IDS™ | Asset Finance Technology

International Decision Systems, Inc.
Minneapolis, Minnesota

System and Organization Controls Report on the Description of the IDScloud Solution Services

Controls Placed in Operation Relevant to Security, Availability, and Confidentiality

SOC 3® Report

August 1, 2019 to October 31, 2019

WIPFLi LLP
CPAs and Consultants

This report is not to be copied or reproduced in any manner without the express written approval of International Decision Systems, Inc. and Wipfli LLP. The report, including the title page, table of contents, and sections, constitutes the entire report and should be referred to only in its entirety and not by its component parts. The report contains proprietary information and is considered confidential.

International Decision Systems, Inc.

System and Organization Controls Report Relevant to Security, Availability, and Confidentiality on the Description of the IDScloud Solution Services
August 1, 2019 to October 31, 2019

Table of Contents

Section 1
International Decision Systems, Inc.'s Assertion on Controls

IDS™ | Asset Finance Technology

International Decision Systems, Inc.'s Assertion on Controls

We are responsible for designing, implementing, operating, and maintaining effective controls within International Decision Systems, Inc.'s system throughout the period August 1, 2019 to October 31, 2019, to provide reasonable assurance that International Decision Systems, Inc.'s service commitments and system requirements relevant to security, availability, and Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period August 1, 2019 to October 31, 2019, to provide reasonable assurance that International Decision Systems, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (the "applicable trust services criteria") set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. International Decision Systems, Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period August 1, 2019 to October 31, 2019, to provide reasonable assurance that International Decision Systems, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Section 2
Independent Service Auditor's Report

Independent Service Auditor’s Report

Management of International Decision Systems, Inc.
Minneapolis, Minnesota

Scope

We have examined International Decision Systems, Inc.’s accompanying assertion titled "International Decision Systems, Inc.’s Assertion on Controls" (the “assertion”) that the controls within International Decision Systems, Inc.’s system were effective throughout the period August 1, 2019 to October 31, 2019, to provide reasonable assurance that International Decision Systems, Inc.’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (the “applicable trust services criteria”) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Service Organization's Responsibilities

International Decision Systems, Inc. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that International Decision Systems, Inc.’s service commitments and system requirements were achieved. International Decision Systems, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, International Decision Systems, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management’s assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization’s service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve International Decision Systems, Inc.’s service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve International Decision Systems, Inc.’s service commitments and system requirements based the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independent Service Auditor’s Report (Continued)

Inherent Limitations

There are inherent limitations in the effectiveness in any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization ‘s service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusion about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies and procedures may deteriorate.

Opinion

In our opinion, management’s assertion that the controls within International Decision Systems, Inc.’s system were effective throughout the period August 1, 2019 to October 31, 2019, to provide reasonable assurance that International Decision Systems, Inc.’s service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated, in all material respects.

Wipfli LLP

Wipfli LLP

Minneapolis, Minnesota
December 6, 2019

Attachment A
Description of International Decision Systems, Inc.'s System

Description of International Decision Systems, Inc.'s System

Company Overview

Nature of Business

IDS is a global provider of software and solutions for the asset and equipment finance industry. For over 40 years, IDS has partnered with banks and independent and captive finance organizations of all sizes to provide the underlying software platform to enable customers to build their business. IDS has worked with financial institutions in over 30 countries.

The IDS origination and portfolio management solutions include products designed to help meet customer's asset finance needs. This includes an extensible architecture that integrates into customer business processes and connects to third-party resources as needed. IDS is committed to ongoing investment in its asset finance solution, which helps ensure customers benefit from IDS's knowledge of the collective best practices across industry-leading financing organizations.

Headquartered in Minneapolis, Minnesota, the company also has offices in the United Kingdom, Australia, Singapore, and India.

The IDS location covered in this report includes teams located in Minneapolis, Minnesota, USA.

Product Overview

IDScloud solution (IDScloud) is an asset and equipment finance solution based on IDS's origination, financing, and portfolio management solutions. IDScloud delivers the same leasing and lending engine used by on-premise equipment and asset financing firms through a 100% software-as-a-service (SaaS) model, making it accessible to any size financing firm. IDScloud is packaged to deliver a foundation of core functionality with the ability to add advanced features as customer's business needs evolve. The base configuration is functionally rich and highly configurable, which enables customers to align IDScloud with their business processes. IDScloud is built to be extensible and easily integrate with other third-party software providers. This includes functionality such as e-signature, credit decisioning, customer relationship management (CRM), and enterprise resource planning (ERP) solutions. IDScloud provides flexibility of both cost and functionality needed to deliver an end-to-end solution to any equipment finance company.

Leveraging the strengths and global reach of Amazon Web Services (AWS), IDScloud prioritizes security and is a highly resilient platform available in multiple regions around the world including the United States, Europe, Asia, and Australia. With a composable application programming interface (API)-driven architecture, IDScloud is designed to help ensure scalability of the platform as customers' businesses grow.

The scope of services covered in this report is IDScloud.

IDS's services are hosted in AWS data centers in the United States and Australia.

IDS's colocation data center is in Minnesota.

Additional global locations are deployed based on customer requirements.

Description of International Decision Systems, Inc.’s System

Relevant Aspects of Internal Control

Control Environment

IDS’s organizational structure provides a framework for its control environment, starting at the highest level of IDS. The Board of Directors (BOD) meets on a quarterly basis and provides oversight of management in the establishment and monitoring of company goals, strategic direction, and operational results. Members of the BOD actively oversee security, availability, processing integrity, confidentiality, and privacy initiatives, and management considers requirements relevant to each of these areas when defining authorities and responsibilities.

IDS, through its BOD and executive management, considers the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.

The members of IDS’s executive management team includes:

- Chief Executive Officer (CEO)
- Chief Financial Officer (CFO)
- Chief Operating Officer (COO)
- Chief Technology Officer (CTO)
- VP, Sales
- VP, Marketing
- VP, Human Resources
- Managing Director, APAC

IDS’s organizational structure provides the foundation for planning, executing, monitoring, and achieving IDS’s objectives.

IDS uses various tools to delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility as necessary across the various levels of the organization.

Executive management approves and distributes a delegations of authority document that defines and limits signature and expenditure authority. Within various departments, segregation of duties is mandated and managed by the applicable department leader.

The BOD routinely evaluates changes and proposed changes to key departmental organizational structures and related required skill sets.

Executive management and the BOD establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary. Executive management communicates its objectives by publishing of policies and procedures on IDS’s intranet as well as through ongoing compensation and training. IDS monitors employee’s adherence to its policies and provides its employees with a means to report behavior that does not conform with IDS’s policies and procedures.

Integrity and Ethical Values

IDS is committed to conducting its business according to ethical and legal standards. IDS expects its officers, directors, employees, contractors, and service providers to follow ethical standards, use sound business judgment, and avoid conflicts of interest.

Relevant Aspects of Internal Control (Continued)

Control Environment (Continued)

Integrity and Ethical Values (Continued)
The expectations of the BOD and executive management concerning integrity and ethical values are defined in IDS's published Business Ethics Policy and are understood across the entity and by appropriate third parties. The Business Ethics Policy is reviewed and updated annually by IDS's Legal department and presented to and approved by the BOD. Employees are required to read and accept the Business Ethics Policy.

IDScloud Team Organization and Management
The lead product manager serves as the IDScloud initiative leader. This role is responsible for the overall IDScloud program across a number of workstreams including service proposition, technology, client onboarding, client support, and program financials. A dedicated IDScloud team has been formed to architect and build the infrastructure, onboard and implement clients, and provide ongoing support of the application and infrastructure, including providing automation and self-service options wherever possible.

The IDScloud team meets routinely to plan, check status, and discuss and assign tasks to meet other nondevelopment related company objectives.

Strategic Plan
IDS's strategic plan, which is developed by the BOD and executive management, focuses on developing the core business, presenting products, and understanding market challenges related to asset leasing. Annually, management reviews and develops plans and resources to meet strategic goals. Relevant segments of these goals are assigned to appropriate departments, with the leaders of those departments held responsible for implementation of these goals.

IDScloud Human Resources Governance and Oversight
Human resources (HR), in cooperation with the legal department, maintains and annually reviews and modifies employee-related policies and procedures as needed. Policy training is delivered and tracked using the HR information system (HRIS), Cornerstone.

New Hire Process
When a manager wants to hire a new employee for the IDScloud team (net new headcount or replacement), the manager follows a process to obtain approval to post the position. Once approved, the recruiter meets with the manager to agree to a hiring strategy (job description, interview panel, potential sources of talent, etc.). A compensation range for the position is established based on market data.

After the position is posted, the recruiter reviews applicants and shares top candidates with the hiring manager for consideration. Preferred candidates are interviewed, and a top candidate is selected. Once the top candidate is selected, references are checked, and HR works with the hiring manager to determine the offer package. The offer proposal is shared with the global HR lead and the senior director of finance and ultimately the COO for approval.

Relevant Aspects of Internal Control (Continued)

Control Environment (Continued)

New Hire Process (Continued)
After the offer is approved, delivered, and accepted, IDS may order a background check to verify previous employment experience, education credentials, and criminal activity. Next, a start date and onboarding plan are established. Technology provisioning and policy communication are included in each employee’s onboarding.

After a new employee joins IDS, HR checks in with the employee after 30 and 90 days to hear feedback and help ensure the new hire is successful and that the firm and the role are as expected. Feedback is shared with managers as appropriate.

Performance Management
Each year, IDS’s executive team establishes company goals and a budget, which are approved by the IDS BOD. This information is used to guide team and individual goals deeper in the organization. Employee performance is measured against these goals, and feedback is shared throughout the year (i.e., manager and employee meetings, customer feedback, dashboards and reporting, annual performance review).

Training and Professional Development
Managers organize onboarding plans for new employees that include department overviews and training plans. IDS provides tuition assistance for both ongoing education and certification. In some cases, IDS hires experts or professional coaches for training of employees, such as agile training and secure coding training.

Risk Assessment
IDS policies set forth the Company’s approach to risk management, outline the risk management process, and identify reporting procedures. In addition, they describe the relationship between management, the teams, and the committees designed to mitigate risk and the BOD.

IDS’s approach to managing risk is to (i) protect IDS from those risks of significant likelihood and consequence in the pursuit of its stated strategic goals and objectives; (ii) provide a consistent risk management framework in which the risks concerning business processes and functions are identified, considered, and addressed; (iii) encourage proactive rather than reactive management; (iv) provide assistance to and improve the quality of decision making throughout IDS; and (v) assist in safeguarding IDS’s assets, employees, customers, and reputation.

IDS’s approach includes the following activities:

- **Policies and procedures:** IDS’s policies and procedures are designed to help mitigate risk. Risks associated with vendors are generally classified and managed through the Vendor Management Policy, risks associated with IT infrastructure are managed through the Security Policy, risks associated with catastrophic events are managed through the Business Continuity Plan, and so forth.
- **Business impact analysis:** IT maintains a master systems inventory through an annual business impact analysis of systems used by IDS. At least once annually, a business impact analysis is completed and/or updated by each systems owner. This includes rating the technology impact, financial impact, legal impact, and recovery time objectives of the system.

Relevant Aspects of Internal Control (Continued)

Control Environment (Continued)

Risk Assessment (Continued)

- **Employee responsibility:** IDS employees understand IDS's policies and procedures as they apply to the individual employee's role. Through IDS's employees and management team, individual departments monitor risk at a departmental level.
- **Management of risk through escalation channels:** Operations personnel follow defined protocols for resolving and escalating reported events. This includes performing a root-cause analysis that is escalated to management if required. Defined groups and committees meet on a regular and/or ad hoc basis to consider the potential significance of the risks that have been escalated, including:
  - Determining the criticality of identified assets in meeting objectives.
  - Assessing the impact of identified threats and vulnerabilities in meeting objectives.
  - Assessing the likelihood of identified threats.
  - Determining the risk associated with assets based on asset criticality, threat impact, and likelihood.
- **Review and monitoring of contracts:** The legal department reviews contracts to help limit IDS's risk exposure. Contracts with third parties are monitored by the legal department and/or applicable business owner, and performance is communicated to relevant parties.

Information and Communication

IDS has internal lines of communication to collect, process, and distribute important information in a timely manner.

The method of communication considers the timing, audience, and nature of the information. IDS communicates information to customers using several different methods, including the following:

- Through its support website
- Through direct email
- Through reports generated from the system

Information may be directed to a specific individual based on role or distributed as a general announcement to a group of individuals.

Internal
IDS obtains or generates and uses relevant, quality information to support the functioning of internal controls. Internal communications consider the affected employees, nature of the information, and urgency of the communication. Employee communication is a continual, iterative process. IDS internally uses various applications to process data. IDS communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal controls.

Management communicates objectives to department leaders, and department leaders communicate specific employee responsibilities. Information also flows from the employee base to management and is recorded by management.

Relevant Aspects of Internal Control (Continued)

Information and Communication (Continued)

Internal (Continued)
Periodically, IDS conducts employee “all-hands” meetings, which are attended by employees at every location in person or via teleconference. The meeting is led by the CEO or other IDS leaders. The CEO uses this meeting to communicate company projects, events, and changes. Employees have the opportunity to ask questions at the meeting.

External
At the customer level, IDS has developed mechanisms enabling the IDScloud operations and support teams to be notified and, in turn, notify customers of potential operational issues that impact the customer experience. These mechanisms are derived from information systems that are designed to produce information which is timely, current, accurate, complete, accessible, protected, verifiable, and retained. IDS personnel are provided with information on how to report systems failures, incidents, concerns, and other complaints to personnel. IDS personnel and customers report internal computing and other cloud-related infrastructure issues by logging a ticket in the incident management tracking system.

IDS has a Product Vulnerability Management Policy that uses an industry-standard mechanism for measuring product vulnerabilities and delivers a process for communicating the characteristics and impact of IT vulnerabilities in its software products.

Technical documentation is available on IDS’s customer-facing website for external users and describes and explains how to use the solution. Customers are responsible for reporting operational failures, incidents, problems, concerns, and complaints, which may be reported to IDS’s support team via telephone or through IDS’s incident management system. The process for reporting issues is described on the customer-facing website and in system documentation. Suppliers, external auditors, regulators, and financial analysts may report findings to the relevant department with which they are transacting. Material issues are raised via the Risk Management Policy.

Use and Monitoring of Subservice Providers

IDScloud data centers are located in the AWS cloud. IDScloud solution runs actively at these sites at times. IDScloud’s infrastructure is designed to scale to accommodate foreseeable growth with existing and potential customers, including availability, data throughput, and data retention.

AWS regions are hosted across dedicated geographical regions as depicted in the AWS region mappings. Each AWS region acts as a standalone data center. IDScloud AWS infrastructure is designed for efficient disaster recovery, with each data center acting as a failover. The IDScloud solution uses monitoring tools for servers and applications hosted in AWS that send alerts to IDS for resolution. IDScloud AWS logs are also collected in a centralized server located in a dedicated, secure server.

The IDS corporate network is connected to the AWS cloud through an encrypted virtual private network (VPN) tunnel. IDS uses dedicated, secured, and isolated virtual desktop instances (VDI) to interface with the AWS solution. These VDIs are then used to remotely connect to parts of the IDScloud solution on AWS based on role, responsibility, and rights. Sessions on these VDIs are captured and stored in AWS. Potential sensitive data transmitted and processed between the VDIs and AWS is encrypted to help protect against third-party disclosure in transit.

Relevant Aspects of Internal Control (Continued)

Use and Monitoring of Subservice Providers (Continued)

IDScloud uses HEAT by Ivanti as a hosted customer support tool. Ivanti also hosts in AWS utilizing a similar architecture design for resiliency.

Both AWS and Ivanti are reviewed as part of the Vendor Management Policy, and IDS retains copies of both companies' current SOC 2 Type 2 reports.

Control Activities

Policies and Procedures
IDS's policies and procedures standardize key control elements and communicate control requirements to IDS employees. Policies and procedures are updated regularly by the policy owner and are made available to employees through IDS's intranet.

Security Awareness Training
IDS helps ensure its employees are aware of security risks and the associated policies and procedures through various mechanisms.

Employment Termination
IDS operates as an at-will employer, and employment can be terminated by IDS at any time for lawful reasons. Employee terminations can be voluntary or involuntary. Involuntary terminations require documentation of issues and require approval from the IDS risk committee.

Access is revoked when an employee's employee record is changed to termination in the IDS HR system. This change generates an automatic notification to the IT department triggering the IT department to remove and manually review access to systems for that employee.

Network Security
Servers and network components are secured with access control mechanisms and protected by hardened industry-standard security and intrusion detection systems. These systems are monitored and receive updates from product vendors to address system vulnerabilities. Systems are updated in a timely manner if required to address reported vulnerabilities.

IDS's network has been designed using a meshed topology and redundancy within IDS offices to help eliminate a single point of failure that could interrupt access to IDS's VDIs and IDScloud AWS solution.

IDScloud uses AWS's virtual private cloud (VPC) and virtual subnets (VLAN) to segment the network and associated customer environments from other customers, development, and user acceptance training environments.

Physical Access
An identification (ID) card-based physical access control system has been implemented at IDS's facility entry and exit points. Privileged access to the sensitive areas where in-house IDS systems are housed is monitored by cameras and restricted by ID card controls. A review of physical access cards is performed annually.

Relevant Aspects of Internal Control (Continued)

Control Activities (Continued)

Policies and Procedures (Continued)

Remote Access

IDS employees access the internal system and the designated IDScloud VDI environments through an encrypted VPN and an encrypted VMware connection. These connections terminate through a VPN device and security server requiring a username and password for authentication. IDS requires two-factor authentication on these connections.

Wireless Security

IDS has wireless services within IDS, but they do not connect directly with IDS's resources. The wireless network is secured with WPA2 technology, and connected assets are controlled through a zone director dashboard. Separate and segmented guest wireless is provided to IDS visitors and for IDS personal employee devices.

Antivirus

IDS employee workstations and IDScloud servers have an industry-standard antivirus solution deployed. This antivirus solution is centrally managed and has real-time updates on virus definitions deployed. Alerts on potential infections are sent via email and SMS text messages to the IT team and appropriate security personnel.

Security Groups

External communication to cloud instances is protected using AWS security groups. This network access is controlled on a per-device level with a least-privilege access model and using defined traffic and allow ports. IDS's corporate network is connected to AWS regions via secure VPN tunnels.

Intrusion Detection

Suspicious activity triggers alerts that are sent to responsible security staff via email, monitoring systems, and SMS text messages. The responding individual(s) investigate the alerts, and if qualifying conditions are met, a security incident is recorded.

System and Performance Monitoring

IDScloud uses an automated monitoring system that provides a high level of service performance and availability. Monitoring activities are intended to identify and remediate areas of strategic, financial, operational, and/or legal risk. AWS log tools are used in conjunction with centralized monitoring of the server and applications.   These tools are designed to monitor servers and application performance, application traffic, and anomaly detection.

IDScloud personnel are responsible for following defined protocol for reporting incidents. IDScloud leverages the HEAT by Ivanti system, which maintains records of incidents. Communication that requires the customer's acknowledgement is managed through IDS personnel. IDS personnel also communicate with the customer regarding issue resolution, and if the issue impacts multiple customers, the root-cause analysis is conveyed via email.

Vulnerability Assessments and Penetration Testing

IDScloud-based systems use recognized AWS security competency solutions to run in AWS and scan AWS instances to detect vulnerabilities, malware, and compliance issues. Identified vulnerabilities are recorded and addressed by IDScloud team members in accordance with company policies and procedures.

Relevant Aspects of Internal Control (Continued)

Control Activities (Continued)

Policies and Procedures (Continued)

System Passwords

Users are required to enter a user ID and password to access the IDS and IDScloud networks and application. Complexity standards for passwords have been established to help enforce control. Password expiration is established, and account lockout after failed attempts occurs. Password sharing is prohibited.

Access Reviews

Customer implementation project managers are responsible for notifying the IT Service Desk via email that access for IDS project team members can be eliminated as a project closeout step. Accounts are reviewed quarterly for IDScloud access, and renewed approval is required from the IDScloud manager.

Software Development Life Cycle

IDS has adopted an Agile software development life cycle (SDLC) as its standard development methodology. The intent is to promote agility using a practical, flexible approach to deliver maximum value to IDS customers. This includes the development of customer applications on IDScloud. Procedures for this process are available for employees on IDS’s corporate intranet site.

IDScloud Change Management Policy

IDS requires changes to be managed in a rational and predictable manner so employees, contractors, customers, and vendors can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce any negative impact to information users and to increase the value of information systems and tools.

IDScloud Change Control

Procedures and controls have been established to manage changes to infrastructure facilities and systems, in advance of any change, to ensure satisfactory control of changes to systems, networks, equipment, software, or processes. Complete documentation of changes is required. This includes snapshots of the environment prior to the change and after the change.

Standalone test or development systems that have no possibility of affecting production systems are not subject to the change management process.

IDScloud Engineering Change Process

The engineering process for the IDScloud solution follows industry-standard code development processes. Using defined workflow controls, IDScloud implements and tracks changes to the IDScloud solution. To help ensure controls work, IDS uses the following features:

- Status checks – Status checks are available in IDS’s development system to record code input and modifications to such code.
- Protected branches – IDS does not allow “commits” directly into the master branch, and mergers do not occur until the required status checks pass on it.

Relevant Aspects of Internal Control (Continued)

Control Activities (Continued)

Policies and Procedures (Continued)
Outage Notifications
The customer agreement sets forth IDS's responsibility for providing notifications for system outages or downtime. Regularly scheduled maintenance time is planned for Wednesday evenings (CST) as outlined in the IDScloud engagement guide. Client communications with details on production updates typically are sent on the Monday prior to the Wednesday deployment. In addition, the SaaS agreement provides notice for a time period each week that is specifically reserved for routine scheduled maintenance as needed.

Client Implementation
For customer implementations, the customer and IDS mutually execute a statement of work that describes the scope of the implementation project, assumptions, parties' obligations, tasks, and fees. This statement of work is subject to a master services agreement signed by IDS and the customer that sets forth the terms and conditions governing the services engagement. The master services agreement defines:

- What constitutes confidential information.
- For what purpose confidential information may be used.
- To whom and under what conditions confidential information may be provided.
- The standard of care utilized to protect the confidential information.

Data upload or conversion activities are done on AWS's conversion environment provided to the customer by the IDScloud team. Members of the IDScloud implementation team prepare the data within the AWS conversion environment for production use. Once complete, the data is moved to the production environment in AWS, and the conversion environment is destroyed.

IDScloud Services Availability
IDS uses commercially reasonable efforts to make production environments available at least 99.5% of the time during each calendar quarter (excluding planned maintenance outages). IDS measures the percentage of time the services are available and provides for service level credits should it fail to meet its commitment.

Compromise of Customer Data
If IDS becomes aware that the security of customer data, including personal data, has been compromised, or that customer data has been or is reasonably expected to be subject to a use or disclosure not authorized by the SaaS agreement, IDS will:

- Promptly (and in any event within 48 hours of becoming aware of such data security incident) notify the customer, in writing, of the occurrence of such data security incident.
- Investigate the data security incident and conduct a reasonable analysis of the cause(s) of the data security incident.
- Provide periodic updates of any ongoing investigation to IDS's impacted customers.
- Develop and implement an appropriate plan to remediate the cause of the data security incident to the extent such cause is within IDS's control.
- Cooperate with the customer's reasonable investigation or the customer's efforts to comply with any notification or regulatory requirements.

Relevant Aspects of Internal Control (Continued)

Control Activities (Continued)

Policies and Procedures (Continued)
Application Security
IDS’s information security program (including the adoption and enforcement of internal policies and procedures) is designed to:

- Identify reasonably foreseeable and internal risks to security and unauthorized access to the IDS network.
- Minimize security risks, including through risk assessment and regular testing.
- Address information security, physical security, and business continuity management.

The transfer of data from customer to the IDScloud is managed through a secure server that is used to transfer data from the customer to the IDScloud solution. Customer application data may not be exported from the IDScloud solution to IDS’s on-site locations.

Data Backup
Critical infrastructure and data are backed up regularly for the IDScloud solution. IDS uses commercially supported solutions within the AWS infrastructure. Data is stored in relational databases and deployed with AWS’s relational database device (RDS). Daily snapshots of the RDS, along with incremental snapshots throughout the day, are performed and retained for a period of time.

For client reconciliation and audit purposes, IDS performs monthly native SQL backups that are retained for 12 months. These backups are retained in accordance with IDScloud contractual commitments.

The IDScloud Operations team monitors and reviews the status of the backups and retention limits. The Operations Team also reviews logs and metrics to resolve any issues.

Business Continuity and Disaster Recovery
IDS maintains and verifies that its critical cloud subservicers maintain business continuity and disaster recovery plans that provide information and procedures.

Tests of the business continuity plans are performed every year. The results are documented, and changes are made to the policies and procedures according to the lessons learned.

Attachment B
Principle Service Commitments and System Requirements

Principle Service Commitments and System Requirements

IDS designs its processes and procedures related to its system to meet its objectives for its IDScloud services. Those objectives are based on the service commitments IDS makes to user entities, the laws and regulations that govern the provision of services, and the financial, operational, and compliance requirements IDS has established for the IDScloud services.

Security, availability, and confidentiality commitments to user entities are documented and communicated in the Master Software-as-a-Service Agreements IDS executes with clients. Security, availability, and confidentiality commitments are standardized and include but are not limited to the following:

- Maintaining an information security program
- Limiting employee and contractor access to those who have a legitimate business need for such access privileges
- Ensuring customer data is protected by encryption while in use, at rest, and during transmission
- Maintaining breach notification protocols, including notifying the customer of the occurrence, investigating the incident, providing a periodic update on the investigation, and cooperating with the customer's investigation
- Conducting annual penetration testing to expose vulnerabilities
- Deploying layers of defense such as firewalls and intrusion prevention and detection

IDS establishes operational requirements that support the achievement of security, availability, and confidentiality commitments; relevant laws and regulations; and other system requirements. Such requirements are communicated in IDS's system policies and procedures, system design documentation, and contracts with clients. Information security policies define an organization-wide approach to how systems and data are protected. These include policies related to how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained.