Crowe

Smart decisions. Lasting value.™

System and Organization Controls Report SOC 3®

Independent Service Auditor's Report on Controls at a Service Organization Relevant to Security, Availability, and Confidentiality

Related to Iron Mountain Information Management, LLC's Information Technology (IT) Infrastructure Environment and Application Hosting Services

Under the AICPA, Statement on Standards for Attestation Engagements No. 18 (SSAE No. 18), Section AT-C 205, *Examination Engagements*

For the Period January 1, 2021 to September 30, 2021

IRON MOUNTAIN®

Table of Contents

© 2021 Crowe LLP

SECTION I: Independent Service Auditor’s Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Iron Mountain Information Management, LLC

Scope

We have examined Iron Mountain Information Management, LLC's (Iron Mountain's) accompanying assertion titled "Assertion of Iron Mountain Information Management, LLC's Management" (assertion) that the controls within Iron Mountain's IT Infrastructure Environment and Application Hosting Services System (system) were effective throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that Iron Mountain's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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

Iron Mountain 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 Iron Mountain's service commitments and system requirements were achieved. Iron Mountain has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Iron Mountain is responsible for selecting, and identifying in its assertion, the applicable trust service 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 the controls were not effective to achieve Iron Mountain's service commitments and system requirements based on the applicable trust service criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Iron Mountain's service commitments and system requirements based on applicable trust services criteria

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

© 2021 Crowe LLP

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 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 conclusions 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 or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Iron Mountain's Iron Mountain Information Technology (IT) Infrastructure Environment and Application Hosting Services System were effective throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that Iron Mountain's service commitments and system requirements were achieved based on the applicable trust services criteria is fairy stated, in all material respects.

Crowe LLP

Atlanta, Georgia
November 15, 2021

© 2021 Crowe LLP

SECTION II: Assertion of Iron Mountain Information Management, LLC's Management

November 15, 2021

ASSERTION OF IRON MOUNTAIN INFORMATION MANAGEMENT, LLC'S MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Iron Mountain Information Management, LLC's (Iron Mountain or service organization) Information Technology (IT) Infrastructure Environment and Application Hosting Services System throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that Iron Mountain's service commitments and system requirements relevant to Security, Availability, and Confidentiality (applicable trust services criteria) 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 January 1, 2021 to September 30, 2021, to provide reasonable assurance that Iron Mountain's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (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*). Iron Mountain'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 A.

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 January 1, 2021 to September 30, 2021, to provide reasonable assurance that Iron Mountain's service commitments and system requirements were achieved based on the applicable trust services criteria.

Iron Mountain Information Management, LLC

ATTACHMENT A: Description of the Boundaries of the System and Principle Service Commitments and System Requirements

Description of the Boundaries of the System

Business and Organization

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.

Four of Iron Mountain's primary business operation relevant to the system description include: Records Management, Data Management, Secure Destruction and Digital Solutions Services.

Records Management

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

- Records Management program development andimplementation
- 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 Records Management Workflow –Inbound Process

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.

Iron Mountain manages two primary tape vaulting programs for customers. These programs are Open Media and Closed Containers.

- Open Media: Storage of customer media at the tape level and tracked via the designated volume serial (VolSer) label of the tape. Storage is allocated by a unique customer number and segregated in racking assigned to the customer. Media delivery and pickup is accomplished through the assignment of "transport" containers individually assigned to the customer with their unique customer number.
- Closed Container: Storage of customer media in containers. The customer is assigned a unique customer number and storage containers which are not opened by Iron Mountain Staff.

Secure Destruction

The Iron Mountain Secure Destruction Services develops, implements, and manages secure, sustainable destruction solutions that help and enable customers to manage the risks associated with the disposal of information. The Iron Mountain Secure Destruction Service is a nationally recognized service provider targeting customers of all sizes and in nearly all industries. The Service is a natural fit with Iron Mountain's Records Management core service offering, customer base and supporting operations. Iron Mountain offers off site destruction through a plant hub and spoke network as well as onsite destruction using a mobile shred fleet.

© 2021 Crowe LLP

Iron Mountain's Secure Destruction Service is predicated on the security of customer's material. Iron Mountain has invested millions of dollars in safeguards throughout the chain of custody to help ensure best in class technology and well defined, auditable handling procedures to keep customer's material secure from the time of pick up to the actual destruction.

Digital Solutions 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 using their Digital Solution Services. The solution includes:

- Digital Record Center (DRC)
- Document Imaging Services

Iron Mountain's Digital Solutions services provides the resources necessary to convert hardcopy documents already stored in Iron Mountain facilities or received from customers via mail or courier to an electronic format and make them readily available to users across a customer's organization, share documents electronically across the organization, enhance business processes, and safeguard their information from loss or destruction.

© 2021 Crowe LLP

Subservice Organizations

Iron Mountain uses a third-party service provider (subservice organization) to assist in the delivery of their Information Technology (IT) Infrastructure Environment and Application Hosting Services System. Iron Mountain has assumed that certain controls have been implemented by the subservice organization that are necessary, in combination with Iron Mountain's own controls, to provide reasonable assurance that Iron Mountain's service commitments and system requirements are achieved based on the applicable trust services criteria.

Below is a listing of the subservice organizations used by Iron Mountain, as well as the expected complementary subservice organization controls (CSOCs). The subservice organization controls are not included in the boundaries of the system.

Subservice Organization	Service(s) Provided	Expected CSOCs

Cyxtera	Data center hosting services, including physical security and environmental safeguards, to support the System components in the Toronto and Montreal data centers.	• CC6.4
		  ○ 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

© 2021 Crowe LLP

Components of the Information Technology (IT) Infrastructure Environment and Application Hosting Services

Infrastructure and Software

The software utilized to manage and support the in-scope System consists of various business line applications and supporting infrastructure and 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 scanners, which are strategically placed over critical network points and are monitored by the Iron Mountain IT Department.

The following table highlights the primary applications that support each of the aforementioned services:

Application	Records Management	Data Management	Secure Shed	Digital Solutions
IMConnect	√	√	√	
SafeKeeperPLUS	√		√	
SecureBase/SecureSync		√		
Digital Record Center				√
Kofax				√

IMConnect

Iron Mountain Connect or IMConnect (www.ironmountainconnect.com) is the customer's primary point of authentication for various Iron Mountain service line applications. It is a global application that supports 19 different language translations.

SafeKeeperPLUS (SKP)

SKP is a proprietary application developed by Iron Mountain. The purpose of the application is to allow Iron Mountain employees to manage the physical inventory of Iron Mountain facilities for their Records Management customers.

SecureBase and SecureSync

The SecureBase and SecureSync applications are internally developed products that are used by employees and customers respectively for scheduling media (e.g., backup tapes) pickups, tracking media inventory, reporting, and administrative tasks as part of the Data Management services.

© 2021 Crowe LLP

Digital Solutions Services

The Digital Solutions product uses three software platforms that have been enhanced by Iron Mountain and are used by customers to digitize, store, access, and manage documents.

- Digital Record Center (DRC) – The DRC portion supports the following:
- Kofax Central (Kofax) – Centralizes imaging functionality, streamlining imaging operations

Cloud Storage for Medical Images

Cloud Storage for Medical Images is previously named as Digital Record Center for Medical Images (DRC-Mi), a next generation solution designed for the secure and reliable object storage to meet commitments and requirements.

People

In order to support and maintain the Security, Availability and Confidentiality of the in-scope System, the following core support services are fully involved:

- Global Technology Office Group
  - Global Infrastructure Services Group
  - Workplace Technologies & Collaboration Group
  - Software Engineering Support Group
  - Information Security Group

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

- The Global Technology Organization group is responsible for developing strategic plans to align business and IT objectives as well as communicate current IT concerns and environmental changes to the respective business lines. This plan is communicated and presented on a quarterly basis during the GTO all hands meeting.
- The Global Technology Office group is responsible for developing strategic plans to align business and IT objectives as well as communicate current IT concerns and environmental changes to the respective business lines. This plan is communicated and presented on a quarterly basis during the GTO all hands meeting.
  - The Global Infrastructure Services group is responsible for the following functional areas:
    - The Global Systems group is responsible for computer hardware, 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 service, system and network monitoring.
    - 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 and Backup 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 Enterprise Change Management committee is responsible for managing the Change Advisory Board (CAB).
- The Workplace Technologies & Collaboration Group is responsible for Access Administration, Access Control, Desktop Support, End User Support, and Application Support (Level 1). Additionally, CTO reporting's are a shared responsibility between the Workplace Technologies & Collaboration Group and the Global Infrastructure Services group
- 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.
- The IT Security group is responsible for securing the systems and network based on the guidelines and policies defined by Information Security group.

Iron Mountain has engaged TCS, a third-party vendor, 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 TCS is performing. On a weekly basis, operational leads from TCS and IRM meet to discuss the day-to-day operations and concerns, while leadership meetings occur on a monthly basis. TCS'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's intranet sites. Policies and procedures are reviewed and updated on a regular basis. Control activities in support of these policies and procedures have also been designed and are described in further detail in the section title "Overview of Iron Mountain's Control Activities".

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.

Physically Stored

Iron Mountain provides its customers with a safe and secure way to transport, store, and destroy vital physical data. Iron Mountain utilizes vehicles equipped with advanced security systems to help ensure that client data is securely transported to and from Iron Mountain's storage facilities. Within these facilities, further security measures are in place to secure customer data, such as badge systems, security guards,

© 2021 Crowe LLP

motion detection systems, camera, etc. In addition, Operations personnel are regularly trained and evaluated on the handling of customer data to ensure that proper chain of custody is maintained at all times while customer data is in Iron Mountain's possession. Formal loss mitigation procedures have also been developed and include steps to be followed when customer assets are potentially misplaced.

© 2021 Crowe LLP

Principle Service Commitments and System Requirements

Iron Mountain designs its processes and procedures relevant to the Business Operations Services System to meet objectives for its services. Iron Mountain's objectives are based on the service commitments made to customers in applicable contracts, applicable laws and regulations, and the financial, operational and compliance requirements that Iron Mountain has established for its services. The principal service commitments and system requirements commitments include:

- Implementing logical and physical access restrictions to help ensure that logical and physical access to programs, data, and IT resources is restricted to appropriately authorized users and that access is restricted to performing appropriately authorized actions.
- Implementing technical and non-technical controls, along with safeguards, to help ensure the availability of data in accordance with the system documentation and requirements.
- Implementing technical and non-technical controls to retain and dispose of confidential data in accordance with agreed upon retention terms.

Iron Mountain establishes operational requirements that support the achievement of itssecurity, availability and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Iron Mountain's policies and procedures, system design documentations and contracts with third parties (customers and vendors).

© 2021 Crowe LLP

Complementary User Entity Controls

The Iron Mountain Information Technology (IT) Infrastructure Environment and Application Hosting Services control structure is designed with the assumption that certain controls would be implemented by user entities. This section describes user entity controls identified by Iron Mountain as necessary to achieve certain applicable trust services criteria.

The user entity controls described below should not be regarded as a comprehensive list of all controls which should be employed by user entities. There may be additional controls that would be appropriate to address Security, Availability, and Confidentiality concerns which are not identified in this report. Each user entity is responsible for the identification, implementation and operating of appropriate controls to address their specific concerns as related to Iron Mountain's Information Technology (IT) Infrastructure Environment and Application Hosting Services.

Complementary User Entity Controls	Relevant Trust Services Criteria
Users of the System are responsible for helping ensure that access to the system limited to authorized and appropriate individuals.	Criteria CC6.2, CC6.3
Users of the System are responsible for reviewing documentation provided by Iron Mountain related to changes made to the systems.	Criteria CC8.1
Users of the System are responsible for reporting any security or confidentiality breaches and availability incidents, which impact the systems.	Criteria CC7.3
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 CC1.5
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 CC6.6
User entities are responsible for communicating security and confidentiality provisions to individuals accessing information within the systems and/or produced by the System.	Criteria CC2.2
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 CC7.3
Users of the System are responsible for ensuring that authorized individuals are available at the time of pickup or providing Iron Mountain with pre-authorization.	Criteria CC6.7

© 2021 Crowe LLP

Complementary User Entity Controls	Relevant Trust Services Criteria
Users of the System are responsible for ensuring that changes to authorized signers are communicated to Iron Mountain in a timely basis.	Criteria CC6.7
User entities are responsible for communicating retention period of confidential information, when to dispose of confidential information, and to confirm requests of disposals are processed.	Criteria C1.1, C1.2

© 2021 Crowe LLP