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

September 1, 2020 through February 28, 2021

International Decision Systems, Inc.

System and Organization Controls Report Relevant to Security, Availability, and Confidentiality on the Description of the IDScloud Solution Services
September 1, 2020 through February 28, 2021

Table of Contents

Section 1
International Decision Systems, Inc.’s Assertion

International Decision Systems, Inc.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within International Decision Systems, Inc.'s ("IDS") IDScloud Solution Services (the "System") throughout the period September 1, 2020 through February 28, 2021, to provide reasonable assurance that IDS's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in 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 September 1, 2020 through February 28, 2021, to provide reasonable assurance that IDS'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)*. IDS'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 September 1, 2020 through February 28, 2021, to provide reasonable assurance that IDS's service commitments and system requirements were achieved based on the applicable trust services criteria.

Section 2
Independent Service Auditor's Report

WIPFLI

Independent Service Auditor's Report

Management of International Decision Systems, Inc.
Minneapolis, Minnesota

Scope
We have examined International Decision Systems, Inc.'s ("IDS") accompanying assertion titled "International Decision Systems, Inc.'s Assertion" (the "assertion") that the controls within IDS's IDScloud Solution Services (the "System") were effective throughout the period September 1, 2020 through February 28, 2021, to provide reasonable assurance that IDS'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
IDS 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 IDS's service commitments and system requirements were achieved. IDS has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, IDS 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 IDS'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 IDS'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.

WIPFLI

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 IDS's system were effective throughout the period September 1, 2020 through February 28, 2021, to provide reasonable assurance that IDS'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

March 18, 2021

Attachment A
Description of the Boundaries of International Decision Systems, Inc.'s IDScloud Solution Services

Attachment A Description of the Boundaries of International Decision Systems, Inc.'s IDScloud Solution Services

Company Overview

Nature of Business

International Decision Systems, Inc. ("IDS" or the "Company") 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 to provide the underlying software platform to help enable clients to build their business. IDS has worked with financial institutions in over 30 countries.

IDS's origination and portfolio management solutions include products designed to help meet clients' asset finance needs. This includes an extensible architecture that integrates into client business processes and connects to third-party resources as needed. IDS is committed to ongoing investment in its asset finance solution, which helps ensure clients will 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 San Francisco, the United Kingdom, Australia, and India.

IDS's location covered in this report includes teams located in Minneapolis, Minnesota.

Product Overview

The IDScloud Solution Services ("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 clients' business needs evolve. The base configuration is functionally rich and highly configurable, which enables clients to align IDScloud with their business processes.

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 clients' businesses grow.

IDS's services are hosted in AWS data centers in the United States and Australia, with additional global locations available to be deployed based on client requirements.

Attachment A Description of the Boundaries of International Decision Systems, Inc.'s IDScloud Solution Services

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 or more frequent basis, and a group of Managing Directors (MD) meets monthly to provide oversight to management in the establishment and monitoring of company goals, strategic direction, and operational results. Members of the MD and 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.

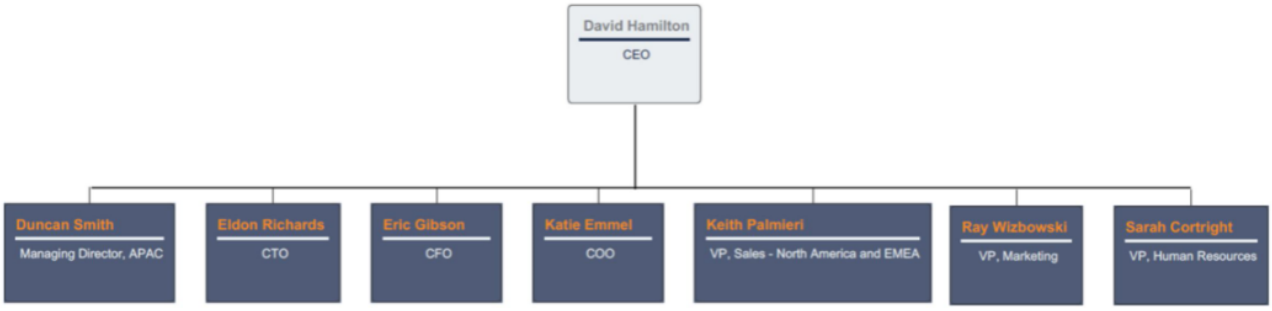
IDS, through its BOD, MD, and executive management, considers the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.

The members of IDS's executive management team includes the following:

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

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

IDS's executive management team is listed below:



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 Company. Examples of the assignment and limitation on authority are:

- An electronic routing process providing the professional service's team with a workflow to approve statements of work presented to clients.
- Delegations of authority including expenditure authority, legal review, and sign-off on contracts with nonstandard terms.
- Establishment of a security advisory team that meets on at least a quarterly basis.
- Daily standups with the IDScloud tech team and weekly IDScloud executive updates.
- Regularly scheduled meetings with ownership and the BOD.

Relevant Aspects of Internal Control (Continued)

Control Environment (Continued)

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 executive management team, in conjunction with the MD, routinely evaluates changes and proposed changes to key departmental structures and related required skill sets.

Executive management establishes 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 policies and procedures on IDS's intranet as well as through ongoing compensation and training. IDS monitors employees' adherence to its policies and provides employees with a means to report behavior that does not conform with IDS's policies and procedures. IDS has established the following controls to hold individuals accountable for internal control responsibilities:

- Quarterly check-ins for employee and status updates
- Performance reviews at least once a year
- Incentive plans
- Disciplinary action

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.

The expectations of ownership 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 on an annual basis.

IDScloud Team Organization and Management

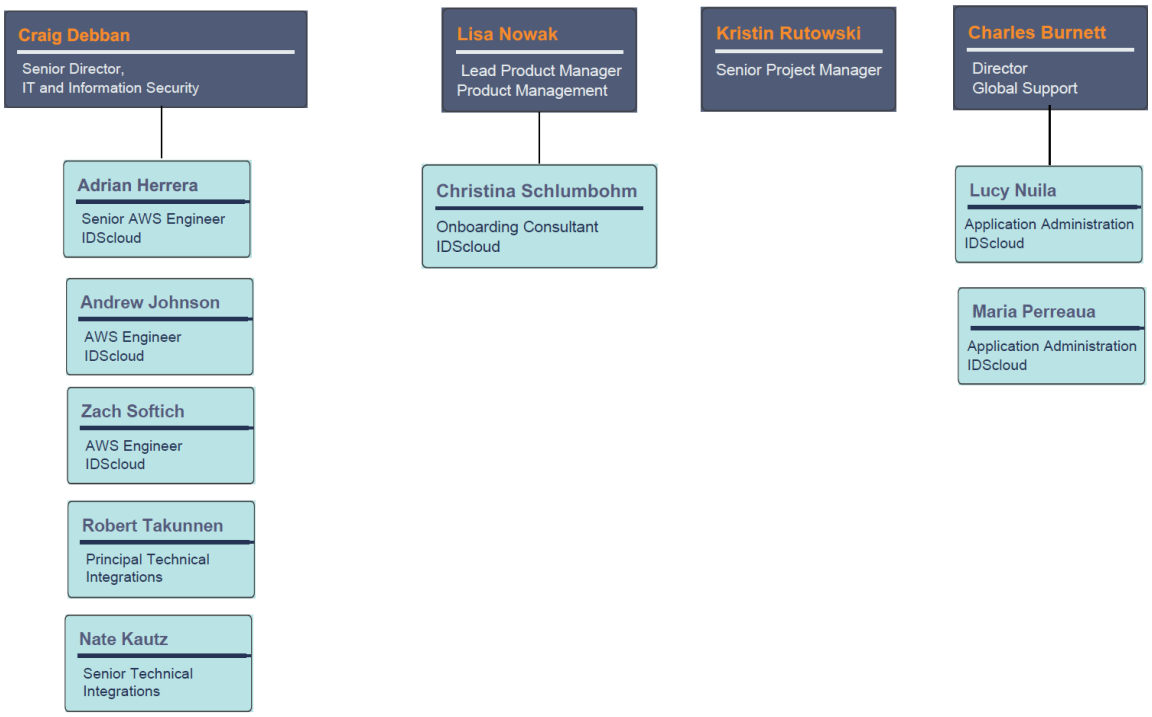
The lead product manager serves as the IDScloud initiative leader. This role is responsible for the overall IDScloud program across a number of workstreams, including service proposition, technology, client onboarding, client support, and program financials. A dedicated IDScloud team has been formed 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.

Relevant Aspects of Internal Control (Continued)

Control Environment (Continued)

IDScloud Team Organization and Management (Continued)

The IDScloud team meets routinely to plan, check status, discuss, and assign tasks to meet other non-development-related company objectives. The IDScloud team's organization is below:



Strategic Plan

IDS's strategic plan, which is developed with 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. Policies include but are not limited to the following:

- Business Ethics Policy
- Drug and Alcohol Policy
- Employee Handbook
- Security Policy
- Harassment Policy

Relevant Aspects of Internal Control (Continued)

Control Environment (Continued)

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.

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 obtain feedback and help ensure the new hire is successful and that the Company and the role are as expected. Feedback is shared with managers as appropriate.

Training and Professional Development

Managers organize onboarding plans for new employees, including 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.

Specifically, product managers at IDS are kept up to date on relevant industry information that impacts the development and relevance of the application.

Risk Assessment

IDS policies set forth the Company's approach to risk management, outlining the risk management process, and identify reporting procedures. In addition, they describe the relationship among 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 will be 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 assets, employees, clients, and reputation.

Relevant Aspects of Internal Control (Continued)

Control Environment (Continued)

Risk Assessment (Continued)

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.
- **Employee responsibility:** IDS employees understand IDS's policies and procedures as they apply to the individual employee's role. Through IDS employees and management team, individual departments monitor risk at a departmental level.
- **Managing 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 an 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 contacts to help limit IDS 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 clients 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.

Relevant Aspects of Internal Control (Continued)

Information and Communication (Continued)

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 clients 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 the 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.

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 client level, IDS has developed mechanisms enabling the IDScloud operations and support teams to be notified and, in turn, notify clients of potential operational issues that impact the client experience. These mechanisms are derived from information systems that are designed to produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. IDS personnel are provided with information on how to report system failures, incidents, concerns, and other complaints to personnel. IDS personnel and clients 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.

Relevant Aspects of Internal Control (Continued)

Information and Communication (Continued)

External (Continued)

Technical documentation is available on an IDS client-facing website for external users and describes and explains how to use the solution. Clients 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 client-facing website and in system documentation. Suppliers, external auditors, regulators, and financial analysists may report findings to the relevant department with which they are transacting. Material issues are raised via the Risk Management Policy.

The client agreement sets forth IDS's responsibility for providing notifications for system outages or downtime. Regularly scheduled maintenance time is planned for Wednesday evenings as outlined in the IDScloud engagement guide. Client communications with details on production updates typically is communicated 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.

Use and Monitoring of Subservice Providers

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

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

IDS's corporate network is connected to the AWS cloud through an encrypted virtual private network (VPN) tunnel. IDS uses dedicated, secured, and isolated virtual local area networks (VLAN) to interface with the AWS solution. These VLANs are then used to remotely connect to parts of IDScloud on AWS based on role, responsibility, and rights. In addition, encrypted session connections occur from IDS endpoints to and from AWS to help protect against third party disclosure in transit.

IDScloud is supported by HEAT, an Ivanti product, as a hosted client support tool. Ivanti also hosts within AWS utilizing a similar architecture design for resiliency.

IDScloud uses DataDog as a cloud-based availability and performance monitoring tool. DataDog runs on AWS, and information collected through this tool is stored long term on AWS Glacier.

IDScloud utilizes Arctic Wolf as a security operations center service to monitor IDScloud network traffic and prevent unauthorized access, changes, and disruption to every client account.

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

Relevant Aspects of Internal Control (Continued)

Control Activities

Policies and Procedures

IDS 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. Information security policies include, but are not limited to the following:

- Security Policy
- Vendor Management Policy
- Security Risk Management Policy
- Information Classification and Data Handling Policy
- Access Control Policy
- Backup and Retention Policy
- Technical Testing and Compliance Policy
- Product Vulnerability Management Policy
- Information Security Incident Response Policy
- Infrastructure Change Management Policy
- Business Continuity and Disaster Recovery Policy
- Business Ethics
- Employee Handbook

Security Awareness Training

IDS helps ensure its employees are aware of security risks and the associated policies and procedures through various mechanisms that include but are not limited to the following:

- New employee onboarding procedure
- Annual security awareness training
- Product training
- Secure coding training (as applicable by role)
- Periodic emails from the Information Security Officer

Employment

IDS requires that background checks be completed prior to hiring. In addition, after employment but before access to the Company systems, employees must review and sign off on key policies and complete mandatory security training. This access and acceptance is managed through HR and IT.

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 approval from IDS's Risk Committee.

Access is revoked when an employee's employee record is changed to termination in IDS's 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.

Relevant Aspects of Internal Control (Continued)

Control Activities (Continued)

Employment Termination (Continued)

This process includes:

- Revoking or disabling the user's access to applications on the day the termination takes effect.
- Revoking or disabling access to IDS's domain and, depending on position, access to IDScloud.
- Collecting IDS physical assets.
- Reformatting assets prior to redistribution or certifying destruction by a third-party vendor.
- Creating separate tasks for managers and/or potential business users to review based on the former employee's prior access to certain data.

Under certain conditions, privileged individual accounts may need to remain accessible after the termination date. In these cases, the account password is changed, and the account is marked as locked. Data is migrated from the terminated account to a designated active account. When management determines that necessary data has been preserved, the account is fully closed.

Client Implementation

For client implementations, the client 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 client, 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.

Each client has its requirements and specifications outlined in a contract executed by IDS and the client. New clients are provided with a user manual and, as needed, receive training on the application. For existing IDS clients that are transferring to the IDScloud platform, IDS receives, imports, and validates the data transferred into the application. For both new and transferring clients, Product Support maintains an implementation project plan containing details necessary to implement the client's application instance.

During the onboarding process, clients are provided with a test environment. Production Support maintains user access to the client's production environment for a defined period of time after the client approves the application setup.

Data upload or conversion activities are done on AWS's conversion environment provided to the client 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 within AWS, and the conversion environment is destroyed.

Relevant Aspects of Internal Control (Continued)

Control Activities (Continued)

Employment Termination (Continued)

Client Implementation (Continued)

Dedicated IDS project managers oversee tracking of goals and objectives to match agreed-upon services and statements of work to the delivery of IDScloud to our clients. Project plans are shared and discussed with the client during routine and ad hoc meetings during the implementation phase.

Security

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's offices to help eliminate a single point of failure that could interrupt access to IDS's virtual desktop infrastructure (VDI) and the IDScloud-AWS solution.

IDScloud uses AWS virtual private cloud (VPC) and virtual subnets (VLAN) to segment the network and associated client environments from other clients, development, and user acceptance training environments. Clients are protected using web application firewalls (WAF).

Arctic Wolf delivers 24/7 cybersecurity protection for every IDScloud client.

Physical Access

A digital identification (ID)-based physical access control system has been implemented at IDS's facility entry and exit points. Integrated with the Company's Active Directory, access is controlled through a cloud-based tool. 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.

Remote Access

IDS employees access the internal systems and 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.

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 short message service (SMS) text messages to the IT team and appropriate security personnel.

Relevant Aspects of Internal Control (Continued)

Control Activities (Continued)

Security (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 IDS's 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 client to the IDScloud is managed through a secure server that is used to transfer data from the client to IDScloud.

Encryption
IDS utilizes the AWS Key Management Service and Certificate Services to provide encryption certificates and encryption keys across the client data and web interface with IDScloud providing encryption at rest and in transit.

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, through various hardware and subservice organizations, are sent to responsible security staff via email, monitoring systems, and SMS text messages. The responding individual(s) investigates the alerts, and if qualifying conditions are met, a security incident is recorded.

Compromise of Client Data
If IDS becomes aware that the security of client data, including personal data, has been compromised or that client 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 client, 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 impacted clients.
- Develop and implement an appropriate plan to remediate the cause of the data security incident to the extent such cause is in IDS's control.
- Cooperate with the client's reasonable investigation or the client's efforts to comply with any notification or regulatory requirements.

Relevant Aspects of Internal Control (Continued)

Control Activities (Continued)

Security (Continued)

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 server and application performance, application traffic, and anomaly detection.

IDScloud personnel are responsible for following defined protocol for reporting incidents. Incidents are tracked, recorded, and stored indefinitely. Communication that requires the client's acknowledgement is managed through IDS personnel. IDS personnel also communicate with the client regarding issue resolution, and if the issue impacts multiple clients, 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 the Company's policies and procedures.

System Passwords

Users are required to enter a user ID and password to access 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

Client 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 management team.

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's clients. This includes the development of the applications on IDScloud. Procedures on this process are available for employees on IDS's corporate intranet site.

Changes to the calculation logic in our software follow a requirements gathering, design, test case production, and quality assurance (QA) testing process. Standard reports are tested and reviewed for accuracy and completeness prior to each major release. IDS follows the SDLC process when resolving errors as well as while running calculation validations, which is done on a continuous basis.

Relevant Aspects of Internal Control (Continued)

Control Activities (Continued)

Change Management

IDScloud Change Management Policy
IDS requires changes to be managed in a rational and predictable manner so employees, contractors, clients, 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. These controls include, but are not limited to:

- Generating a change order detailing the following:
  - Change detail
  - Risk level for each change
  - Test results
  - Desire timing
  - Back-out plans as appropriate.
- Obtaining required authorizations.
- Notifying and training affected parties.
- Coordinating the implementation schedule with other activities within the organization.

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 Routine Updates
Standard financial reports are generated through the application. The standard reports comprise the expected reporting each client can rely on for use in their financial statements, including the Financial Accounting Standards Board (FASB) Standard Report, FASB Disclosure Report, and General Ledger (GL) Feeds. The application uses field-level validation when data is entered.

IDS retrieves, validates, and updates rate tables within the application on a monthly basis. Changes to the calculations in the application are communicated to clients upon release of the update.

Relevant Aspects of Internal Control (Continued)

Control Activities (Continued)

Change Management

IDScloud Engineering Change Process

The engineering process for IDScloud follows industry-standard code development processes. Using defined workflow controls, IDScloud implements and tracks changes to IDScloud. 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.

Data Backup and Recovery

Critical infrastructure and data are backed up regularly for IDScloud. IDS uses commercially supported solutions within the AWS infrastructure. Data is stored in relational databases and deployed with the AWS Relational Database Service (RDS). Daily snapshots of RDS, along with incremental snapshots throughout the day, are performed and retained for a period of time and in accordance with client agreements. Monthly and long-term backups are retained indefinitely using AWS services.

On at least an annual basis, IDS performs a disaster recovery test focusing on failures of RDS and restoration to a different availability zone within AWS. Although rare, these are the most likely occurrences to cause a disruption.

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. Alarms are configured to notify appropriate response teams, and escalation communication channels are established through electronic collaboration methods.

Attachment B
Principle Service Commitments and System Requirements of International Decision Systems, Inc.'s IDScloud Solution Services

Attachment B Principle Service Commitments and System Requirements of International Decision Systems, Inc.'s IDScloud Solution Services

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

Security, availability, and confidentiality commitments to user entities are documented and communicated in Service Level Agreements (SLA) and other client agreements, as well as in the description of the service offering provided online. Security, availability, and confidentiality commitments are standardized and include but are not limited to:

- Security principles within the fundamental designs of IDScloud that are designed to permit system users to access the information they need based on their role in the system, while restricting them from accessing information not needed for their role.

- Use of encryption technologies to protect client data both at rest and in transit.

- Monitoring tools, multiple availability zones within AWS, and dynamic environment provisioning provide high availability commitment for IDScloud.

IDS establishes operational requirements that support the achievement of security 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 around 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. In addition to these policies, standard operating procedures on how to carry out specific manual and automated processes required in the operation and development of the IDScloud platform have been documented.