers and technicians. Applications are hosted on the lnsite Core Banking PaaS system as specified by the user entity. IDS is not responsible for the development, maintenance, or management of the applications hosted on the lnsite Core Banking PaaS system.

Remote Backup Service

The IDS remote backup service provides an alternative to traditional tape backup. It provides users with an automated online solution that includes centralized and automated backups of file servers, PCs, and application/database servers, along with secure off-site storage and online restoration.

Overview of Operations (Continued)

Additional Services

In addition to hosting the lnsite Core Banking PaaS system, IDS offers other services available to its clients, including hosting the following applications that are developed and maintained by ASI (shown below). These additional services, applications, and offerings are not included in the scope of this report.

- IDS On-Time system
- Insite iTeller
- Insite iPortal
- Insite Checking Imaging
- Insite Online Banking
- Insite Business Banking
- Insite Mobile Banking
- Insite iDeposit
- Real-Time ATM
- Insite Document Imaging
- Microsoft Office Suite
- Secure email

Scope of Report

The scope of this report includes the principles for the lnsite Core Banking PaaS system provided to IDS' customers, specifically the application hosting and data backup services.

Although the platform may host some of the applications and systems listed above, the scope of this report is limited to the controls related to the PaaS. Development and maintenance of the applications used by the user entities is the responsibility of ASI (or other application provider). IDS is responsible only for maintaining the hosted platform that is used to access those applications.

IDS uses the following subservice organizations to perform aspects of the lnsite Core Banking PaaS system:

- Automated Systems, Inc. for network security services related to the resolution of potential security threats identified during automated vulnerability scans of client environments
- SHAZAM for data center colocation, network security services, and physical security and environmental controls for the data center facility in Johnston, Iowa. (The SHAZAM data center is used to host customer environments that have ATM services.)
- TierPoint for data center colocation, network security services, and physical security and environmental controls for the data center facility in Papillion, Nebraska. (The TierPoint data center is used to host customer environments that do not have ATM services.)

The accompanying description includes only those controls relevant to the applicable trust services criteria of IDS and does not include controls performed by subservice organizations.

Overview of Operations (Continued)

Infrastructure and Software

The lnsite Core Banking PaaS system is a hosted PaaS for community banks. User entities coordinate specific aspects of their systems and applications to be hosted and backed up as part of the PaaS. IDS uses Hewlett-Packard (HP) and Dell enterprise-class servers, VMware, and Windows servers to create the platform for user entities.

IDS also uses the following major equipment components:

- Nimble Storage and Dell Equallogic SANs
- Cisco, HP, and Dell enterprise switches
- HP Tipping Point

Operating System

The principal component of the operating system for the server equipment is the VMware Hypervisor, ESXi. The other operating systems installed on top of the virtualized layer are Windows 2008 R2, 2012 R2, and 2016.

Description of the Insite Core Banking Platform-as-a-Service System

People

The primary responsibility for the delivery and security of services provided by the hosting services team is assigned to the chief operating officer (COO). In addition, a senior security engineer is responsible for monitoring the environment and IDS' security and availability commitments. Other key individuals responsible for the daily operations of IDS are the system administrator, the network technicians, and the network manager. Management informally meets quarterly to develop strategic plans and monitor the operation of the organization. The senior security engineer meets with management to develop short- and long-term agendas for developing the technical infrastructure and defining the overall business initiatives of the company.

Management of IDS is the responsibility of Craig Slaby, COO and information security officer. The other key individuals responsible for the daily operations of IDS include:

Individual	Position
Darrell Ptascheck	Network Technician Manager
Eric McClelland	Network Technician
Edward Buchanan	Network Technician
Jennifer Wilson	Network Monitor
Tristan Lawson	Senior Security Engineer
Nicole Woods	Information Security Analyst

IDS maintains an organization chart that defines reporting lines and is reviewed annually by management. The IDS organization is categorized into the following functional areas:

Description of the Insite Core Banking Platform-as-a-Service System (Continued)

Information Technology (IT)

IT is responsible for daily operations and oversees the computer infrastructure, website, network connectivity, and user access security. IT is also responsible for the support and administration of the hosted services infrastructure. The senior security engineer and information security officer are responsible and accountable for developing, maintaining, and enforcing the Company's system availability and related security policies.

IT also monitors the status of hardware, operating systems, and security features for errors or potential breaches of security.

Management

Management is responsible for human resources (HR), administrative policies and procedures, accounting, facilities, and staff training.

Service and Support

Service and Support is responsible for providing assistance to clients to solve issues and answer questions related to the use of hosted products. Services are provided via telephone, email, or Web conference. IDS platform users can report security and availability failures, incidents, concerns, and complaints to IDS through a secure online customer portal.

Procedures

IDS has established procedures for the key controls and processes within the hosting environment, including change management, security, personnel, monitoring, incident response, and other areas as they relate to security and availability. In addition, key information regarding employee expectations, acceptable use, and internal processes is documented in the Employee Handbook.

Information Technology Security Policy

IDS has implemented an IT Security Policy. Security policies and guidelines are documented and communicated throughout the organization. IDS' policy on information security addresses the following:

- Information classification
- Handling of sensitive information
- Destruction of information, data, and media
- Access management
- Password management
- Physical security of computers
- Communication systems
- Remote access
- Viruses and malicious software
- Establishing network connections
- Encryption
- Firewall maintenance and monitoring
- Logging and monitoring
- Third-party access and outsourced services
- Third-party information disclosure
- Privacy
- Change management
- Reporting a problem
- Incident response

Description of the Insite Core Banking Platform-as-a-Service System (Continued)

Procedures (Continued)

The senior security engineer is responsible for maintaining and updating the policies as needed. Updates are presented to management and the IT Steering Committee for review and approval as needed.

Data

IDS regards data as proprietary and restricts access to resources based on role. Clients are assigned logically separate environments, and client data is restricted to the assigned environment.

The input and output of data hosted on the Insite Core Banking PaaS system is the responsibility of user entities. Users can input data into the applications hosted on the platform and extract information from those applications for use in their own environments. Processing and safeguarding of the data within the hosted applications is the responsibility of the provider that develops and maintains the application.

IDS personnel do not add, modify or remove data within client environments. IDS' interactions with client data are limited to performing maintenance on database servers, conducting data backups, and performing data restoration exercises with clients as requested.

IDS is also responsible for implementing network-level encryption and determining whether production data is secured to meet client requirements. A data classification matrix exists as part of the Information Sensitivity Policy to define the requirements for maintaining security over this information.

Control Environment

IDS attempts to attract and retain highly skilled business professionals. Employee job descriptions that include a position summary and describe major duties, academic and professional requirements, and responsibilities are developed by the department managers. IDS performs employment screening and new employee orientation as well as provides ongoing training opportunities for personnel.

Personnel Practices

Personnel policies and procedures are documented in the IDS Employee Handbook and communicated to employees. IDS performs employment screening, including background checks prior to hire, and new employee orientation. Employees acknowledge receipt of the Employee Handbook and personnel policies and procedures upon hire.

Description of the Insite Core Banking Platform-as-a-Service System Provided by Insite Data Services

Relevant Aspects of Internal Control

Risk Assessment Process

Management is responsible for setting strategic direction and prioritizing system needs and development projects, personnel administration, and day-to-day policy issues. A formal risk assessment is performed annually to identify potential natural, environmental, human and technical threats to the IDS platform.

During the risk assessment process IDS evaluates controls that are in place to mitigate threats and vulnerabilities.

Internal and external vulnerability scans are performed for the hosted platform using an industry-accepted scanning tool:

- IDS automatically runs external vulnerability scans of client environments on a quarterly basis.
- IDS automatically runs internal vulnerability scans of client environments on a weekly basis.

Results of the internal and external vulnerability scans are logged by the vulnerability scanning system, and the system automatically creates a ticket for tracking and resolving high-risk issues identified during the scans. The subservice organization, ASI, is responsible for completing the necessary updates to systems and resolving tickets created as a result of these scans.

An IT Steering Committee exists and includes members of management and is led by the COO. The committee meets on a quarterly basis to discuss environmental, regulatory, and technological issues that may impact security and availability commitments. The related policies are updated based on management feedback and approved by the IT Steering Committee.

Information and Communication Systems

The Insite Core Banking PaaS system is composed of servers, workstations and other infrastructure devices that maintain the hosted platform for user entities of the system. IDS uses HP and Dell enterprise class servers to create a hosted platform to run applications that support core processing.

Employee Communications

IDS' management is committed to maintaining effective communication with employees. Updates on performance and other matters of interest are communicated at employee meetings and through other methods, such as the Company intranet, email and hand-delivered distributions.

The senior security engineer is assigned the responsibility and is accountable for reviewing security and availability policies at least annually and updating the policies as needed. Policies are presented to the IT Steering Committee for approval. They provide guidance to employees and serve as a foundation for detailed divisional and departmental policies and procedures. Policies broadly cover planning and development, operations, IT and customer service.

Information and Communication Systems (Continued)

Employee Communications (Continued)

In addition, employees and contractors are provided with annual training to refresh expectations on security and availability matters, including:

- Facilities security
- Information security
- Information classification
- Data destruction
- Acceptable use of communications systems
- Third-party access
- Incident reporting and incident response
- Discipline for policy violations

Either the information security officer or the senior security engineer conducts the security awareness training with employees. Upon completion of the training, IDS employees sign a Policy Compliance Agreement annually to acknowledge their understanding of security and availability requirements.

Management has established a detailed network topology diagram that documents the system and its boundaries, including the implementation of key system components, connection points, and client environments. The description of the system and its boundaries is made available to authorized internal users and stored on a technical documentation repository.

External Communications

IDS communicates security obligations of users and IDS' commitments to users through master services agreements (MSA), service level agreements (SLA), and a Hosted Services Acceptable Use Policy. The MSA and SLA describe the Company's security and availability obligations and commitments to users. Client agreements and the Hosted Services Acceptable Use Policy also provide information on the system description and operation of the hosted platform environment and describe the system responsibilities of both parties and the system technical support available to external users. System users can report security and availability failures, incidents, concerns, and complaints to IDS through a secure online portal.

Changes made to the IDS platform that would affect system security and availability commitments and requirements are communicated to users who are affected by the change. Changes are communicated to customers via an email maintenance notification. During the period August 1, 2017, to July 31, 2018, there were no changes to the IDS security and availability commitments or requirements.

Information and Communication Systems (Continued)

Monitoring Controls

Management Oversight

As needed, the COO meets informally with senior management to make recommendations for improvements to the organization's ability to enhance its system security and availability objectives. The IT Steering Committee meets quarterly to provide oversight of business activities, review policies, and authorize significant changes to the business and/or system, as well as hold recurring discussions on projects, security and availability commitments, policy updates, and upcoming changes to the environment.

Management conducts an annual review of vendors that are key to delivering client service. The COO is responsible for conducting the review and evaluating the status of vendors, including review of vendor nondisclosure agreements, vendor System and Organization Controls (SOC) reports, financials, SLAs, visits to the vendor locations, and business continuity/disaster recovery plans and tests.

System Monitoring

To monitor for threats to system disruption, IDS performs the following system monitoring activities:

- Automated tools monitor system availability, storage capacity, and uptime. The system monitoring tools generate alerts that are sent to IT operations personnel for investigation and resolution.
- Internal and external vulnerability scans are performed for the hosted platform using an industry-accepted scanning tool. Issues identified by the scan are communicated to ASI, the subservice organization, for investigation and resolution.

IDS has defined a process to identify, report, and analyze incidents relating to security and availability issues and documented the process in the Incident Management Policy. IDS' incident management process focuses on the analysis of closed incidents to identify the root causes of errors impacting IT services. Identified incidents are reviewed by management, and corrective actions are taken based on defined incident policies and procedures. High-severity incidents are documented and tracked in the IDS ticketing system. Incidents are reviewed by management, and change requests are prepared for problem resolution if deemed necessary by management. System security and availability breaches and issues are documented and tracked in a ticketing system and reviewed by the COO.

Controls Related to the Common Criteria

Physical Access

IDS has partnered with two subservice organizations to provide data center and colocation services and to maintain physical security and environmental controls over the sensitive system components. SHAZAM provides colocation services from its data center in Johnston, Iowa, for IDS customers using ATM services. TierPoint provides colocation services from its data center in Papillion, Nebraska, for non-ATM IDS customers.

Physical access to the SHAZAM and TierPoint data centers that contain the Insite Core Banking PaaS system servers is authorized by IDS management for new users. No IDS employees were granted new physical access to the third-party data centers during the period August 1, 2017, to July 31, 2018.

Management reviews IDS users with access to the data centers annually for appropriateness. Updates to user access are completed by IT personnel if needed. Physical access to the SHAZAM and TierPoint data centers is removed for terminated IDS users and tracked in a ticket.

Logical Access

IDS is responsible for administering security on the hosted platform, the operating systems, and the network that are part of the Insite Core Banking PaaS system.

Internal User Access

Access to systems in the hosted environment requires the use of unique logon credentials, and audit logs are enabled on the domains to record user activity on the systems. For clients that have requested audit logs of administrator activity on their platform, the audit logs generated from Total Privileged Access Management (TPAM) and Beyond Trust, which are user activity logging tools. The TPAM reports are posted to the client's customer portal, and the Beyond Trust reports are emailed monthly for review. Financial institutions are responsible for reviewing security reports sent by IDS for authorized activity and implementing appropriate countermeasures if applicable.

Access to the production servers also requires the use of authentication credentials (a minimum length of seven characters, complexity requirements enabled, expiration after 42 days, and password history of four iterations). Accounts are set to lock out after 30 minutes of inactivity and three invalid access attempts. New employee system access is documented in a ticket and is approved by IDS management prior to the employee being issued system credentials. Clients are responsible for authorizing and maintaining the users in their environment.

Employees are removed from their positions when terminated or discharged. Accounts are disabled, and keys and electronic access devices are obtained from terminated employees. A request is submitted to information systems upon termination to trigger removal of user access to systems.

The network infrastructure for IDS is managed by SHAZAM and TiePpoint. At the SHAZAM colocation facility, SHAZAM is responsible for maintaining and administering the firewall. At the TierPoint facility, IDS has installed a firewall that is managed and administered by IDS' operations personnel. There is also a firewall deployed in SHAZAM which IDS maintains which is located behind the SHAZAM maintained firewall. IDS has firewalls in place to restrict the traffic permitted from the Internet to the platform based on previously authorized or whitelisted IP addresses. The senior security engineer is responsible for maintaining the firewall rulesets.

Controls Related to the Common Criteria (Continued)

Logical Access (Continued)

Internal User Access (Continued)

Authentication to network infrastructure (routers, switches, and firewalls) in the hosted environment requires the use of passwords. Users are authenticated by the VPN server through specific client software and unique user ID and passwords that match the requirements of the network passwords. Remote access through the VPN server is secured with Advanced Encryption Standard (AES) 256-bit encryption.

IDS performs an annual review of users with the ability to modify security settings, including system security, firewalls, network security devices, and other hardware, to validate that users are authorized and access is appropriate. IDS also performs an annual review of system administrator privileges or superuser functionality to determine whether access is restricted to authorized and appropriate individuals.

External User Access

In order to securely connect to the lnsite Core Banking PaaS system, clients are provided with a VPN appliance to create a secure connection between the client location and the hosted platform. Clients are responsible for installing and maintaining the VPN appliance provided by IDS personnel during setup. Responsibility for adhering to this system requirement is documented in the MSA.

Clients are able to access the platform via an online portal. After logging on to their local workstation, clients accessing the platform via the online portal are required to authenticate with a username and password. Password settings are controlled by the client and client administrators are responsible for maintaining authentication requirements in accordance with the client's specific information security requirements. Once authenticated to the lnsite Core Banking PaaS system, clients may then access their specific hosted environment.

IDS uses documented hardening guidelines to establish new systems with the appropriate security setup. Services and protocols deemed unnecessary by management are disabled by default.

AntiVirus and Intrusion Detection

Microsoft Windows servers and internal workstations managed by IDS run antivirus software and antimalware to reduce the risk of malicious software or viruses from infecting the systems. Virus definitions are automatically updated on a daily basis.

IDS has deployed an intrusion detection system at the TierPoint colocation facility to detect unauthorized and/or malicious activity on the network. If malicious or unauthorized activity is detected on the network, an alert is sent to IDS personnel.

Controls Related to the Common Criteria (Continued)

Change Management

IDS performs limited changes to the Insite Core Banking PaaS system and client environments. IDS does not perform change management or software development activities for the applications hosted on the platform; that is the responsibility of ASI and/or other software vendors. IDS is responsible for applying patches to infrastructure, operating system updates, and performing network maintenance for the Insite Core Banking PaaS system.

IDS has developed a Change Management Policy that defines requirements for testing, documenting, and authorizing changes to operating systems, computing hardware, networks, and infrastructure. Technical staff evaluate and document implications of changes to determine the impact they will have on the system. Once technical staff have completed the evaluation, a change request proposal containing an overview of the change is presented to an IDS IT manager for approval. Changes that require testing prior to being promoted to production are implemented in a test environment and evaluated for effectiveness. System changes are documented in a BugNET ticket that contains details of the date of submission and date of change, owner and custodian contact information, nature of change, test results (if applicable), and authorization and completion of the change. Changes to the system components are automatically logged by the BugNET system, including changes made by customer administrators.

In the event of an emergency (such as system failures or issues that need immediate correction to restore operations), changes can be made without prior approval from an IDS IT manager. Once the change has been implemented, a change request is filled out and submitted to management for management approval.

Controls Related Specifically to Availability Criteria

System Monitoring

Automated tools have been implemented to monitor the system availability, storage capacity, and uptime. Alerts are generated and sent to Operations personnel when activity exceeds predefined thresholds.

Backup Procedures and Disaster Recovery

IDS is responsible for the backup of production data that is hosted on the Insite Core Banking PaaS system. Remote backup is performed for user organizations that have engaged for this service. The remote backup service performs off-site backup of data that is hosted at the user organizations' facilities. A Data Backup Policy defines the requirements for completing backups of client-hosted data.

The CommVault tool is configured to perform one full backup upon initial setup and daily incremental backups thereafter, which are stored in the SHAZAM data center. The backup data is replicated between the SHAZAM data center and the Willowmere DR facility and the TierPoint data center in Papillion is replicated with the Bellevue facility. Full backups are kept for 30 days and then deleted.

Controls Related Specifically to Availability Criteria (Continued)

System Monitoring (Continued)

Disaster recovery and contingency processes are tested annually in accordance with the entity's system availability policies. In addition, IDS performs data recovery tests of client hosted data for customers who submit a request to IDS. Financial institutions are responsible for coordinating disaster recovery testing with IDS resources. Upon completion of the data recovery exercise, IDS will send a letter to the applicable bank to confirm the testing results and successful restoration.

Subservice Organizations

IDS uses subservice organizations to perform various functions to support the delivery of services. The scope of this report does not include the controls and related control objectives at the subservice organizations. The following is a description of services provided by the subservice organizations:

Subservice Organization	**Service Provided**
TierPoint	TierPoint is responsible for colocation of its data center in Papillion, Nebraska, for non-ATM customers. It maintains physical and environmental security controls over the data center, monitors and administer the intrusion detection system (IDS), distributed denial-of-service (DDoS) mitigation, and load balancing for the servers hosted at its data center.
Shazam	Shazam is responsible for colocation of its data center for ATM customers. It maintains physical and environmental security controls over the data center, monitors and administer the intrusion detection system (IDS), distributed denial-of-service (DDoS) mitigation, and load balancing for the servers hosted at its data center.
Automated Systems, Inc.	ASI is the parent organization of IDS and is responsible for providing network security services related to the resolution of identified security threats through the external automated vulnerability scans.

Complementary User Entity Controls

IDS' controls were designed with the assumption that certain complementary user entity controls would be operating effectively at user entities. The controls described in this report occur at IDS and cover only a portion of a comprehensive internal controls structure. Each user entity must address the various aspects of internal control that may be unique to its particular system. This section describes the complementary user entity controls that should be developed, placed in operation and maintained at user entities as necessary to meet the trust services criteria stated in the description of IDS' system. The table below identifies the criteria to which the complementary user entity controls relate. User entities should determine whether adequate controls have been established to provide reasonable assurance that:

Complementary User Entity Controls	Most Relevant Criteria
The client is responsible for installing and maintaining the VPN appliance provided by IDS to create secure connections to the Insite Core Banking PaaS system, as well as physically securing the VPN appliance and restricting access to authorized personnel.	CC5.6
Client is responsible for notifying IDS of employment changes.	CC5.2
Client is responsible for periodically reviewing access lists.	CC5.4
Client is responsible for ensuring authentication controls are configured appropriately.	CC5.3
Client is responsible for reviewing admin activity reports supplied weekly and monthly and notifying IDS of suspicious.	CC4.1
Client is responsible for reporting suspected breaches or incidents.	CC4.1

Complementary Subservice Organization Controls

IDS's controls related to the Insite Core Banking Platform-as-a-Service System cover only a portion of overall internal control for each user entity of IDS. It is not feasible for the trust services criteria related to Insite Core Banking Platform-as-a-Service System to be achieved solely by IDS. Therefore, each user entity's internal control must be evaluated in conjunction with IDS's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Complementary Subservice Organization Control	Most Relevant Criteria
Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	CC4.1
Operations and security personnel follow defined protocols for resolving and escalating reported events.	CC4.1
Access to the facility hosting production systems is restricted to personnel or visitors authorized by the tenant.	CC5.5
Access to the facility hosting production systems is not granted to personnel or visitors unless authorized by the tenant previously.	CC5.5
Access to the facility hosting production systems is removed/disabled upon tenant notification.	CC5.5
Access to the facility is controlled via keycard system or other preventative access control systems.	CC5.5
Access to entrances and sensitive areas is monitored and/or recorded by security cameras.	CC5.5
Firewalls have been installed at the data center.	CC5.8
Intrusion detection systems are in place to monitor Web traffic and identify potential patterns or threats.	CC5.8
Identified vulnerabilities in system components are investigated, corrected, and resolved in a timely manner.	CC6.1
Security incidents are tracked, resolved, and communicated to the information security officer in a timely manner.	CC6.1
Environmental controls within the facility and data center are implemented to prevent or mitigate threats to the systems, including: • Cooling systems • Battery and natural gas generator backup in the event of power failure • Redundant communications lines • Smoke detectors • Dry-pipe sprinklers	A1.2

Section 4
Trust Services Principles, Criteria, and Related Controls and Independent Service Auditor's Tests of Controls and Results

Trust Services Principles, Criteria, and Related Controls and Independent Service Auditor's Tests of Controls and Results

Objectives of the Examination

This report is intended to provide user entities of IDS' Insite Core Banking PaaS Insert system with information about IDS' controls pertaining to its Insite Core Banking PaaS system and also to provide user entities with information about the operating effectiveness of the controls that were tested. This report, when combined with an understanding and assessment of the controls in place at user entities, is intended to assist user entities in understanding the controls in place at IDS for the services being outsourced.

In addition, Wipfli's testing of controls was restricted to the principles and related controls listed in this section of the report and was not extended to all controls described in Section 3 or to controls that may be in effect at user entities. It is each interested party's responsibility to evaluate this information in relation to the controls in place at each user entity, and if certain complementary user entity controls are not in place at a user entity, IDS' controls may not compensate for such weaknesses.

The principles and description of controls are the responsibility of IDS' management.

Description of Testing Procedures Performed

As a part of Wipfli's examination of IDS' controls, Wipfli performed a variety of tests, each of which provided the basis for understanding the framework for controls, and determined whether the controls were actually in place and operated effectively in accordance with IDS' description of controls throughout the period August 1, 2017 to July 31, 2018.

Wipfli's tests of the effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, are sufficient to provide reasonable, but not absolute, assurance that the specified criteria were achieved throughout the period August 1, 2017 to July 31, 2018. Wipfli's tests of the operational effectiveness of the controls were designed to cover a representative number of samples throughout the period August 1, 2017 to July 31, 2018, for each of the controls listed in this section, which were designed to achieve the criteria for the specified principles.

In selecting particular tests of operational effectiveness, Wipfli considered:

- The nature of the items being tested.
- The types of available evidential matter.
- The assessed level of control risk.
- The expected efficiency and effectiveness of the test.

Trust Services Principles, Criteria, and Related Controls and Independent Auditor's Tests of Controls and Results

Description of Testing Procedures Performed (Continued)

The procedures performed to test operating effectiveness are listed next to each of IDS' respective control descriptions. Test procedures performed in connection with determining the operating effectiveness of the controls included the following:

Test Procedure	Description of Test Procedure
Corroborative Inquiry	Made inquiries of appropriate organizational personnel to obtain information or corroborating evidence regarding the control descriptions, processes, and procedures. **NOTE:** Because inquiries were performed for all controls, this test was not listed individually for every control activity included in the control testing tables.
Observation	Witnessed the utilization of controls by organization personnel. This included, but was not limited to, viewing the functionality of system applications and automated controls, scheduling routines, and witnessing the processing of transactions.
Inspection	Read documents and reports that contain an indication of performance of the control. This included, but was not limited to, reading documents and reports to determine whether authorization was evidenced and transaction information was properly recorded and controlled and examining reconciliations and evidence of review to determine whether outstanding items were properly monitored, controlled, and resolved.
Reperformance	Independently performed the relevant control. This included, but was not limited to, comparing reconciliations with proper source documents, assessing the reasonableness of reconciling items, and recalculating mathematical solutions.

Results of Testing Performed

Test results are scored as "No exceptions noted," or the exception is noted and described in Section 5.

The following tables describe the tests of operating effectiveness that were performed in meeting the principles noted. The principles, along with the criteria and the control descriptions, are an integral part of management's description of their system. The control descriptions were specified by IDS.

Definition of Security and Availability Principles

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

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

Common Criteria and Related Controls for Security and Availability

CC.1.0 Common Criteria Related to Organization and Management – The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, and qualification of personnel and the environment in which they function

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and requirements as they relate to security and availability.	The senior security engineer and information security officer are responsible and accountable for developing, maintaining, and enforcing IDS' system availability and related security policies. This role is documented in the Information Availability Policy and the Information Security Policy.	Inquired of management to determine whether the senior security engineer and information security officer are responsible and accountable for developing, maintaining and enforcing IDS' system availability and related security policies and whether these roles were documented in the Information Availability Policy and the Information Security Policy.	No exceptions noted.
			Inspected a copy of the Availability Policy and the Information Security Policy to determine whether the roles and responsibilities of the information security officer and senior security engineer were documented.	No exceptions noted.
		Management has documented roles and responsibilities for the design, development, implementation, operation, monitoring, and maintenance of the system through job descriptions.	Inquired of management to determine whether management had documented roles and responsibilities for the design, development, implementation, operation, monitoring, and maintenance of the system through job descriptions.	No exceptions noted.

CC.1.0 Common Criteria Related to Organization and Management (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			For a sample of key systems employees, inspected a copy of their job descriptions to determine whether management had documented roles and responsibilities for the design, development, implementation, operation, monitoring, and maintenance of the system through job descriptions.	No exceptions noted.
		Management has documented reporting lines and responsibilities in an organizational chart that is reviewed and approved by management on an annual basis.	Inquired of management to determine whether management had documented reporting lines and responsibilities in an organizational chart that was reviewed and approved by management on an annual basis.	No exceptions noted.
			Inspected a copy of the organizational chart to determine whether it included documented reporting lines and responsibilities and was reviewed and approved by management on an annual basis.	No exceptions noted.

CC.1.0 Common Criteria Related to Organization and Management (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security and availability.	The senior security engineer and information security officer are responsible and accountable for developing, maintaining, and enforcing IDS' system availability and related security policies. This role is documented in the Information Availability Policy and the Information Security Policy.	Inquired of management to determine whether the senior security engineer and information security officer were responsible and accountable for developing, maintaining, and enforcing IDS' system availability and related security policies, and whether these roles were documented in the Information Availability Policy and the Information Security Policy.	No exceptions noted.
			Inspected a copy of the Availability Policy and the Information Security Policy to determine whether the roles and responsibilities of the information security officer and senior security engineer were documented.	No exceptions noted.
		Management has documented reporting lines and responsibilities in an organizational chart that is reviewed and approved by management on an annual basis.	Inquired of management to determine whether management had documented reporting lines and responsibilities in an organizational chart that was reviewed and approved by management on an annual basis.	No exceptions noted.

CC.1.0 Common Criteria Related to Organization and Management (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			Inspected a copy of the organizational chart to determine whether it included documented reporting lines and responsibilities and was reviewed and approved by management on an annual basis.	No exceptions noted.
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities.	Management has documented roles and responsibilities for the design, development, implementation, operation, monitoring, and maintenance of the system through job descriptions.	Inquired of management to determine whether management had documented roles and responsibilities for the design, development, implementation, operation, monitoring, and maintenance of the system through job descriptions.	No exceptions noted.
			For a sample of key systems employees, inspected a copy of their job descriptions to determine whether management had documented roles and responsibilities for the design, development, implementation, operation, monitoring, and maintenance of the system through job descriptions.	No exceptions noted.

CC.1.0 Common Criteria Related to Organization and Management (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		Annual security awareness training is completed to educate employees on security and availability responsibilities.	Inquired of management to determine whether annual security awareness training was completed to educate employees on security and availability responsibilities.	No exceptions noted.
			For a sample of current employees, inspected training attendance records to determine whether annual security awareness training was attended.	Exception noted: Security awareness training records were not retained for the reporting period.
		Annual performance appraisals of employees are performed.	Inquired of management to determine whether annual performance appraisals of employees were performed.	No exceptions noted.
			For a sample of current employees, inspected performance evaluation documentation to determine whether annual performance reviews were completed.	No exceptions noted.

CC.1.0 Common Criteria Related to Organization and Management (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to security and availability.	Personnel policies, procedures, and code of conduct guidelines are documented in the IDS Employee Handbook. New hires acknowledge receipt of the handbook upon hire.	Inquired of management to determine whether personnel policies, procedures, and code of conduct guidelines were documented in the IDS employee handbook and whether employees acknowledged receipt of the Employee Handbook upon hire.	No exceptions noted.
			For a sample of employees hired within the reporting period, inspected a copy of the policy acknowledgments to determine whether employees reviewed and acknowledged personnel policies upon hire.	No exceptions noted.
		Background checks for new hires are completed prior to employment.	Inquired of management to determine whether background checks were completed for candidates prior to employment.	No exceptions noted.
			For a sample of employees hired within the reporting period, inspected a copy of the background check results to determine whether employees were subject to a background check prior to employment.	No exceptions noted.

CC.1.0 Common Criteria Related to Organization and Management (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		Annual security awareness training is completed to educate employees on security and availability responsibilities.	Inquired of management to determine whether annual security awareness training was completed to educate employees on security and availability responsibilities.	No exceptions noted.
			For a sample of current employees, inspected training attendance records to determine whether annual security awareness training was attended.	Exception noted: Security awareness records were not retained for the reporting period.

CC2.0 – Common Criteria to Related Communications - The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system users to permit users to understand their role in the system and the results of system operation.	A detailed network topology diagram documents the system and its boundaries.	Inquired of management to determine whether management maintained a detailed network topology diagram that documented the system and its boundaries.	No exceptions noted.
			Inspected a copy of the current network topology diagram to determine whether management maintained a current diagram that documented the system and its boundaries.	No exceptions noted.
		The MSA describes the system, operation of the hosted platform environment, responsibilities of both parties, and the technical support available to external users.	Inquired of management to determine whether the MSA described the system, operation of the hosted platform environment, responsibilities of both parties, and the technical support available to external users.	No exceptions noted.
			Inspected a copy of the standard MSA to determine whether it described the system, operation of the hosted platform environment, responsibilities of both parties, and the technical support available to external users.	No exceptions noted.

CC.2.0 Common Criteria to Related Communications (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC2.2	The entity's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities.	IDS communicates security and availability obligations of users and the company's security and availability commitments to users through an MSA.	Inquired of management to determine whether IDS communicated security and availability obligations of users and the company's security and availability commitments to users through an MSA.	No exceptions noted.
			For a sample of new clients, inspected a copy of the signed MSA to determine whether management communicated security and availability commitments to clients using an MSA.	No exceptions noted.
		Personnel policies, procedures, and code of conduct guidelines are documented in the IDS Employee Handbook. New hires acknowledge receipt of the handbook upon hire.	Inquired of management to determine whether personnel policies, procedures, and code of conduct guidelines are documented in the IDS Employee Handbook and whether new hires acknowledge receipt of the handbook upon hire.	No exceptions noted.
			For a sample of employees hired within the reporting period, inspect a copy of the policy acknowledgments to determine whether employees review and acknowledge personnel policies upon hire.	No exceptions noted.

CC.2.0 Common Criteria to Related Communications (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		IDS performs an annual vendor management review to assess the performance and controls of vendors.	Inquired of management to determine whether IDS performed an annual vendor management review to assess the performance and controls of vendors.	No exceptions noted.
			For a sample of critical vendors, inspected documented results from the vendor management reviews to determine whether management completed annual reviews that reassessed the performance and controls of vendors.	No exceptions noted.
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	The senior security engineer and information security officer are responsible and accountable for developing, maintaining and enforcing IDS' system availability and related security policies. This role is documented in the Information Availability Policy and Information Security Policy.	Inquired of management to determine whether the senior security engineer and information security officer were responsible and accountable for developing, maintaining, and enforcing IDS' system availability and related security policies and whether these roles were documented in the Information Availability Policy and the Information Security Policy.	No exceptions noted.

CC.2.0 Common Criteria to Related Communications (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			Inspected a copy of the Availability Policy and the Information Security Policy to determine whether the roles and responsibilities of the information security officer and senior security engineer were documented.	No exceptions noted.
			For a sample of new customers enrolled within the reporting period, inspected a copy of the signed MSA to determine whether management communicates security and availability commitments to customers through the use of an MSA.	No exceptions noted.
		Personnel policies, procedures, and code of conduct guidelines are documented in the IDS Employee Handbook. New hires acknowledge receipt of the handbook upon hire.	Inquired of management to determine whether personnel policies, procedures, and code of conduct guidelines were documented in the IDS Employee Handbook and that employees acknowledged receipt of the handbook upon hire.	No exceptions noted.
			For a sample of employees hired within the reporting period, inspected a copy of the policy acknowledgments to determine whether employees reviewed and acknowledged personnel policies upon hire.	No exceptions noted.

CC.2.0 Common Criteria to Related Communications (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		The MSA describes the system, operation of the hosted platform environment, responsibilities of both parties, and the technical support available to external users.	Inquired of management to determine whether the MSA described the system, operation of the hosted platform environment, responsibilities of both parties, and the technical support available to external users.	No exceptions noted.
			Inspected a copy of the standard MSA to determine whether it described the system, operation of the hosted platform environment, responsibilities of both parties, and the technical support available to external users.	No exceptions noted.
CC2.4	Internal and external personnel with responsibility for designing, developing, implementing, operating, maintaining and monitoring controls, relevant to the security and availability of the system, have the information necessary to carry out those responsibilities.	The senior security engineer and information security officer are responsible and accountable for developing, maintaining and enforcing IDS' system availability and related security policies. This role is documented in the Information Availability Policy and the Information Security Policy.	Inquired of management to determine whether the senior security engineer and information security officer were responsible and accountable for developing, maintaining, and enforcing IDS' system availability and related security policies, and whether these roles were documented in the Information Availability Policy and the Information Security Policy.	No exceptions noted.

CC.2.0 Common Criteria to Related Communications (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			Inspected a copy of the Availability Policy and the Information Security Policy to determine whether the roles and responsibilities of the information security officer and senior security engineer were documented.	No exceptions noted.
		The IT Steering Committee meets quarterly to review security and availability policies, procedures, business activities, performance measures, and system developments.	Inquired of management to determine whether the IT Steering Committee met quarterly to review security and availability policies, procedures, business activities, performance measures, and system developments.	No exceptions noted.
		IDS communicates security and availability obligations of users and the company's security and availability commitments to users through an MSA.	Inquired of management to determine whether IDS communicated security and availability obligations of users and the company's security and availability commitments to users through an MSA.	No exceptions noted.
			For a sample of new clients enrolled within the reporting period, inspected a copy of the signed MSA to determine whether management communicated obligations of the users, and security and availability commitments to clients through the use of an MSA.	No exceptions noted.

CC.2.0 Common Criteria to Related Communications (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC2.5	Internal and external system users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.	The Incident Management Policy documents how to report concerns, availability issues, system security violations, suspected breaches within the organization, and customer notifications.	Inquired of management to determine whether the Incident Management Policy documented how to report concerns, availability issues, system security violations, suspected breaches within the organization, and customer notifications.	No exceptions noted.
			Inspected a copy of the Incident Management Policy to determine whether management had defined a process that included how to report concerns, availability issues, system security violations, suspected breaches within the organization, and customer notifications.	No exceptions noted.
		System security and availability breaches and issues are documented and tracked in a ticketing system and reviewed by the COO.	Inquired of management to determine whether system security and availability breaches and issues were documented and tracked in a ticketing system and reviewed by the COO.	No exceptions noted.

CC.2.0 Common Criteria to Related Communications (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			There were no security and availability issues during the period.	
		The support line for reporting security and availability failures, incidents, concerns, and complaints to IDS is included in the client authentication portal.	Inquired of management to determine whether the support line for reporting security and availability failures, incidents, concerns, and complaints to IDS was included in the client authentication portal.	No exceptions noted.
			Inspected the client authentication portal to determine whether contact information and instructions for reporting security and availability failures, incidents, concerns, and complaints to IDS was included in the customer authentication portal.	No exceptions noted.
		Personnel policies, procedures, and code of conduct guidelines are documented in the IDS Employee Handbook. New hires acknowledge receipt of the handbook upon hire.	Inquired of management to determine whether personnel policies, procedures, and code of conduct guidelines were documented in the IDS Employee Handbook and whether employees acknowledged receipt of the Employee Handbook upon hire.	No exceptions noted.

CC.2.0 Common Criteria to Related Communications (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			For a sample of employees, inspected a copy of the policy acknowledgments to determine whether they reviewed and acknowledged personnel policies upon hire.	No exceptions noted.
CC2.6	System changes that affect internal and external system user responsibilities or the entity's commitments and requirements relevant to security and availability are communicated to those users in a timely manner.	Changes that affect system security and availability commitments are communicated to users who are affected by the change through an email maintenance notification.	Inquired of management to determine whether changes that affect system security and availability commitments were communicated to users who were affected by the change through an email maintenance notification.	No exceptions noted.
			For a sample of changes that affected system security and availability implemented within the period, inspected notifications sent to clients.	No exceptions noted.

CC3.0 – Common Criteria Related to Risk Management and Design and Implementation of Controls - The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks, including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC3.1	The entity (1) identifies potential threats that would impair system security and availability commitments and system requirements (including threats arising from use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system) (2) analyzes the significance of risks associated with the identified threats. (3) determines mitigation strategies for those risks (including implementation of controls, assessments and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies),	IDS management performs an annual risk assessment to identify environmental, regulatory, and technical changes and other potential threats that could impair system security and availability commitments and assesses risk associated with identified threats or changes.	Inquired of the senior security engineer to determine whether IDS management performed an annual risk assessment to identify environmental, regulatory, and technical changes and other potential threats that could impair system security and availability commitments and assessed risk associated with identified threats or changes.	No exceptions noted.
			Inspected a copy of the most recent risk assessment to determine whether it identified environmental, regulatory, and technical changes and other potential threats that could impair system security and availability commitments and that IDS management assessed risk associated with identified threats or changes.	No exceptions noted.

CC3.0 – Common Criteria Related to Risk Management and Design and Implementation of Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
	(4) identifies and assesses changes (for example, environmental, regulatory and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.	The IT Steering Committee meets quarterly to review security and availability policies, procedures, business activities, performance measures, and system developments.	Inquired of management to determine whether the IT Steering Committee met quarterly to review security and availability policies, procedures, business activities, performance measures, and system developments.	No exceptions noted.
		The vulnerability management system is configured to automatically complete external network vulnerability scans of client environments on a quarterly basis.	Inquired of the senior security engineer to determine whether the Qualys tool was configured to automatically complete external network vulnerability scans of client environments on a quarterly basis.	No exceptions noted.
			Inspected a sample of vulnerability scan results to determine whether management configured the scanning tool to perform quarterly automated vulnerability scans of the client environments.	No exceptions noted.
		The vulnerability management system is configured to automatically complete internal network vulnerability scans on the Insite Core Banking PaaS system on a weekly basis.	Inquired of the senior security engineer to determine whether the Qualys tool was configured to automatically complete internal network vulnerability scans on the Insite Core Banking PaaS system on a weekly basis.	No exceptions noted.

CC3.0 – Common Criteria Related to Risk Management and Design and Implementation of Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			Inspected a sample of vulnerability scan results to determine whether scans were automated and performed weekly.	No exceptions noted.
CC3.2	The entity designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and update the controls as necessary.	IDS management performs an annual risk assessment to identify environmental, regulatory, and technical changes and other potential threats that could impair system security and availability commitments and assesses risk associated with identified threats or changes.	Inquired of the senior security engineer to determine whether IDS management performed an annual risk assessment to identify environmental, regulatory, and technical changes and other potential threats that could impair system security and availability commitments and whether IDS management assessed risk associated with identified threats or changes.	No exceptions noted.
			Inspected a copy of the most recent risk assessment to determine whether it identified environmental, regulatory, and technical changes and other potential threats that could impair system security and availability commitments and whether IDS management assessed risk associated with identified threats or changes.	No exceptions noted.

CC3.0 – Common Criteria Related to Risk Management and Design and Implementation of Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		The senior security engineer and information security officer are responsible and accountable for developing, maintaining, and enforcing IDS' system availability and related security policies. This role is documented in the Information Availability Policy and the Information Security Policy.	Inquired of management to determine whether the senior security engineer and information security officer were responsible and accountable for developing, maintaining, and enforcing IDS' system availability and related security policies and that these roles are documented in the Information Availability Policy and the Information Security Policy.	No exceptions noted.
			Inspected a copy of the Availability Policy and the Information Security Policy to determine whether the roles and responsibilities of the information security officer and senior security engineer were documented.	No exceptions noted.
		The vulnerability management system is configured to automatically complete external network vulnerability scans of client environments on a quarterly basis.	Inquired of the senior security engineer to determine whether the Qualys tool was configured to automatically complete external network vulnerability scans of client environments on a quarterly basis.	No exceptions noted.

CC3.0 – Common Criteria Related to Risk Management and Design and Implementation of Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			Inspected a sample of vulnerability scan results to determine whether management configured the scanning tool to perform quarterly automated vulnerability scans of the client environments.	No exceptions noted.
		The vulnerability management system is configured to automatically complete internal network vulnerability scans on the Insite Core Banking PaaS system on a weekly basis.	Inquired of the senior security engineer to determine whether the Qualys tool was configured to automatically complete internal network vulnerability scans on the Insite Core Banking PaaS system on a weekly basis.	No exceptions noted.
			Inspected a sample of vulnerability scan results to determine whether scans were automated and performed weekly.	No exceptions noted.
		Disaster recovery and contingency plans are tested annually, including data restoration exercises.	Inquired of management to determine whether disaster recovery and contingency plans were tested annually, including data restoration exercises.	No exceptions noted.
			Inspected a copy of the most recent disaster recovery and contingency plan test results to determine whether the disaster recovery plan and contingency plan were tested annually.	No exceptions noted.

CC4.0 – Common Criteria Related to Monitoring of Controls - The criteria relevant to how the entity monitors the system, including the suitability, design, and operating effectiveness of the controls, and takes action to address deficiencies identified.

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	The vulnerability management system is configured to automatically complete external network vulnerability scans of client environments on a quarterly basis.	Inquired of the senior security engineer to determine whether the Qualys tool was configured to automatically complete external network vulnerability scans of client environments on a quarterly basis.	No exceptions noted.
			Inspected a sample of vulnerability scan results to determine whether management configured the scanning tool to perform quarterly automated vulnerability scans of the client environments.	No exceptions noted.
		The vulnerability management system is configured to automatically complete internal network vulnerability scans on the Insite Core Banking PaaS system on a weekly basis.	Inquired of the senior security engineer to determine whether the Qualys tool was configured to automatically complete internal network vulnerability scans on the Insite Core Banking PaaS system on a weekly basis.	No exceptions noted.
			Inspected a sample of vulnerability scan results to determine whether scans were automated and performed weekly.	No exceptions noted.

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		IDS management performs an annual risk assessment to identify environmental, regulatory, and technical changes and other potential threats that could impair system security and availability commitments and assesses risk associated with identified threats or changes.	Inquired of the senior security engineer to determine whether IDS management performed an annual risk assessment to identify environmental, regulatory, and technical changes and other potential threats that could impair system security and availability commitments and that IDS management assessed risk associated with identified threats or changes.	No exceptions noted.
			Inspected a copy of the most recent risk assessment to determine whether it identified environmental, regulatory, and technical changes and other potential threats that could impair system security and availability commitments and that IDS management assessed risk associated with identified threats or changes.	No exceptions noted.

CC4.0 – Common Criteria Related to Monitoring of Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		The IT Steering Committee meets quarterly to review security and availability policies, procedures, business activities, performance measures, and system developments.	Inquired of management to determine whether the IT Steering Committee met quarterly to review security and availability policies, procedures, business activities, performance measures, and system developments.	No exceptions noted.
		Disaster recovery and contingency plans are tested annually, including data restoration exercises.	Inquired of management to determine whether disaster recovery and contingency plans were tested annually, including data restoration exercises.	No exceptions noted.
			Inspected a copy of the most recent disaster recovery and contingency plan test results to determine whether the disaster recovery plan and contingency plan were tested annually.	No exceptions noted.

Common Criteria and Related Controls for Security and Availability

CC5.0 – Common Criteria Related to Logical and Physical Access Controls - The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principles of security and availability.

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC5.1	Logical access security software, infrastructure and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability.	Remote access to the production environment requires a unique user ID and two-factor authentication.	Inquired of the senior security engineer to determine whether remote access to the production environment required a unique user ID and two-factor authentication.	No exceptions noted.
			Inspected a configuration from the system to determine whether two-factor authentication was enforced for remote access to the production environment.	No exceptions noted.
			Inspected a listing of users with remote access to the production environment to determine whether unique IDs were assigned.	No exceptions noted.

CC5.0 – Common Criteria Related to Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		A username and password are required to access the production servers. Password settings are configured to require the following: • Minimum length of seven characters • Password complexity enabled • Account lockout threshold of three invalid login attempts • Maximum password age of 42 days • Password history of four prior iterations	Inquired of the senior security engineer to determine whether a username and password were required to access the production servers and whether password settings were configured to enforce complexity requirements.	No exceptions noted.
			Inspected the configuration of in-scope production systems and servers to determine whether complex passwords were enforced.	No exceptions noted.
		TPAM automatically records and logs administrator account activity and usage on the IDS platform. On a monthly basis, IDS sends reports to user organizations, summarizing administrative activity and usage on their respective servers.	Inquired of the senior security engineer to determine whether TPAM automatically recorded and logged administrator account activity and usage on the IDS platform and whether on a monthly basis IDS sent reports to user organizations, summarizing administrative activity and usage on their respective servers.	No exceptions noted.
			Inspected the system configuration to determine whether administrator account activity was logged on the IDS platform.	No exceptions noted.

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			For a sample of customers, inspected reports to determine whether management sent monthly reports summarizing administrative activity on their servers.	No exceptions noted.
		Firewalls managed by IDS at TierPoint are configured to restrict access to predefined IP addresses.	Inquired of the senior security engineer to determine whether firewalls managed by IDS at TierPoint were configured to restrict access to predefined IP addresses.	No exceptions noted.
			Inspected configurations from the IDS firewalls to determine whether access was restricted to predefined IP addresses.	No exceptions noted.
		Clients accessing the platform via the online portal are required to authenticate by username and password.	Inquired of the senior security engineer to determine whether clients accessing the platform via the online portal were required to authenticate by username and password.	No exceptions noted.
			Observed the login process to the online portal to determine whether clients accessing the online portal were required to authenticate by username and password.	No exceptions noted.

CC5.0 – Common Criteria Related to Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		An intrusion detection system monitors production servers at the TierPoint data center and alerts IDS management of unauthorized and/or malicious activity.	Inquired of the senior security engineer to determine whether an intrusion detection system monitored production serves at the TierPoint data center and alerted IDS management of unauthorized and/or malicious activity.	No exceptions noted.
			Inspected the configuration of the intrusion detection system to determine whether servers were configured to alert IDS management of unauthorized and/or malicious activity.	No exceptions noted.
			Observed an alert from the client firewall to determine whether unauthorized and/or malicious activity was noted and sent alerts to management.	No exceptions noted.
		IDS maintains the Security Standards for Network Devices Policy, providing guidance to staff on device hardening requirements.	Inquired of the senior security engineer to determine whether IDS maintained the Security Standards for Network Devices Policy, providing guidance to staff on device hardening requirements.	No exceptions noted.

CC5.0 – Common Criteria Related to Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			Inspected configuration screenshots of a sample of servers deployed to determine whether the servers were hardened based on guidance.	No exceptions noted.
		IDS uses AES 256-bit encryption for the transmission of client information over public networks.	Inquired of the senior security engineer to determine whether IDS used AES 256-bit encryption for the transmission of client information over public networks.	No exceptions noted.
			Inspected the system configuration to determine whether data transmitted over public networks was encrypted using AES 256-bit encryption.	No exceptions noted.
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	New employee system access is approved by IDS management.	Inquired of the senior security engineer to determine whether new employee system access was approved by IDS management.	No exceptions noted.
			For a sample of new employees, inspected system access documentation to determine whether access was approved by IDS management.	No exceptions noted.
		Access to systems is disabled and removed by IT for terminated employees.	Inquired of the senior security engineer to determine whether access to systems was disabled and removed by IT for terminated employees.	No exceptions noted.

CC5.0 – Common Criteria Related to Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			For a sample of terminated employees, inspected system access documentation to determine whether access was disabled and removed.	No exceptions noted.
		Users with the ability to modify security settings, including system security, firewalls, network security devices, and other hardware, are reviewed by management annually to determine that access is restricted to authorized personnel.	Inquired of the senior security engineer to determine whether users with the ability to modify security settings, including system security, firewalls, network security devices, and other hardware, were reviewed by management annually to determine whether access was restricted to authorized personnel.	No exceptions noted.
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software and data) to meet the entity's commitments and system requirements as they relate to security and availability.	A username and password are required to access the production servers. Password settings are configured to require the following: • Minimum length of seven characters • Password complexity enabled • Account lockout threshold of three invalid login attempts • Maximum password age of 42 days • Password history of four prior iterations	Inquired of the senior security engineer to determine whether a username and password were required to access the production servers and whether password settings were configured to enforce complexity requirements.	No exceptions noted.

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			Inspected the configuration of in-scope production systems and servers to determine whether complex passwords were enforced.	No exceptions noted.
		TPAM automatically records and logs administrator account activity and usage on the IDS platform. On a monthly basis, IDS sends reports to user organizations, summarizing administrative activity and usage on their respective servers.	Inquired of the senior security engineer to determine whether TPAM automatically recorded and logged administrator account activity and usage on the IDS platform and whether on a monthly basis IDS sent reports to user organizations, summarizing administrative activity and usage on their respective servers.	No exceptions noted.
			Inspected the system configuration to determine whether administrator account activity was logged on the IDS platform.	No exceptions noted.
			For a sample of customers, inspected evidence to determine whether management sent monthly reports summarizing administrative activity on their servers.	No exceptions noted.
		Clients accessing the platform via the online portal are required to authenticate by username and password.	Inquired of the senior security engineer to determine whether clients accessing the platform via the online portal were required to authenticate by username and password.	No exceptions noted.

CC5.0 – Common Criteria Related to Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			Observed the login process to the online portal to determine whether clients accessing the online portal were required to authenticate by username and password.	No exceptions noted.
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them to meet the entity's commitments and system requirements as they relate to security and availability.	New employee system access is approved by IDS management.	Inquired of the senior security engineer to determine whether new employee system access was approved by IDS management.	No exceptions noted.
			For a sample of new employees, inspected system access documentation to determine whether access was approved by IDS management.	No exceptions noted.
		Access to systems is disabled and removed by IT for terminated employees.	Inquired of the senior security engineer to determine whether access to systems was disabled and removed by IT for terminated employees.	No exceptions noted.
			For a sample of terminated employees, inspected system access documentation to determine whether access was disabled and removed.	No exceptions noted.

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		Users with the ability to modify security settings, including system security, firewalls, network security devices, and other hardware, are reviewed by management annually to determine that access is restricted to authorized personnel.	Inquired of the senior security engineer to determine whether users with the ability to modify security settings, including system security, firewalls, network security devices, and other hardware, were reviewed by management annually to determine whether access was restricted to authorized personnel.	No exceptions noted.
			Inspected a copy of the most recent administrator access reviews to determine whether users with the ability to modify security settings, including system security, firewalls, network security devices, and other hardware, were reviewed by management annually to determine whether access was restricted to authorized personnel.	No exceptions noted.

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		Administrator account activity and usage on the IDS platform is logged via the TPAM tool. On a monthly basis, IDS sends reports to user organizations, summarizing administrative activity and usage on their respective servers.	Inquired of the senior security engineer to determine whether administrator account activity and usage on the IDS platform was logged via the TPAM tool and whether on a monthly basis IDS sent reports to user organizations, summarizing administrative activity and usage on their respective servers.	No exceptions noted.
			For a sample of customers, inspected reports to determine whether management sent monthly reports summarizing administrative activity on their servers.	No exceptions noted.
			Inspected a copy of the most recent administrator access reviews to determine whether users with the ability to modify security settings, including system security, firewalls, network security devices, and other hardware, were reviewed by management annually to determine that access was restricted to authorized personnel.	No exceptions noted.

CC5.0 – Common Criteria Related to Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage and other sensitive locations, as well as sensitive system components, within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and availability.	Physical access for IDS personnel to the colocation data centers is authorized by IDS management.	Inquired of the senior security engineer to determine whether physical access for IDS personnel to the colocation data centers was authorized by IDS management.	No exceptions noted.
			Inspected a listing of users with access to the data centers and determine whether this access was authorized by IDS management.	No exceptions noted.
		Management reviews IDS users with access to the data centers annually for appropriateness. Updates to user access are completed by IT personnel if needed.	Inquired of the senior security engineer to determine whether management reviewed IDS users with access to the data centers annually for appropriateness and whether updates to user access were completed by IT personnel if needed.	No exceptions noted.
			Inspected a copy of the most recent review of data center access to determine whether management performed this access annually.	No exceptions noted.

CC5.0 – Common Criteria Related to Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		Physical access to the colocation data centers is removed for terminated IDS users and tracked in a ticket.	Inquired of the senior security engineer to determine whether physical access to the colocation data centers was removed for terminated IDS users and tracked in a ticket.	No exceptions noted.
			For a sample of terminated employees, inspected data center access lists to determine whether physical access was disabled and removed.	No exceptions noted.
CC5.6	Logical access security measures have been implemented to protect against security and availability threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	IDS maintains the Security Standards for Network Devices Policy providing guidance to staff on device hardening requirements.	Inquired of the senior security engineer to determine whether IDS maintained the Security Standards for Network Devices Policy, providing guidance to staff on device hardening requirements.	No exceptions noted.
			Inspected configuration screenshots of a sample of servers deployed to determine whether the servers were hardened based on guidance.	No exceptions noted.

CC5.0 – Common Criteria Related to Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		IDS uses AES 256-bit encryption for the transmission of client information over public networks.	Inquired of the senior security engineer to determine whether IDS used AES 256-bit encryption for the transmission of client information over public networks.	No exceptions noted.
			Inspected the system configuration to determine whether data transmitted over public networks was encrypted using AES 256-bit encryption.	No exceptions noted.
		Firewalls managed by IDS are configured to restrict access to predefined IP addresses.	Inquired of the senior security engineer to determine whether firewalls managed by IDS were configured to restrict access to predefined IP addresses.	No exceptions noted.
			Inspected configurations from the IDS firewalls to determine whether access was restricted to predefined IP addresses.	No exceptions noted.
		The vulnerability management system is configured to automatically complete external network vulnerability scans of client environments on a quarterly basis.	Inquired of the senior security engineer to determine whether the tool was configured to automatically complete external network vulnerability scans of client environments on a quarterly basis.	No exceptions noted.

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			Inspected a sample of vulnerability scan results to determine whether management configured the scanning tool to perform quarterly automated vulnerability scans of the client environments.	No exceptions noted.
		The vulnerability management system is configured to automatically complete internal network vulnerability scans on the Insite Core Banking PaaS system on a weekly basis.	Inquired of the senior security engineer to determine whether the tool was configured to automatically complete internal network vulnerability scans on the Insite Core Banking PaaS system on a weekly basis.	No exceptions noted.
			Inspected a sample of vulnerability scan results to determine whether scans were automated and performed weekly.	No exceptions noted.
		An intrusion detection system monitors production servers and alerts IDS management of unauthorized and/or malicious activity.	Inquired of the senior security engineer to determine whether an intrusion detection system monitored production servers and alerted IDS management of unauthorized and/or malicious activity.	No exceptions noted.
			Inspected the configuration of the intrusion detection system to determine whether servers were configured to alert IDS management of unauthorized and/or malicious activity.	No exceptions noted.

CC5.0 – Common Criteria Related to Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			Observed an alert from the client firewall to determine whether unauthorized and/or malicious activity generated system alerts and sent the alerts to management.	No exceptions noted.
CC5.7	The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they relate to security and availability.	IDS uses AES 256-bit encryption for the transmission of client information over public networks.	Inquired of the senior security engineer to determine whether IDS used AES 256-bit encryption for the transmission of client information over public networks.	No exceptions noted.
			Inspected the system configuration to determine whether data transmitted over public networks was encrypted using AES 256-bit encryption.	No exceptions noted.
		Users with the ability to modify security settings, including system security, firewalls, network security devices, and other hardware, are reviewed by management annually to determine that access is restricted to authorized personnel.	Inquired of the senior security engineer to determine whether users with the ability to modify security settings, including system security, firewalls, network security devices, and other hardware, were reviewed by management annually to determine whether access was restricted to authorized personnel.	No exceptions noted.

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			Inspected a copy of the most recent administrator access reviews to determine whether users with the ability to modify security settings, including system security, firewalls, network security devices, and other hardware, were reviewed by management annually to determine whether access was restricted to authorized personnel.	No exceptions noted.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security and availability.	Antivirus software and/or antimalware policies are installed on servers and internal workstations and are configured to update virus signatures daily.	Inquired of the senior security engineer to determine whether antivirus software and antimalware policies were installed on servers and internal workstations and were configured to update virus signatures daily.	No exceptions noted.
			For a sample of servers in the environment, observed system configurations to determine whether antivirus software and/or antimalware policies were installed on servers and were configured to update virus signatures daily.	No exceptions noted.

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		An intrusion detection system monitors production servers and alerts IDS management of unauthorized and/or malicious activity.	Inquired of the senior security engineer to determine whether an intrusion detection system monitored production servers and alerted IDS management of unauthorized and/or malicious activity.	No exceptions noted.
			Inspected the configuration of the intrusion detection system to determine whether servers were configured to alert IDS management of unauthorized and/or malicious activity.	No exceptions noted.
			Inspected an alert from the client firewall to determine whether unauthorized and/or malicious activity was noted and generated system alerts and whether it sent the alerts to management.	No exceptions noted.

Common Criteria and Related Controls for Security and Availability

CC6.0 – Common Criteria Related to System Operations - The criteria relevant to how the organization manages the execution of the system procedures and detects and mitigates processing deviation, including logical and physical security deviations, to meet the objectives of the principles of security and availability.

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC6.1	Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters or errors are identified, monitored and evaluated, and countermeasures are designed, implemented and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security and availability.	Procedures for identifying, reporting, and acting on incidents are documented in the Incident Management Policy.	Inquired of the senior security engineer to determine whether procedures for identifying, reporting, and acting on incidents were documented in the Incident Management Policy.	No exceptions noted.
			Inspect a copy of the Incident Management Policy to determine whether it included procedures for identifying, reporting, and acting on incidents.	No exceptions noted.
		The vulnerability management system is configured to automatically complete external network vulnerability scans of client environments on a quarterly basis.	Inquired of the senior security engineer to determine whether the tool was configured to automatically complete external network vulnerability scans of client environments on a quarterly basis.	No exceptions noted.
			Inspected a sample of vulnerability scan results to determine whether management configured the scanning tool to perform quarterly automated vulnerability scans of the client environments.	No exceptions noted.

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		The vulnerability management system is configured to automatically complete internal network vulnerability scans on the Insite Core Banking PaaS system on a weekly basis.	Inquired of the senior security engineer to determine whether the tool was configured to automatically complete internal network vulnerability scans on the Insite Core Banking PaaS system on a weekly basis.	No exceptions noted.
			Inspected a sample of vulnerability scan results to determine whether scans were automated and performed weekly.	No exceptions noted.
		An intrusion detection system monitors production servers and alerts IDS management of unauthorized and/or malicious activity.	Inquired of the senior security engineer to determine whether an intrusion detection system monitored production servers and alerted IDS management of unauthorized and/or malicious activity.	No exceptions noted.
			Inspected the configuration of the intrusion detection system to determine whether servers were configured to alert IDS management of unauthorized and/or malicious activity.	No exceptions noted.
			Observed an alert from the client firewall to determine whether unauthorized and/or malicious activity was noted and generated system alerts and whether is sent the alerts to management.	No exceptions noted.

CC6.0 – Common Criteria Related to System Operations (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		The IT Steering Committee meets quarterly to review security and availability policies, procedures, business activities, performance measures, and system developments.	Inquired of management to determine whether the IT Steering Committee met quarterly to review security and availability policies, procedures, business activities, performance, measures and system developments.	No exceptions noted.
CC6.2	Security and availability incidents, including logical and physical security breaches, failures, concerns, and other complaints, are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures.	Procedures for identifying, reporting, and acting on incidents are documented in the Incident Management Policy.	Inquired of the senior security engineer to determine whether procedures for identifying, reporting, and acting upon incidents were documented in the Incident Management Policy.	No exceptions noted.
			Inspected a copy of the Incident Management Policy to determine whether it included procedures for identifying, reporting, and acting on incidents.	No exceptions noted.
		An intrusion detection system monitors production servers and alerts IDS management of unauthorized and/or malicious activity.	Inquired of the senior security engineer to determine whether an intrusion detection system monitored production servers and alerted IDS management of unauthorized and/or malicious activity.	No exceptions noted.

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			Inspected the configuration of the intrusion detection system to determine whether servers were configured to alert IDS management of unauthorized and/or malicious activity.	No exceptions noted.
			Inspected an alert from the client firewall to determine whether unauthorized and/or malicious activity was noted and generated system alerts and whether it sent the alerts to management.	No exceptions noted.
		System security and availability breaches and issues are documented and tracked in a ticketing system and reviewed by the COO.	Inquired of management to determine whether system security and availability breaches and issues were documented and tracked in a ticketing system and reviewed by the COO.	No exceptions noted.
			Inquired of the senior security engineer to determine whether any security or availability incidents occurred.	No exceptions noted.

CC7.0 – Common Criteria Related to Change Management - The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principles of security and availability.

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC7.1	The entity's commitments and system requirements as they relate to security and availability are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval and maintenance of system components.	Management has a Change Management Policy that defines the requirements for testing, documenting, and authorizing changes to the system.	Inquired of management to determine whether management had a Change Management Policy that defined the requirements for testing, documenting, and authorizing changes to the system.	No exceptions noted.
			Inspected a copy of the Change Management Policy to determine whether management had a Change Management Policy that defined the requirements for testing, documenting, and authorizing changes to the system.	No exceptions noted.
		IDS maintains the Security Standards for Network Devices Policy, providing guidance to staff on device hardening requirements.	Inquired of the senior security engineer to determine whether IDS maintained the Security Standards for Network Devices Policy, providing guidance to staff on device hardening requirements.	No exceptions noted.
			Inspected configuration screenshots of a sample of servers deployed during the testing period to determine whether the server was hardended based on guidance.	No exceptions noted.

CC7.0 – Common Criteria Related to Change Management (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security and availability.	An IT steering Committee that consists of IDS management reviews security and availability policies, procedures, business activities, performance measures, and system developments. Meetings are held quarterly, and minutes are maintained based on results of the discussions.	Inquired of management to determine whether an IT Steering Committee that consisted of IDS management reviewed security and availability policies, procedures, business activities, performance measures, and system developments and that meetings were held quarterly and minutes were maintained based on results of the discussions.	No exceptions noted.
		IDS maintains the Security Standards for Network Devices Policy, providing guidance to staff on device hardening requirements.	Inquired of the senior security engineer to determine whether IDS maintained the Security Standards for Network Devices Policy, providing guidance to staff on device hardening requirements.	No exceptions noted.
			Inspected configuration screenshots of a sample of servers deployed during the testing period to determine whether the servers were hardened based on guidance.	No exceptions noted.

CC7.0 – Common Criteria Related to Change Management (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and availability.	Emergency changes are documented, reviewed, and approved by IDS IT management.	Inquired of management to determine whether emergency changes were documented, reviewed, and approved by IDS IT management.	No exceptions noted.
			For a sample of emergency changes deployed throughout the period, inspected documentation to determine whether changes were documented, reviewed, and approved by IDS IT management.	No exceptions noted.
		High-severity incidents are documented and tracked in the IDS ticketing system. Incidents are reviewed by management, and change requests are prepared for problem resolution if deemed necessary by management.	Inquired of management to determine whether high-severity incidents are documented and tracked in the IDS ticketing system, whether incidents were reviewed by management, and that change requests were prepared for problem resolution if deemed necessary by management.	No exceptions noted.
			For a sample of high-severity incidents that occurred throughout the period, inspected documentation to determine whether the incidents were documented and reviewed by management and whether change requests were created as necessary.	No exceptions noted.

CC7.0 – Common Criteria Related to Change Management (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC7.4	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and availability.	System changes, including operating system, software, and infrastructure updates, are documented on change request forms, subject to testing by operations personnel, and approved prior to implementation to production.	Inquired of management to determine whether system changes, including operating system, software, and infrastructure updates, were documented on change request forms, subject to testing by operations personnel, and approved prior to implementation to production.	No exceptions noted.
			For a sample of system changes that were made throughout the period, inspected change documentation to determine whether the changes were documented on change request forms, subject to testing by operations personnel, and approved prior to implementation to production.	No exceptions noted.

Additional Criteria and Related Controls for Availability

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.	Automated tools have been implemented to monitor the system availability, storage capacity, and uptime. Alerts are generated and sent to operations personnel when activities exceed predefined thresholds.	Inquired of the senior security engineer to determine whether automated tools had been implemented to monitor the system availability, storage capacity, and uptime and whether alerts were generated and sent to operations personnel when activities exceeded predefined thresholds.	No exceptions noted.
			Observed the configuration from the system to determine whether automated tools had been implemented to monitor the system availability, storage capacity, and uptime and whether alerts were generated and sent to operations personnel when activities exceeded predefined thresholds.	No exceptions noted.
A1.2	Environmental protections, software, data backup processes and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained and monitored to meet the entity's availability commitments and system requirements.	Management has defined data backup requirements for client-hosted data in the Backup Policy. Backups are performed in accordance with the Backup Policy.	Inquired of the senior security engineer to determine whether management had defined data backup requirements for client-hosted data in the Backup Policy and whether backups were performed in accordance with the Backup Policy.	No exceptions noted.
			Inspected a copy of the Backup Policy to determine whether management had defined data backup requirements for client-hosted data.	No exceptions noted.

Additional Criteria and Related Controls for Availability

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			For a sample of dates, inspected backup job logs and results to determine whether backups were completed in accordance with the Backup Policy.	No exceptions noted.
		The backup tool is configured to retain completed application and server data backups for restoration.	Inquired of the senior security engineer to determine whether the backup tool was configured to retain completed application and server data backups for restoration.	No exceptions noted.
			Inspected system configurations to determine whether the backup tool was configured to retain application and server backups.	No exceptions noted.
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	Disaster recovery and contingency plans are tested annually, including data restoration exercises.	Inquired of management to determine whether disaster recovery and contingency plans were tested annually, including data restoration exercises.	No exceptions noted.
			Inspected a copy of the most recent disaster recovery and contingency plan test results to determine whether the disaster recovery plan and contingency plan were tested annually.	No exceptions noted.

Additional Criteria and Related Controls for Availability

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		IDS performs data recovery tests of client-hosted data and communicates the results for customers who submit a request to IDS.	Inquired of the senior security engineer to determine whether IDS performed data recovery tests of client-hosted data and communicated the results for customers who submitted a request to IDS.	No exceptions noted.
			For a sample of requested data restorations, inspected ticket documentation to determine whether management performed the restoration and communicated the results to the client.	No exceptions noted.

Section 5
Other Information Provided by Insite Data Services

Other Information Provided by Insite Data Services

Management's Responses to Exceptions Noted During Testing of Controls

The information included below describes the management responses provided by Insite Data Services in response to the control findings identified in Section 4 of this report. It is presented by the management of Insite Data Services to provide additional information and is not a part of Insite Data Services' description of its Insite Core Banking PaaS made available to user entities throughout the period August 1, 2017 to July 31, 2018. The information provided in the management responses has not been subjected to the procedures applied in the examination of the description of the Insite Core Banking PaaS and the suitability of the design and operating effectiveness of controls to meet the trust services principles criteria stated in the description of the Insite Core Banking PaaS system, and accordingly Wipfli LLP expresses no opinion on it.

Exception Noted: CC1.3 and 1.4 - Security awareness training records were not retained for the reporting period.

Management Response: Security awareness and general security training is scheduled and held by the IDS team every two weeks. The documentation of the trainings held and who attends them has been improved to ensure tracking of attendance and information coverage. The tracking is completed through the use of email confirmations of attendance which are added to tracking within the Jira ticketing system. The process has been detailed in the updated information security policy.