IRON MOUNTAIN®

IRON MOUNTAIN

System and Organization Controls SOC3® Report

Description of Iron Mountain Information Technology (IT) Infrastructure Environment and Application Hosting Services System relevant to Security, Confidentiality and Availability for the period January 1, 2017 through September 30, 2017

Table of Contents

Ernst & Young, LLP
200 Clarendon Street
Boston, Massachusetts 021116

Tel: +01 617 266 2000
Fax: +01 617 266 5843
ey.com

Report of Independent Accountants

To the Management of Iron Mountain Information Management, LLC:

Approach:
We have examined management's assertion that Iron Mountain Information Management, LLC ("Iron Mountain") maintained effective controls to provide reasonable assurance that:

- the Iron Mountain Information Technology (IT) Infrastructure Environment and Application Hosting Services System was protected against unauthorized access, use, or modification to achieve Iron Mountain's commitments and system requirements
- the Iron Mountain IT Infrastructure Environment and Application Hosting Services System was available for operation and use to achieve Iron Mountain's commitments and system requirements
- the IT Infrastructure Environment and Application Hosting Services System information is collected, used, disclosed, and retained to achieve Iron Mountain's commitments and system requirements

during the period January 1, 2017 to September 30, 2017 based on the criteria for security, availability and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100A, *Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of Iron Mountain's management. Our responsibility is to express an opinion based on our examination.

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. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Iron Mountain's relevant security, availability and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Iron Mountain's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent Limitations:
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability and confidentiality are achieved.

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion:

In our opinion, Iron Mountain's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability and confidentiality.

Ernst + Young LLP

November 29, 2017
Boston, Massachusetts

IRON MOUNTAIN®

Management's Assertion Regarding the Effectiveness of Its Controls Over the Information Technology (IT) Infrastructure Environment and Application Hosting Services System Based on the Trust Services Principles and Criteria for Security, Availability and Confidentiality

November 29, 2017

Iron Mountain Information Management, LLC ("Iron Mountain") utilizes Cyxtera (formerly CenturyLink) (the subservice organization) to provide data center hosting services consisting of physical security and environmental safeguards to support the Information Technology (IT) Infrastructure Environment and Application Hosting Services System.

We, as management of, Iron Mountain are responsible for designing, implementing and maintaining effective controls over the Information Technology (IT) Infrastructure Environment and Application Hosting Services System (System) to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in Security controls, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations in an entity's Security's controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer

- Ineffective controls at a vendor or business partner

- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

We have performed an evaluation of the effectiveness of the controls over the system throughout the period January 1, 2017 to September 30, 2017, to achieve the commitments and system requirements related to the operation of the System using the criteria for the security, availability and confidentiality (Control Criteria) set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this evaluation, we assert that the controls were effective throughout the period January 1, 2017 to September 30, 2017 to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification to achieve Iron Mountain's commitments and system requirements
- the System was available for operation and use, to achieve Iron Mountain's commitments and system requirements
- the System information is collected, used, disclosed, and retained to achieve Iron Mountain's commitments and system requirements

based on the Control Criteria.

Our attached description of the boundaries of the IT Infrastructure Environment and Application Hosting Services System identifies the aspects of the IT Infrastructure Environment and Application Hosting Services System covered by our assertion.

Very truly yours,

The Management of Iron Mountain Information Management, LLC

System Description of Iron Mountain's IT Infrastructure Environment and Application Hosting Services System

Company Overview

Iron Mountain is a trusted global outsourcing partner for both records management and data management services. The Company's comprehensive services help businesses save money and manage risks associated with legal and regulatory compliance, protection of vital information, and business continuity.

Iron Mountain's primary business segments are: Records Management, Data Management Services, Secure Shredding and Document Management Solutions / Technology Escrow Services.

Records Management

Iron Mountain's Record Management Service provides clients the ability to choose from a variety of document management solutions, which includes:

- Records Management program development and implementation
- Policy-based records management programs, which feature secure, cost-effective storage, flexible retrieval access and retention management
- Customized services for vital records, film & sound and regulated industries
- Digital record center content management.

Data Management

Iron Mountain's Data Management Service offers clients the ability to securely vault backup tapes at offsite facilities. Iron Mountain works with their clients to develop a solution that allows for fast and efficient data recovery.

Secure Shredding

Iron Mountain's Secure Shredding provides information destruction services in order to help clients securely dispose of information, including information stored on media.

Document Management Solutions / Technology Escrow Services

As data continues to move in a digital format, Iron Mountain has designed solutions to assist companies with maintaining the availability and security of their digital records. Solutions include:

- Intellectual Property Management (IPM) services to assist companies with securing their source code and other proprietary information
- Cloud Storage for Medical Images (previously named Digital Record Center for Medical Images/ DRC-Mi)
- Digital Services / Digital Management Solutions

Executive Summary

This description covers Iron Mountain's IT Infrastructure and Application Hosting Services System (herein referred to as the 'System') that supports the aforementioned services provided by Iron Mountain. The scope of this description includes the technology infrastructure hardware and software components supporting the application operating system, databases and network devices by Iron Mountain's Global Information Services and Application Development groups. The systems are physically located in the Iron Mountain data center locations in Boyers, Pennsylvania, Milton Keynes, United Kingdom, along with co-locations managed by Cyxtera in Toronto, Ontario, Canada and/or Montreal, Quebec, Canada (collectively referred to as the 'in-scope production data centers'). Iron Mountain utilizes their data center in Kansas City, Missouri to host the disaster recovery systems supporting the IT Infrastructure Environment and Application Hosting Services System.

The System is compromised of the following components:

- Infrastructure (facilities, equipment and networks)
- Software (systems and utilities)
- People (developers, operators, users and managers)
- Procedures (automated and manual)
- Data (transaction streams, files, databases and tables).

The following sections of this description define each of these five components comprising the System.

Infrastructure

The system includes five data centers, located in Pennsylvania, United States; Missouri, United States; Quebec, Canada, Ontario, Canada and Milton Keynes, United Kingdom. Housed within these data centers are the supporting operating system platforms (UNIX, Linux, and Windows based), networking components (routers, switches, firewalls), and data storage devices. The data centers are inter-connected to several designated Iron Mountain office locations by an IP based network architecture. The IT personnel that support these data centers are primarily based at the Company's corporate office facilities in Massachusetts and Pennsylvania as well as each of the Company's datacenter locations in Pennsylvania, United States; Missouri, United States; Quebec, Canada, Ontario, Canada and Milton Keynes, United Kingdom .

This system description covers the IT infrastructure (e.g., network, operating system, and database components) supporting the following applications, which are managed by Iron Mountain's Global Infrastructure Services group:

- Iron Mountain Connect Web Portal
- SafeKeeper Plus (SKP)
- SecureBase / SecureSync
- Document Management Storage – Digital Records Center Imaging (DRCi and DRC)
- Document Management Storage – Kofax Central (Kofax)
- Intellectual Property Management ("IPM") solution
- Cloud Storage for Medical Images

Iron Mountain is presently managing approximately 400 servers supporting the in-scope technology solutions. These servers are summarized below by operating system and the various purposes served.

Operating System	Server Purpose	
RHEL 5.x RHEL 6,x RHEL 7,x HP-UX 11.2x HP-UX 11.3x AIX 6.x	Database servers System management tools Networking systems Backup/Recovery services	Web servers and FTP Monitoring tools Application servers
RHEL 5.x RHEL 6.x Windows 2012 Windows 2008 RHEL 5.x RHEL 6.x Windows 2012 Windows 2008	Web servers and proxies Customer data intake servers (ESF, MQ, FTI) Backup/Recovery services Image storage Domain controllers Data Ingestion processes Monitoring tools Application servers Database servers	Monitoring tools FTP services Application servers Data Ingestion Processes Application servers Database servers FTP services Backup/Recovery services Domain controllers

Software

The software utilized to manage and support the in-scope System consists of various business line applications and supporting infrastructure and support tools that are used to support the monitoring, job scheduling and processing, change management, and help desk support. Iron Mountain uses a three-tiered network architecture as its standard: Web Tier, Application Tier, and Database Tier. All tiers are separated by firewalls and protected by intrusion detection systems.

People

Below is a brief description of each of these functional areas:

- The Global Infrastructure Services group is responsible for the following functional areas:
  - The Global Systems group is responsible for server operating system and middleware configuration, integration and operations. Additionally, this group is responsible for some system access administration functions.
  - The Global Operations Center is responsible for system and network monitoring as well as job scheduling.
  - The Global Networks group is responsible for global network management including global network communication device (router/switch) and network security device (firewall, IDS) configuration, integration, and operations.
  - The Global Storage group is responsible for the global storage configuration, integration and operations, along with the backup/recovery, disaster recovery planning and testing.
  - The Global Databases group is responsible for the global database configuration, integration and operations.
  - The Security Administration is responsible for securing the systems and network based on the guidelines and policies defined by Information Security Group.
- The Global Service Delivery group is responsible for Access Administration, Access Control, Desktop Support, End User Support, and Application Support a manages the Enterprise Change Management committee.

- The Software Engineering Support group is responsible for Service Level Agreement Management Solution Developments as well as manages and plans for the overall enterprise architecture design and development.

As of August 1, 2017, Iron Mountain engaged with HCL for cross-functional IT services based on the ITIL model, including Service Strategy, Service Design, Service Transition, Service Operations and Continual Service Improvement. Iron Mountain maintains management oversight of the activities HCL is performing. On a weekly basis, operational leads from HCL and IRM meet to discuss the day-to-day operations and concerns, while leadership meetings occurs on a monthly basis. HCL's relationship with Iron Mountain is managed through Iron Mountain's overall vendor management program, which includes vendor assessments.

Procedures

Iron Mountain has documented policies and procedures to support the operations and controls in support of their service. Relevant policies and procedures are made available to employees through the Iron Mountain Compliance & Security Services (COMPASS) and SharePoint intranet sites.

Specific examples of the relevant policies and procedures include the following:

- Requirements of authorized users regarding responsibility and accountability
- Account administration
- Data classification, retention and destruction
- Security incident report and response
- Training and education
- Change management and application development
- Physical and environmental protection
- Third party access and management

Data

Client data is retained in accordance with applicable data protection and other regulations set out in Client contracts and Iron Mountain policies. As defined within the Iron Mountain data classification policy, Client data is considered confidential and is retained and disposed of in accordance with Iron Mountain's commitments and requirements as defined within the data classification policy and customer contract. Confidential client data includes the physical data stored in boxes and on tapes stored at Iron Mountain facilities, digital images, and electronic escrow data stored within the systems. This does not include the data (e.g. metadata) securely retained within the systems used solely for tracking the assets stored with Iron Mountain. Client confidential data, electronic or hard copy, is retained according to the commitments and requirements, as defined within the contracts and agreements. The standard retention of client confidential information is for Iron Mountain to retain data indefinitely. Client confidential data is retained, returned, or destroyed solely at the specific request of the client or based upon the agreement within the client termination agreement. These requests, along with client requests for changes to retention or disposal requirements, are documented and tracked within a ticket until closure. Access to client data is limited to authorized Iron Mountain personnel and is only granted in accordance with physical and logical Iron Mountain system security administration policies.

Subservice Organizations

Iron Mountain utilizes Cyxtera (subservice organization) to provide data center hosting services, including physical security and environmental safeguards, to support the System components in the Toronto and Montreal data centers. It is expected that the subservice organization has implemented the following controls to support achievement of the associated criteria:

Criteria Reference	Expected Subservice Organization Controls
CC5.5	Access to the data center is restricted to authorized employees and contractors through the use of card readers and other systems (e.g. hand readers).
	Visitors to the data center are required to sign a visitor log.
	Physical access to the data center facilities is restricted to appropriate personnel who require such access to perform their job functions.
	Administrative access to the card system and other systems (e.g. biometric readers) is limited to authorized and appropriate personnel.
	Camera surveillance of the data center is monitored and retained for a period of time.
A1.2	Environmental safeguards at the data center facilities are designed, implemented, operated, and maintained, including the following: · Fire detection and suppression systems · Climate, including temperature and humidity, control systems · Uninterruptible power supplies (UPS) and backup generators · Redundant power and telecommunications lines

User Responsibilities

Iron Mountain communicates the responsibilities of its user entities (e.g. Customers) through the contract acceptance and addendum process. The following highlight some of those responsibilities:

- Users of the IT Infrastructure and Application Hosting Services System are responsible for ensuring that access to the system limited to authorized and appropriate individuals. (Criteria CC5.4)
- Users of the IT Infrastructure and Application Hosting Service s System are responsible for reviewing documentation provided by Iron Mountain related to changes made to the systems. (Criteria CC7.1, CC7.4)
- Users of the IT Infrastructure and Application Hosting Service s System are responsible for reporting any security or confidentiality breaches and availability incidents, which impact the systems. (Criteria CC6.2)
- User entities are responsible for approving and validating the appropriateness (and maintaining the confidentiality) of data provided to Iron Mountain and any changes to that data. (Criteria CC1.2)
- User entities are responsible for adequately securing data contained in any output reports provided by Iron Mountain, including appropriateness of individuals accessing the output reports through the systems and storage/disposal of the output reports. (Criteria C1.3)
- User entities are responsible for communicating security and confidentiality provisions to individuals accessing information within the systems and/or produced by the System. (Criteria CC1.4)
- User entities are responsible for communicating any identified security, availability and/or confidentiality violations impacting the in-scope systems and/or data to Iron Mountain on a timely basis, as necessary. (Criteria CC6.2)
- User entities are responsible for communicating retention period of confidential information and when to dispose of confidential information. (Criteria C1.7, C1.8)