Insite Data Services, Inc.
Lincoln, Nebraska

System and Organization Controls Report Relevant to Security and Availability

SOC 3® Report

August 1, 2017 to July 31, 2018

WIPFLi LLP
CPAs and Consultants

Insite Data Services, Inc.

SOC 3 Report
August 1, 2017 to July 31, 2018

Table of Contents

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

Insite Data Services, Inc.’s Assertion on Controls

Management of Insite Data Services, Inc.’s (IDS) assertion regarding the effectiveness of its controls over IDS’s Insite Core Banking Platform-as-a-Service System (the “System”) for its domestic operations in United States locations based on the trust services security and availability criteria.

IDS maintained effective controls over the security and availability of the System to provide reasonable assurance that:

- The System was protected against unauthorized access, use, or modification, and
- The System was available for operation and use to meet the entity's commitments and system requirements

to meet IDS’s commitments and system requirements during the period of August 1, 2017 to July 31, 2018, based on the American Institute of Certified Public Accountants’ (AICPA) Trust Services Criteria for security and confidentiality, which are available at www.aicpa.org.

The attached description of IDS’s System summarizes those aspects of the System covered by our assertion.

Section 2
Independent Service Auditor's Trust Services Report

WIPFLi LLP

Independent Service Auditor's Trust Services Report

Scope
We have examined management's assertion that during the period August 1, 2017 to July 31, 2018, Insite Data Services, Inc.(IDS) maintained effective controls over its Core Banking Platform-as-a-Service System based on the AICPA trust services security and availability criteria to provide reasonable assurance to meet IDS's commitments and system requirements that:

- The system was protected against unauthorized access, use, or modification.
- The system was available for operation and use to meet the entity's commitments and system requirements

IDS's management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the system covered by its assertion is attached. We did not examine this description, and accordingly we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of IDS's relevant controls over the security and availability of the system, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Inherent Limitations
Due to the nature and inherent limitations of controls, IDS's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion
In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on the AICPA trust services security and confidentiality criteria.

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, Inc.

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 Insite 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 Insite 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 Insite Core Banking System and other applications. This hosted platform is known as the Insite 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 Insite 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 Insite 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's 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. (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. (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 Insite 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.

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's security and availability commitments. Other key individuals responsible for the daily operations of IDS are the system administrator, network technicians, and 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
Sharon Tate	Network Technician
Ben Roberts	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.

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.

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

People (Continued)

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.

IT Information Technology Security Policy

IDS has implemented an IT Security Policy. Security policies and guidelines are documented and communicated throughout the organization. IDS's 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
- Establishment of network connections
- Encryption
- Firewall maintenance and monitoring
- Logging and monitoring
- Third-party access and outsourced services
- Third-party information disclosure
- Privacy
- Change management
- Reporting of a problem
- Incident response

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.

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

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's 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.

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.

Relevant Aspects of Internal Control

Risk Assessment Process (Continued)

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, 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 enterprise-class servers to create a hosted platform to run applications that support core processing.

Employee Communications

IDS's 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's 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 for 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.

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.

Relevant Aspects of Internal Control (Continued)

Information and Communication Systems (Continued)

Employee Communications (Continued)

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's 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 of August 1, 2017, to July 31, 2018, there were no changes to IDS's security and availability commitments or requirements.

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 critical 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.

Relevant Aspects of Internal Control (Continued)

Monitoring Controls (Continued)

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 has documented the process in the Incident Management Policy. IDS's 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 for IDS's customers using ATM services. TierPoint provides colocation services for IDS's non-ATM 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 of 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.

Relevant Aspects of Internal Control (Continued)

Controls Related to the Common Criteria (Continued)

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 that meet IDS-defined authentication controls. For clients that have requested audit logs of administrator activity on their platform, audit logs are posted to the client's customer portal or emailed to the client monthly. 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 strong authentication credentials. Accounts are set to lock out after a period of inactivity and 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. Passwords 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 TierPoint. 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's Operations personnel. IDS has a firewall in place to restrict the traffic permitted from the Internet to the platform based on previously authorized or whitelisted IP addresses. The system security engineer is responsible for maintaining the firewall rulesets.

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 IDs 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 that 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.

Relevant Aspects of Internal Control (Continued)

Controls Related to the Common Criteria (Continued)

Logical Access (Continued)

External User Access

To securely connect to the Insite 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 Insite Core Banking PaaS System, clients may 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.

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 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, including changes made by customer administrators, are automatically logged by the ticketing system.

Relevant Aspects of Internal Control (Continued)

Controls Related to the Common Criteria (Continued)

Change Management (Continued)

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 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 lnsite 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 backup tool is configured to perform one full backup upon initial setup and daily incremental backups thereafter. The backup data is replicated between the data centers. Full backups are kept for 30 days.

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 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 for non-ATM customers. It maintains physical and environmental security controls over the data center, monitors and administers the intrusion detection system (IDS), provides distributed denial-of-service (DDoS) mitigation, and conducts 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 administers the IDS, provides distributed DDoS mitigation, and conducts load balancing for the servers hosted at its data center.
ASI	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.