Mitratech Holdings, Inc.

Service Organization Control (SOC) 3 Report

Report on Mitratech Holdings, Inc.'s Enterprise Legal Management Software-as-a-Service System Relevant to Security and Confidentiality

For the Period March 1, 2016 to August 31, 2016

Strictly Private and Confidential

Tel: 214-969-7007
Fax: 214-953-0722
www.bdo.com

600 North Pearl, Suite 1700
Dallas, TX 75201

Independent Service Auditor's Report

To Management of Mitratech Holdings, Inc.:

Scope

We have examined management's assertion that Mitratech Holdings Inc.'s ("Mitratech") Enterprise Legal Management Software-as-a-Service System ("System") throughout the period March 1, 2016 to August 31, 2016, maintained effective controls to provide reasonable assurance that the system was protected against unauthorized access, use, or modification and that information designated as confidential was protected to meet Mitratech's commitments and system requirements based on the criteria for the security and confidentiality principles that are set forth in TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* ("applicable trust services criteria"). This assertion is the responsibility of Mitratech management. Our responsibility is to express an opinion based on our examination.

Mitratech uses subservice organizations (Rackspace, Cyrus One, AlertLogic and Sungard) to provide colocation facilities, security monitoring, and disaster recovery. Certain applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at the subservice organizations are suitably designed and operating effectively. Our examination did not extend to the services provided by the subservice organizations, and we have not evaluated whether the controls management expects to be implemented at the subservice organizations have been implemented or whether such controls were suitably designed and operating effectively throughout the period March 1, 2016 to August 31, 2016.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of the controls related to the security and confidentiality of the System, (2) testing and evaluating the operating effectiveness of 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.

Because of their nature and inherent limitations, controls at a service organization or subservice organization may not always operate effectively to prevent or detect and correct errors or fraud in a timely manner. Also, the projection to the future of our conclusions, based on our findings, is subject to the risks that the system may change or that control performance at a service organization or subservice organization may become inadequate or fail.

In our opinion, in all material respects, management's assertion referred to above, is fairly stated base on the applicable trust services criteria.

BDO USA, LLP

Dallas, Texas
November 3, 2016

Management's Assertion Regarding the Effectiveness of Its Controls

Mitratech Holdings, Inc. ("Mitratech") maintained effective controls over the security and confidentiality of its Enterprise Legal Management Software-as-a-Service System ("System") to provide reasonable assurance that the System was protected against unauthorized access, use, or modification and information designated as confidential was protected to meet Mitratech's commitments and system requirements based on the criteria for the security and confidentiality principles that are set forth in TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* ("applicable trust services criteria") throughout the period March 1, 2016 to August 31, 2016.

The Description of Mitratech Holdings, Inc.'s Enterprise Legal Management Software-as-a-Service System Throughout the Period March 1, 2016 to August 31, 2016 identifies the aspects of the System covered by this assertion.

Mitratech uses subservice organizations (Rackspace, Cyrus One, AlertLogic and Sungard) to provide colocation facilities, security monitoring, and disaster recovery. Certain applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at the subservice organizations are suitably designed and operating effectively.

Mitratech Holdings, Inc.
November 3, 2016

DESCRIPTION OF MITRATECH HOLDINGS, INC.'S ENTERPRISE LEGAL MANAGEMENT SOFTWARE-AS-A-SERVICE SYSTEM THROUGHOUT THE PERIOD March 1, 2016 TO August 31, 2016

System Overview, Scope, and Boundaries

Company Background

Mitratech is one of the market-leading provider of legal, compliance, and operational risk solutions for more than 1200 corporations of all sizes across the globe, representing six of the Fortune 10, almost 40 percent of the Fortune 500, and over 500,000 users in over 150 countries. Mitratech's award winning products are also used by over 12,000 of its clients' external partners, including 99 of the Global 100 and 100 percent of the AmLaw 200 law firms. Mitratech's portfolio of software solutions, which have received Market Leader designations from Hyperion Research, offer end-to-end matter management, spend management, e-Billing, legal hold, contracts management, GRC, and reporting solutions. Clients are able to prove demonstrable value creation for their organization by automating legal and compliance workflows, improving business outcomes through actionable data and insight, increasing collaboration with external partners, and reducing overall risk and cost.

The scope of this report is limited to security and confidentiality controls related to the Enterprise Legal Management Software-as-a-Service system ("System") and does not encompass all aspects of Mitratech services or other services provided by Mitratech. Mitratech uses Rackspace, Cyrus One, AlertLogic, and SunGard, independent subservice organizations, to provide colocation facility, security monitoring, and disaster recovery services for the System. The services and related controls of the subservice organizations are excluded from the scope of the examination.

Infrastructure

Mitratech has a Local Area Network ("LAN") installed at the corporate office, which is used by employees to access infrastructure systems, Internet, e-mail, and printing. Employees use the corporate network to access production systems at the Rackspace and Cyrus One colocation facilities via jump box or two-factor RSA token over a virtual private network ("VPN") which is used at Cyrus One as an alternative to the jump box.

All components of the applications and supporting operating system are kept current through patch updates. Mitratech's Hosting team reviews the appropriate patches; then creates a rollout plan consisting of planning, deployment, and testing. All hardware components are re-imaged with a hardened, tested operating system, and security build prior to deployment.

Software

Mitratech's Enterprise Legal Management Software-as-a-Service system ("System") consists of several principal applications:

- Secretariat – Designed to simplify aspects of corporate governance standards by automating tasks such as filing state forms, drafting consents to prepare annual meeting documents and creating and distributing corporate organizational charts.
- eCounsel – An enterprise level legal matter management solution for medium sized legal departments that lets the legal department track details for any matter, assign and manage internal staff and outside counsel, manage legal spend and analyze trends.

- Corridor – Provides a technology solution to the challenge of managing corporate legal spend by automating the entire life cycle of an invoice from electronic submission through the final comparative analysis of budget versus actual.
- TeamConnect – An enterprise level matter legal management solution that lets the legal department track details for any matter, assign and manage internal staff and outside counsel, manage legal spend and analyze trends.
- Collaborati - Provides a technology solution to the challenge of managing corporate legal spend by automating the entire life cycle of an invoice from electronic submission through the final comparative analysis of budget versus actual.
- LawTrac - An enterprise level legal matter management solution for small size legal departments that lets the legal department track details for any matter, assign and manage internal staff and outside counsel, manage legal spend and analyze trends.
- Document Vault – An integrated document management system.

All applications are available as full-featured browser-based, thin-client web applications which are offered as a Software-as-a-Service ("SaaS") offering. The applications can also be offered on premise and the on premise applications are excluded from the scope of this report. Suite Manager, a .NET application, is installed on a System Administrator's workstation and allows for overall administration of the eCounsel application. Suite Manager is also available from inside the hosted environment via a hosted thin-client solution.

People

Roles and responsibilities are defined in written job descriptions. Minimum qualifications are also documented in the job descriptions. Mitratech has assigned its employees, including but not limited to, the following roles and responsibilities:

Client Support
- Responsible for production support and problem resolution
- Responsible for training clients in using Mitratech applications

Hosting Support
- Responsible for testing of new software releases and software problem troubleshooting

Operations
- Responsible for the maintenance of software, servers, network infrastructure, monitoring and expanding service capacity, and backup and recovery of data

Security
- Responsible for maintaining security controls, periodic audits of software and infrastructure, incident response, business recovery planning, and compliance activities

Procedures

Information system security policies and procedures have been documented and are updated by management on an as needed basis and reviewed at least annually. Logical security standards have been established and define minimum logical security controls for Mitratech operations and applications.

Management has developed and communicated to user entities and internal users procedures to restrict logical access to the System through service level agreements, training, and systematic mechanisms requiring authentication prior to gaining access to the System.

Mitratech has documented and implemented formal policies, standards, and procedures for its production operations. Detailed procedures have been implemented to guide the continuous support of Mitratech's product line and clients as well as logging of the client support needs. Client support or information requests are received by Mitratech via e-mail, telephone, and/or client portals. Client Support uses the ticketing system to create client support tickets, assess client requests and information, assign work tickets, find contracts, log applicable information pertaining to the client, and close tickets. Client Support tracks client problems for timely resolution.

Periodic monitoring of client problems helps Client Support personnel determine whether appropriate corrective actions or procedures were implemented. Client Support management monitors response rates of client support and information requests.

Mitratech has defined change as any of the following:

- New system – application, operating system, database, hardware platform, or infrastructure;
- Major upgrade to an existing system – version release, new or upgraded components and/or subsystems (hardware or software);
- Minor upgrades to an existing system – patches, modifications to existing systems, and infrastructure changes that are transparent to end-users; and
- Any other change to hardware or software running that may or may not affect the systems.

The Change Control Review Board consists of Hosting Director, Hosting staff, Hosting and Security Vice President, members of the client support team, and members of the development team. Primary responsibilities of the Change Control Review Board include:

- Reviewing and evaluating submitted change requests;
- Recommending the change for approval, rejection or deferring reviewed change requests; and
- Providing an explanation for all rejected or deferred change requests.

Management has classified change requests into three (3) categories:

- Urgent – Severe business or production impact, if not implemented immediately;
- Special – Significant business or production impact, if not implemented; and
- Non-Critical – Limited to no business or production impact, if not implemented.

All changes are formally requested, approved, and tested, and Mitratech requires segregation of duties between development and implementation activities.

Data

All client data provided to Mitratech must be identified and categorized per the Mitratech data classification guidelines.

The Access Account Management Standards & Guidelines document details the various levels of data classification that are defined. Mitratech does not view client data and therefor considers all client data to be highly sensitive.

All corporate data is classified as the following:

- Level 1 – Confidential (Patient Health Information, Payment Card Industry Data Security)
- Level 2 – Private (Employee Information, Vendor Data)
- Level 3 – Sensitive (Financial Data, Business Plans, Internal Project reports)
- Level 4 – Public (Annual Reports, Press Statements)

Mitratech retains client data differently between products in Rackspace and products in Cyrus One. Data for eCounsel, Secretariat, Corridor, and Document Vault is kept up to one year, and data for TeamConnect, Collaborati, and LawTrac is kept for two weeks from the date of receipt unless otherwise specified. Clients may request that their data only be retained for the period necessary to resolve a current issue or need. The main purpose for retaining client data is to aid Mitratech in providing support to its clients. By storing past copies of client data in-house, Mitratech is able to restore a client's data to solve issues and provide other services to the client such as custom reports.

Mitratech restricts access to the SaaS development, test, and production environments to authorized personnel. Additionally, client data in the production environments is not used for development and test purposes. Mitratech uses dummy data in these environments to prevent users from accessing sensitive client data.

Mitratech provides a virtualized hosted and managed solution that allows clients to access the System. Clients are responsible for ensuring completeness, accuracy, timeliness, authorization, and confidentiality of transactional and master data inputs, processing, output, and tracking within their environments. Mitratech uses an industry-leading encryption-at-rest technology to protect client data. This encryption protects both structured and unstructured data with integrated data encryption, encryption key management and a common infrastructure environment. Secure File Transfer Protocol ("SFTP") and Hypertext Transfer Protocol Secure ("HTTPS") are used to secure data files in transit.

User Entity Responsibilities

User entities have ultimate responsibility for their controls, taken as a whole, and they are responsible for establishing internal procedures to implement those controls. Those procedures are the responsibility of the user entity and may include items like those listed below, however, this list should not be regarded as a comprehensive list of all procedures which a user entity may need to have in place. Each user entity must determine if the listed responsibility is relevant to them and if they have addressed relevant responsibilities.

- User entities are responsible for reading, understanding, and complying with Mitratech's privacy policy that is provided on the Mitratech website.
- User entities are responsible for reviewing and/or testing installed products, services, and configurations to ensure completeness and accuracy prior to accepting the installation.
- User entities are responsible for ensuring adequate user provisioning, user access modification, and termination controls for all users accessing systems controlled by the user entity.
- User entities are responsible for ensuring that access to the software used by the user entity is secured with a unique username and password for all individuals.
- User entities are responsible for establishing procedures to ensure that only authorized personnel can perform sensitive functions and to enforce proper segregation of duties for applications used by the user entity.

- User entities are responsible for providing the list of authorized approvers to Mitratech for any changes or access to the system for client personnel and ensuring that access and changes are appropriately authorized.
- User entity personnel with administrator access are then responsible for the creation of lower roles for the given user entity.
- The user entity is responsible for maintaining its authorized users within its subscription, including disablement/deletion of the user entity's employee access.