IRON MOUNTAIN

Service Organization Control 2 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, 2016 through December 31, 2016

Table of Contents

Assertion of Iron Mountain Information Management, LLC

IRON MOUNTAIN®

Assertion of Iron Mountain Information Management, LLC

February 24, 2017

We have prepared the accompanying *Description of the Iron Mountain Information Technology (IT) Infrastructure Environment and Application Hosting Services System for the period January 1, 2016 to December 31, 2016* (Description) of Iron Mountain Information Management, LLC (Iron Mountain or Service Organization) based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization's system set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy* updated as of December 15, 2016 (the description criteria). The Description is intended to provide users with information about the Information Technology (IT) Infrastructure Environment and Application Hosting Services System (System), particularly system controls, intended to meet the criteria for the security, availability and confidentiality principles set forth in the AICPA's TSP section 100, *Trust Services Principles, and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

We confirm to the best of our knowledge and belief, that:

a. the Description fairly presents the System throughout the period January 1, 2016 to December 31, 2016, based on the following description criteria:

i. the Description contains the following information:
   (1) The types of services provided.
   (2) The components of the system used to provide the services, which are the following:
      · Infrastructure. The physical structures, IT, and other hardware components of a system (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).
      · Software. The application programs and IT systems that supports application programs (operating systems, middleware, and utilities).
      · People. The personnel involved in the governance, operation and use of a system (developers, operators, entity users, vendor personnel, and managers).
      · Procedures. The automated and manual procedures.
      · Data. Transaction streams, files, databases, tables, and output used or processed by the system).
   (3) The boundaries or aspects of the system covered by the description.
   (4) For information provided to, or received from, subservice organizations or other parties
      (a) How such information is provided or received; the role of the subservice organization or other parties

(b) The procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls

(5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:
   (a) Complementary user-entity controls contemplated in the design of the Iron Mountain Information Technology (IT) Infrastructure Environment and Application Hosting Services System
   (b) When the inclusive method is used to present a subservice organization, controls at the subservice organization

(6) If the service organization presents the subservice organization using the carve-out method:
   (a) The nature of the services provided by the subservice organization
   (b) Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria

(7) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons therefore.

(8) In the case of a type 2 report, relevant details of changes to the service organization's system during the period covered by the Description.

ii. the Description does not omit or distort information relevant to the service organization's system while acknowledging that the Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria were met if the controls operated as described and if user entities applied the complementary user entity controls contemplated in the design of Iron Mountain's controls and if subservice organizations applied the controls contemplated in the design of Iron Mountain's controls throughout the period January 1, 2016 to December 31, 2016.

c. The Iron Mountain controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria.

The Management of Iron Mountain Information Management, LLC

Independent Service Auditor’s Report

Ernst & Young LLP
200 Clarendon St.
Boston, MA 02116

Tel: +1 617 266 2000
Fax: +1 617 266 5843
ey.com

Building a better working world

Independent Service Auditor's Report

To the Board of Directors
Iron Mountain Information Management, LLC

Scope
We have examined Iron Mountain Information Management, LLC's (Iron Mountain) accompanying *Description of the Iron Mountain Information Technology (IT) Infrastructure Environment and Application Hosting Services System for the period January 1, 2016 to December 31, 2016* of its Information Technology (IT) Infrastructure Environment and Application Hosting Services System (Description) based on the criteria set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy* updated as of December 15, 2016 (the description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security, availability, and confidentiality principles set forth in the AICPA's TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria) throughout the period January 1, 2016 to December 31, 2016. The Description indicates that certain applicable trust services criteria specified in the Description can be met only if complementary user entity controls contemplated in the design of Iron Mountain's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Iron Mountain uses CenturyLink, Inc. (CenturyLink) (subservice organization) to provide hosting services including physical and environmental controls. The description indicates that certain applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at the subservice organization are suitably designed and operating effectively. The description presents Iron Mountain's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organization to meet certain applicable trust services criteria. Our examination did not extend to the services provided by the subservice organization and we have not evaluated whether the controls management expects to be implemented at the subservice organization have been implemented or whether such controls were suitably designed and operating effectively throughout the period January 1, 2016 to December 31, 2016.

Iron Mountain's responsibilities
Iron Mountain has provided the accompanying assertion titled, *Assertion of Iron Mountain Information Management, LLC* (Assertion) about the fairness of the presentation of the Description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. Iron Mountain is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the

services covered by the Description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the Description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Service auditor's responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the Description based on the description criteria and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination. We conducted our examination 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, in all material respects, (1) the Description is fairly presented based on the description criteria, and (2) the controls described therein are suitably designed and operating effectively to meet the applicable trust services criteria throughout the period January 1, 2016 to December 31, 2016.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls, involves performing procedures to obtain evidence about the fairness of the presentation of the Description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the Description. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations
The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs. Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective or fail.

Opinion
In our opinion, in all material respects, based on the description criteria and the applicable trust services criteria:

a. the Description fairly presents the Iron Mountain Information Technology (IT) Infrastructure Environment and Application Hosting Services System that was designed and implemented throughout the period January 1, 2016 to December 31, 2016.

Building a better working world

b. the controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period January 1, 2016 through December 31,2016 and if user entities applied the complementary user entity controls contemplated in the design of Iron Mountain's controls and if subservice organizations applied the controls contemplated in the design of Iron Mountain's controls throughout the period January 1, 2016 to December 31, 2016.

c. the controls tested operated effectively to provide reasonable assurance that the applicable trust service criteria were met throughout the period January 1, 2016 to December 31, 2016, if the complementary user entity controls and subservice organization's controls referred to in the scope paragraph of this report were also operating effectively throughout the period January 1, 2016 to December 31, 2016.

Description of tests of controls
The specific controls tested and the nature, timing, and results of those tests are listed in the accompanying *Description of Criteria, Controls, Tests and Results of Tests* (Description of Tests and Results).

Restricted use
This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Iron Mountain, user entities of the Iron Mountain Information Technology (IT) Infrastructure Environment and Application Hosting Services System and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties
- Internal control and its limitations
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

This report is not intended to be and should not be used by anyone other than these specified parties.

Ernst & Young LLP

February 24, 2017
Boston, Massachusetts

Description of the Iron Mountain Information Technology (IT) Infrastructure Environment and Application Hosting Services System for the period January 1, 2016 to December 31, 2016

Overview of Iron Mountain Information Management, LLC

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.

Iron Mountain's primary business segments are: Records Management, Data Management Services, Secure Shredding and Document Management and Imaging Services / 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 Record Center for Images (DRCi)/ Document Imaging Services

Scope

This report covers Iron Mountain's IT Infrastructure and Application Hosting Services System (herein referred to as the 'in-scope System') that supports the aforementioned services provided by Iron Mountain. The scope of this report 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 (NAT1 SC1-5), Milton Keynes, United Kingdom, 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 and Application Hosting Services System.

Relevant Aspects of the Control Environment, Risk Assessment Process and Monitoring

Control Environment

Iron Mountain's business is built on a foundation of ethics and integrity and the belief and commitment that acting with the highest ethical standards isn't just the right thing to do; it helps build trust with our customers and contributes to our long term success. To help ensure that business at Iron Mountain is always conducted in an ethical and compliant manner, a robust corporate governance structure, headed by the Iron Mountain Board of Directors has been developed. The Board consists of individuals with depth and breadth of business experience. They offer a wide diversity of opinion, and a deep understanding of Iron Mountain's mission and vision.

Iron Mountain's ethics and compliance programs includes among other things:

- The Code of Ethics and Business Conduct
- The Compliance Helpline
- The Global Anti-Corruption and Anti-Bribery program
- The Global Privacy Program

The Code of Ethics and Business Conduct

The cornerstone of ethics and compliance at Iron Mountain is the Code of Ethics and Business Conduct. The Code provides guidance towards reaching decisions that are legal and ethical, and informs employees of ways to find more information when they need it. The Code of Ethics is published in about thirty languages, and has been distributed worldwide, both digitally and in-print. The digital version is available online. In addition to the Code of Ethics document, Iron Mountain has also created an interactive Code of Ethics training course, which reinforces key themes addressed in the Code.

Upon hire, new employees are required to complete the online training course and sign the Code of Ethics Compliance Certificate. In addition, employees must also periodically retrain and recertify on the Code.

The Compliance Helpline

As part of Iron Mountain's commitment to maintaining and enhancing its culture of ethics and compliance, employees are required to report all known or suspected violations of law or Company policy. Iron Mountain provides a number of ways for employees to do that, including the Iron Mountain Compliance Helpline. In line with industry best practices and legal compliance requirements, the Helpline is operated by an independent company, and (where permitted by law), employees can choose to remain completely anonymous when they make a report. The Helpline is available 24 hours a day, 365 days a year, and is reachable either by phone, or online.

To help ensure that employees are comfortable reporting their concerns, Iron Mountain also maintains a strict "no retaliation" policy: any employee or manager who attempts to retaliate, or who encourages others to retaliate, against an individual who has reported a violation in good faith will face serious disciplinary action, up to and including termination.

The Anti-Corruption and Anti-Bribery Program

In addition to the Code of Ethics and Business Conduct and the Compliance Helpline, Iron Mountain has implemented a robust, global anti-corruption and anti-bribery program. The program, which is managed by the Legal Department, in conjunction with our Global Security and Internal Audit teams, is designed to ensure compliance with a variety of laws and international conventions, most notably the U.K. Bribery Act and the U.S. Foreign Corrupt Practices Act.

A broad range of continually updated global policies serve to support the program, including the:

- Fraud, Waste, and Abuse Policy;
- Gifts, Hospitality Policy and Charitable Contributions Policy;
- Travel and Entertainment Policy;
- Background Investigations Policy;
- Political Contributions Policy.

The program also includes:

- An annual multi-factor risk assessment of all Iron Mountain business lines and countries;
- Annual certification to the program by international leadership;
- Ongoing auditing by Iron Mountain's Internal Audit Department;
- Comprehensive pre-contract assessment of subcontractors, agents, and consultants;
- Pre-merger, pre-acquisition, and pre-joint venture formation assessments; and
- A translation program that ensures all relevant Company documents is translated into local language.

The Global Privacy Program

In addition to Iron Mountain's suite of policies and procedures around physically and electronically securing customer information, Iron Mountain has implemented and maintains a global privacy program. The foundation of this program is the Iron Mountain Global Privacy Policy, which is supplemented with additional relevant policies, e.g. HIPAA policy, where necessary. As described below, Iron Mountain trains its workforce upon hire and thereafter on privacy and data security related topics.

Organizational Structure

Iron Mountain's organizational structure provides the framework for planning, directing, managing and monitoring its operations in order to effectively service its customers and achieve its corporate objectives. The key areas of authority and responsibility as well as appropriate lines of reporting are reflected in the company's organizational structure.

Iron Mountain is organized into different service lines, such as: Records Management and Storage; Secure Shredding; Data Management; Data Center Services; or Document Imaging and Management. In addition, the Company offers industry specific solutions for sectors such as: Entertainment; Government; Financial; Healthcare; or Law Firms. The business lines are supported by a number of corporate functions, such as Finance, Information Technology, Marketing, Legal, Privacy & Compliance; or HR.

To help ensure that the Company's employees and subcontractors deliver high quality services,

it has implemented a number of tools, such as policies and procedures relating to appropriate business practices and compliance, training, communication, maintaining and improving knowledge and experience, allocating resources, or clear job responsibilities and duties. All job related materials and the detailed organization charts are posted on the Company's internal website. In addition, Management regularly communicates with employees to ensure that all employees understand the Company's goals and objectives and how their individual actions interrelate and contribute to those objectives and the results.

Risk Assessment

The process of identifying, assessing and managing risks is a critical component of Iron Mountain's internal control system. The purpose of Iron Mountain's risk assessment process is to identify, assess and manage risks that affect the organization's ability to achieve its objectives as it relates to securing customer data and making it available. The management of Iron Mountain also monitors controls to consider whether they are operating as intended, and whether they are modified as appropriate for changes in conditions or risks facing the organization, including those associated with technological, environmental and regulatory changes.

Ongoing monitoring procedures are built into the normal recurring activities of Iron Mountain, and include regular management and supervisory activities. Managers of the various organizational units are regularly in touch with personnel, and may question the accuracy of information that differs significantly from their knowledge of operations.

Iron Mountain has established an independent organizational business unit, Risk Management (RM) group that is responsible for identifying risks to the enterprise, and monitoring the operation of the firm's internal controls. RM's approach is intended to align the enterprise's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business and maximize its opportunities in the rapidly changing market environment. RM attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management, including the Management Committee.

Global Internal Audit (GIA) is responsible for assessing the Iron Mountain risk and control environment through formal examination of financial, operational and administrative controls, risk management practices, and compliance with laws, regulations and Iron Mountain policies and procedures. The Vice President of Global Internal Audit reports functionally to the Chairman of the Iron Mountain Audit Committee and administratively to the Chief Financial Officer. GIA communicates significant findings and the status of corrective actions directly to these individuals. The GIA group adheres to standards of moral and ethical conduct, including those set forth in the Employee Handbook and the Institute of Internal Auditors ("IIA") Code of Ethics and Standards for the Professional Practice of Internal Auditing.

Monitoring

Management uses multiple reports/ dashboards created by the various internally developed applications to monitor the efficiency of certain processes and the effectiveness of certain key controls. Metrics produced from these information systems are used to identify weaknesses, inefficiencies or potential performance issues with respect to a particular process. Managers are given the responsibility to inform the individuals who report to them about these items at the appropriate time.

Control Activities

Control activities are the policies and procedures that help address risk and ensure management directives are carried out. Control activities, whether automated or manual, related to the achievement of specific criteria and are applied at various levels throughout the organization.
Specific control activities are provided in the Overview of Iron Mountain's Control Activities section within this Description as well as within the section: Description of Criteria and Controls.

Information and Communication

Information systems play a key role, as they produce reports, including operational, financial and compliance-related information, used to run and control the business. In a broader sense, effective communication must ensure information flows down, across and up the organization. Effective communication should also be ensured with external parties, such as customers, suppliers, regulators and shareholders about related policy positions.

The Company has other communication tools, which it effectively utilizes to help promote business activities as well as the importance of ethics, development and commitment to the Company. Informational emails (by function and group) and the Company's internal website also serve to keep employees informed. Efforts have been made to help organize and disseminate required information to field operation heads, in order to help them to in turn provide pertinent information to their field employees; these types of efforts should continue to be supported.

Furthermore, formal and informal supervisor/manager meetings, the Compliance Helpline and the Open Door Policy also serve to aid in the dissemination and proper flow of information.

Components of the System

Infrastructure and 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 scanners.

The systems are physically located in the Iron Mountain data center locations in Boyers, Pennsylvania (NAT1 SC1-5), Milton Keynes, United Kingdom, 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 and Application Hosting Services System.

IMConnect

Iron Mountain Connect or IMConnect (www.ironmountainconnect.com) is the customer's primary point of authentication for various Iron Mountain service line applications. IMConnect provides single sign-on access to the following service applications:

- Record Center

- Shredding Center
- Report Center
- Escrow Management

IMConnect also provides self-service support tools designed to help customers manage their use of IMConnect.

- User Administration – Create and Manage User Profiles
- Resources – Help Guides
- Password Reset

IMConnect uses VMWare's TCServer Java Application Server running on Red Hat Enterprise Linux hosted on x86 hardware. Load balanced clusters provide high-availability and scaling. Systems are patched with the latest Red Hat Enterprise Linux (RHEL) update bundle at least twice a year. CA's Siteminder provides access control, while IdentityMinder manages accounts stored on CA LDAP servers. Oracle RAC is used for application database.

Software and infrastructure changes are required to go through a testing lifecycle that includes a release into development, QA, Pre-Production and eventually Production environments. Prior to any production release, changes are be approved for deployment in accordance with Iron Mountain's change management policy.

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 Iron Mountain facilities for their Records Management customers. SKP uses a centralized infrastructure model to store the location and descriptive information of the customers' Business Records. Internal Iron Mountain employees access the application through desktop PC's and laptops, as well as dumb terminals located at our storage facilities and offices that are connected to our internal MLPS network.

External customers are able to access their Records Management inventory through the IMConnect portal and Records Center web interface. Customers are able to perform searches of inventory each individual user is authorized to have access to, as well as perform Order Entry and Order Tracking activities.

SKP also provides access to customers through SFTP/FTP with a tool called IMLink that allows customers to transfer files for ingestion into SKP for maintaining descriptive information, as well as Order Entry.

The major technologies used for the SKP application infrastructure are:

- High-end HP servers running HPUX 11.23 and 11.31 for the database and application tiers
- HP Blades and VMware for Linux and Windows machines for the web and application tiers
- IBM svc storage virtualization and HP disk storage arrays
- Cisco networking, Checkpoint firewalls and F5 load balancers
- Progress OpenEdge 11 databases and application stack
- Progress ESB and SonicMQ messaging
- Java, apache, jdbc, tomcat/tcserver for application development

The SKP application is structured using the common three tier architecture of web/app/database layering. Each layer of the application infrastructure has multiple machines for redundancy and resiliency.

The major infrastructure tiers are separated by centrally managed firewalls for security purposes.

Iron Mountain uses an extensive MPLS network to connect to over 600 remote district storage sites to a centralized computing environment. This provides the ability for our customers to view and manage their Global Records from one centralized application.

Iron Mountain has a secondary site that contains a complete copy of all the SKP database and infrastructure. Data replication technology is used from the primary site to the secondary site to keep the DR databases in sync with the Production environment. The SKP DR environment is tested by Iron Mountain annually.

SecureBase and SecureSync

The SecureBase and SecureSync applications are internally developed products that are used by customers for scheduling media (e.g. backup tapes) pickups, tracking media inventory, reporting and administrative tasks as part of the Data Management services. The applications are maintained through a configuration interface controlled by Iron Mountain dedicated staff. The applications are three-tiered client-server applications using (1) a client that is installed on each user's desktop, (2) a middle-tier modernization application component for connectivity maintenance, and (3) a SQL Server 2008 database backend.

The infrastructure supporting the SecureBase and SecureSync applications are comprised of a desktop client for application connectivity, underlying operating system and database technologies. The supporting IT components are located in Iron Mountain's Boyers, Pennsylvania and Milton Keynes, United Kingdom data center facilities, with failover services in Iron Mountain's Kansas City, Missouri data center. The underlying application and database infrastructure is based on HP Intel-based servers. The operating system for the servers is Windows Server 2008/2012, utilizing Microsoft SQL Server DTS packages and stored procedures to process transactions and store program data. The SQL Server tools reside on each server and on designated desktop PCs.

Iron Mountain user access to the applications, operating system and database layers are authenticated through the Microsoft Active Directory, and granted through access control lists through Assyst request tickets. Authorized user access from the PC of each designated / authorized user within the Company is managed through Active Directory and access control lists within the SecureBase / SecureSync application. The PCs are linked to the network through standard IP protocols.

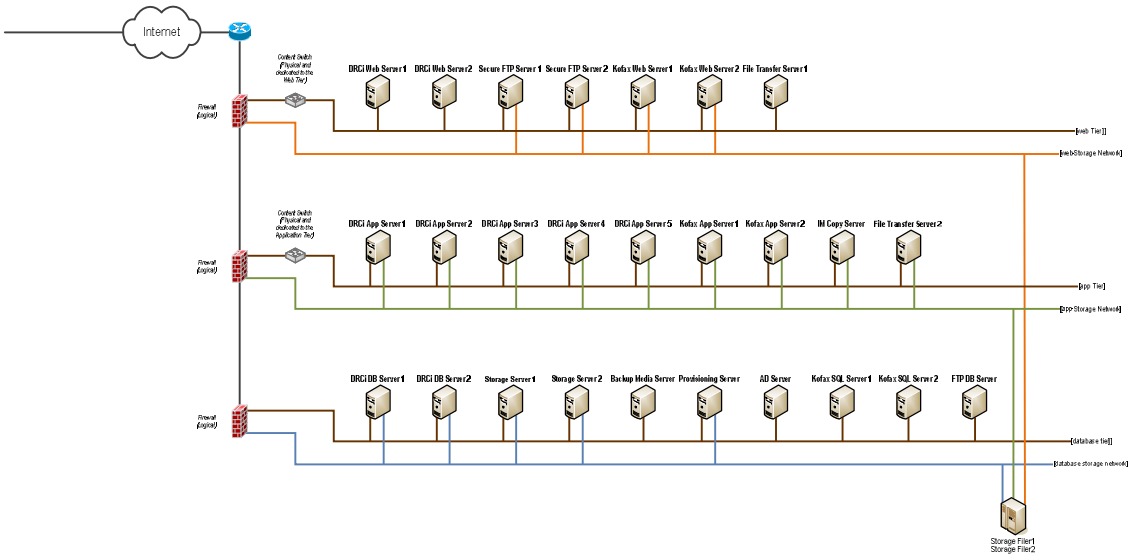
Document Management Solutions ("DMS") Product

The DMS product uses three software platforms that have been enhanced by IRM and are used by customers to digitize, store, access, and manage documents.

- Digital Record Center for Images (DRCI) – The DRCI portion supports the following:
    - Web based Login, Search, Retrieve, Email and download of documents
    - Customers can self-administer their groups through an admin interface
    - Web services allow for 3rd party integration (*managed by the Customer)*
    - Desktop upload enables low volume one off uploads from client desktops

- Digital Record Center@ (DRC@) – The DRC@ provides similar functionality as DRCI but extends functionality to incorporate workflow.
- Kofax Central (Kofax) – Centralizes imaging functionality, streamlining imaging operations

DRCI uses IBM's Content Manager on Demand to store and deliver digital records via the Web. Both Iron Mountain and customers upload digital documents to DRCI and DRC@. Both DRCI and DRC@ are three-tiered client-server application using (1) Apache HTTP Servers in Web Tier (DMZ) as proxy for incoming client requests (2) IBM WebSphere/Tomcat Application servers in a middle-tier for application and presentation to the end users, and (3) IBM DB2 and Microsoft SQL database backend.



Intellectual Property Management ("IPM") Product

IPM is an escrow agent that provides customers with a neutral third party to store an item of values (i.e., source code, confidential information) while two parties have a contract. To support the service, 2 primary applications are used (collectively referred to as the "IPM applications"):

- Escrow Management Center (EMC) – an external interface to customers. This application is accessed through the IMConnect infrastructure. The interface is designed to assist with managing the overall escrow process and deposit materials (i.e., source codes, confidential information). Customer functionality includes:
  - Creation of work orders
  - Create and modify beneficiary information, designated contacts and Exhibit B documents (e.g. packing list, index ID).
  - View work order status and history

  EMC is transmitted via eWork, a workflow management agent, to a SQL database, which is also used by the Jaguar/ Escrow Back Office application.

- Jaguar/Escrow Back Office (EBO) – an internal application for Iron Mountain employees to manage customers' deposit information. This application manages the inventory of the customer orders. Iron Mountain employees' access confidential data through the

Jaguar/EBO application. Access to confidential data is limited to authorized and appropriate Iron Mountain personnel.

The IPM applications are supported by Windows 2008/2012 and Linux RedHat operating system and SQL database servers as the backend storage.

Cloud Storage for Medical Images

Cloud Storage for Medical Images is previously named as Digital Record Center for Medical Images (DRCMi), which service offering is based on the NetApp StorageGRID solution, a next generation solution designed for the secure and reliable object storage to meet commitments and requirements.

The NetApp StorageGRID is built on a next generation software technology that applies grid computing technologies to object storage, and is tailored to the unique and specific requirements of healthcare.

People

The people supporting the in-scope System are part of Iron Mountain's Information Technology department, the Global Infrastructure Services and Global Product Services, who provide the following core support services over the components below:

- Data Center Operations
- Database Administration
- Data Storage Management
- System Administration
- Network Operations
- System Monitoring (including job processing)
- Network Administration
- Information Technology Security Administration
- Application/System Access Administration
- Help Desk Support
- Service Management
- Change Management
- Software Engineering
- Enterprise Architecture and Strategy Planning

In order to provide these services, the Information Technology Department is divided into the following functional areas: Global Infrastructure Services, Global Delivery Solutions Support and Software Engineering. 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 system monitoring and some system access administration functions.
    - 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, as well as network monitoring and job processing functions.
    - The Global Storage group is responsible for the global storage configuration, integration and operations, along with the backup/recovery, disaster recovery planning and testing and virtual infrastructure functions.
    - 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 Delivery Solution Support group is responsible for Access Administration, Access Control, Desktop Support, End User Support, and 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.

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. 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 held 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.

The following highlights the example data types are stored by Iron Mountain applications and the supporting database technologies:

- IMConnect - Data includes items such as login credential and account permissions and is stored in Oracle and LDAP databases.
- SafeKeeperPLUS (SKP) - Data includes items such as records metadata and archive information and is held in Progress database technology.
- SecureBase & SecureSync - Data includes items such as customer media tracking information, media numbers, and media location and is held in a SQL database technology.
- Cloud Storage for Medical Images - Data includes items such as document metadata and document image archives and is held in a NetApp Storage Grid technology.
- DMS - Data includes items such as document metadata and document image archives and is held in a DB2 and SQL database technology.
- IPM – Data includes items such as the description of the deposit information, order history and order status, held in a SQL database.

Clients are also provided access to output reports through the IMConnect portal site and web based Record Center application with access limited to their own data. Users are required to authenticate to the IMConnect Portal site, which requires a username and password.

Overview of Iron Mountain's Control Activities

Policy Management

Formal written policies for significant functions and processes have been developed and communicated throughout the organization. Policies are updated based on a periodic review schedule by an assigned policy owner and are reviewed and approved by designated members of management. Policies contain requirements around the Security, Confidentiality, and Availability of Client data and include (but not limited to) topics such as:

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

Iron Mountain has also developed formal confidentiality agreements (comprising of a Confidential Disclosure Agreement, Business Associate Agreement, and Non-Disclosure Agreement) that describe and communicate required provisions that employees, business partners and Clients agree to. These agreements (as relevant) include such topics as:

- How information is designated as confidential
- Handling, use, destruction and storage of confidential data
- Compliance with applicable laws and regulations
- Distribution and transmission of confidential data to only those who have a business need

Vendor On-boarding & Risk Management Program

Iron Mountain maintains a Third Party vetting program for all new and existing vendors. Vendors are required to sign contractual agreements which outline the vendor's security, availability, and confidentiality commitments and responsibilities. Only 'material' vendors require contracts. Iron Mountain determines whether a vendor is material are based on the following criteria:

- Total contract value
- Length of financial commitment
- Impact on Iron Mountain's customers
- If the supplier is developing any Iron Mountain proprietary product or service
- Access to confidential or protected information
- Logical access to Iron Mountain systems or physical access to Iron Mountain facilities
- Risk assessment classification

At point of vendor creation (after vendor acceptance), each vendor is categorized by vendor risk profile and classified into Critical, High, Medium or Low risk categories. All third parties are submitted for sanctions violations at point of creation, and monitored on an ongoing basis through a third party tool. High and Critical risk vendors have ongoing credit monitoring, annual risk assessment validation and, where appropriate, have physical audit inspections.

Employee On-Boarding & Security Awareness

Internal and external candidates are recruited for open positions based upon formal job descriptions, which are used by Iron Mountain to establish the qualifications and experiences necessary to fulfill the open position. As part of the hiring process, candidates will undergo a background check, which consists of the following components (*where legally permitted)*:

- Social Security trace
- National Criminal Record Check
- Sex Offender Registry Check
- Sanction List searches (i.e. OIG/GSA, FACIS, etc.)
- Criminal history checks at the county, state and federal level
- Employment verifications
- Education verification (where applicable)
- Motor vehicle searches (where applicable)

As part of Iron Mountain's on-boarding process, which is used for employees and contractors (collectively referred to as employees), employees are informed of their security, availability, and confidentiality responsibilities. Upon hiring, employees are provided with a copy of the Iron Mountain Computer Operating and Security Policy, the Iron Mountain Confidentiality Agreement and the Iron Mountain Code of Ethics and Business Conduct. Employees must sign an acknowledgement that they have read and understood the requirements of the agreements.

Iron Mountain utilizes both internal and external training exercises to continually train their employees on relevant topics such as incident management response, security awareness, and data confidentiality requirements. On an annual basis, the groups supporting the services are allocated funds for employee training. Departments fund the development/customization of the training programs and launch training through a variety of mechanism including a centralized formal Learning Management System, formal and information training via coaches, and informational refreshers through other mechanisms (such as Intranet articles, communications, workplace posters, etc.). Annually required training, such as Information Security, Code of Ethics, etc. also include a re-certification of the respective Policy to the required audience. Completion is monitored and tracked and reported to Leadership teams.

Physical Security and Environmental Safeguards

The technology components (i.e., network devices, servers) that comprise the in-scope System are located in one of the following data center locations (collectively referred to as 'in-scope data centers'):

- Iron Mountain owned and managed
  - Boyers, Pennsylvania
  - Kansas City, Missouri
  - Milton Keynes, United Kingdom
- Co-location (owned and managed by CenturyLink)
  - Toronto, Canada
  - Montreal, Canada

All client data is stored within database servers that are owned and managed by Iron Mountain.

Iron Mountain owned and managed data centers

The in-scope data centers are physically secured through badge access control systems that are used to control access to building entrances and computer rooms that house the in-scope systems, including supporting infrastructure, and local area network (LAN) resources (e.g., firewalls, routers). Access to the in-scope data centers require approval by the Data Center manager, and the list of those with access is reviewed on a quarterly basis. The badge access system is restricted to authorized personnel. The badge access system logs both valid and invalid access attempts to the data center facility. Upon demand, Corporate Security personnel can provide management with reports of access and access attempts meeting defined criteria such as those occurring after hours, or other invalid or suspicious access activities.

Approved requests for access badges are sent to Corporate Security personnel, and necessary data is entered into the badge access systems. Visitors are required to wear visitor badges (which are distributed by building receptionists and provide no access capabilities) in addition to being escorted by an employee active badge holder.

Department managers and the Human Resource (HR) Department are responsible for notifying appropriate personnel of employee termination. Terminated employees' access badges are deactivated within the badge access systems. For involuntary terminations, responsible personnel are notified to deactivate the access badge as soon as the employee is notified of the termination. HR personnel periodically provide Corporate Security personnel with a list of terminated employees for use in ensuring that the badge access systems have been properly updated.

The in-scope data center facilities that house the in-scope technology components are safeguarded by the following environmental safeguards: Fire detection and suppression devices, uninterruptible power supply (UPS) device, air conditioning units and a moisture and water detection system.

Co-location Data Centers

As part of Iron Mountain's monitoring and oversight of the CenturyLink data centers, Iron Mountain periodically reviews and receives third party attestation reports to determine the nature, timing, extent and conclusions of controls and whether the information within the reports is sufficient to satisfy the applicable criteria. In addition, Iron Mountain performs periodic site visits to each location to confirm the existence and adequacy of physical security controls.

In order for the Iron Mountain representative to access the facility, they must be authorized by designated Iron Mountain managers who can request access through a portal. Upon authorization, the Iron Mountain representative will be allowed to access the facility by CenturyLink. Iron Mountain has not granted CenturyLink logical access to the systems supported by the IT Infrastructure and Application Hosting Services.

Logical Access

Iron Mountain has defined a process to manage access to the data; prevent unauthorized access to the systems; ensure the protection of network services and detect unauthorized activities. Access to in-scope systems is protected by a combination of network security, internal application security and SQL/DB2 Server database security. Each security layer enforces both a unique username/password combination and further restrictive role-based security.

Passwords

Iron Mountain has developed and maintains a password policy, which is implemented across the various layers of technology managed by the IT Infrastructure and Application Hosting Services to properly secure data and maintain the confidentiality of data. The password policy consists of the following requirements, which are applied on information assets (where technically feasible):

- Password length
- Password complexity
- Password expiration
- Password timeout
- Password history
- Account lockout
- Account lockout duration

User Access Administration

Users requiring access or modifications to any component of the in-scope systems require a manager or an authorized designee to complete an IS-Security User Access Form. The form is then submitted to the Iron Mountain Help Desk, who creates a ticket and assigns the request(s) to the relevant system support group(s).

In the event that an Iron Mountain employee is separating from the company, a notification of termination is processed by Iron Mountain's Human Resource department, who open a ticket within the ticketing system. The Iron Mountain Helpdesk will disable the terminated employee's Active Directory account, which will revoke access to the network, file servers, VPN, Kofax and operating systems. From there, additional tickets will be created to revoke the employee's access to other applications, as necessary, including SKP, SecureBase, SecureSync, DRCi, IPM and IMConnect.

Privileged Access

Access to the in-scope systems is granted based on the least privilege approach and administrative access is restricted to those individuals who require such access to fulfill their job responsibilities. Administrative access to the systems is limited in accordance with the Company's policies.

Periodic Access Reviews

Quarterly Access Reviews are performed for all in-scope systems to ensure only authorized users have access. The results of the reviews are posted to the Iron Mountain Corporation Compliance & Security Services website "COMPASS" site.

Additionally, a review of Domain Administrators is performed for the DMS (DRCi, Kofax), IMConnect Portal, SecureBase, and SKP environments. Documentation associated with the reviews and approval of the access reviews and the supporting system generated listings are maintained on Iron Mountain's intranet site.

On an annual basis, a Periodic Access Review (PAR) over application layers supporting the DRCI CMOD and Kofax production environment is performed. The process is executed to review and confirm user access rights and privileges, including high-privileged access, critical

files. Application access is reviewed by the Global DMS IT Support Team. Additionally, Alfresco was installed in 2016 and contains a limited amount of customer data within the application. Privileged reviews will not be initiated until 2017.

Furthermore, a joint user review is performed by IPM IT Application Team and Business Management on a semi-annual basis to verify the appropriateness of all user access to IPM applications.

Network Security & Security Monitoring

Iron Mountain has implemented various threat detection and prevention mechanisms at the perimeter of the environment. This includes having redundant firewalls installed both on the perimeter and within the network to permit authorized traffic and deny unauthorized access. In the event that the rulesets are updated, a change request is submitted through the standard Iron Mountain change process. The firewall rulesets are monitored by FireMON to determine whether changes to the rulesets have been made. Access to administer the firewalls is restricted to explicitly authorized and appropriate personnel.

Also, Iron Mountain has installed Intrusion Detection Systems (IDS) to record and perform analysis of network traffic patterns, monitor and report information system-related events, create alarms and respond to attempted attacks. When an alert is received, a ticket is opened to document the alert and resolution. Iron Mountain Information Security receives a daily status report, which includes trend data on the alerts received and associated tickets.

Iron Mountain has implemented a Security Information and Event Management (SIEM) tool to help automate security event monitoring and maintain authoritative logs. The SIEM collects security logs from networking devices, remote access interfaces, email gateways, server operating systems, customer facing applications, and anti-virus or malware protection software. The tool correlates the logs and utilizes vendor provided and customized security monitoring rules to detect possible security risks and create alerts. The alerts are reviewed by the Iron Mountain security team and in the event a possible security incident is detected, the Iron Mountain security team will document the incident within a ticket to track through resolution in accordance with the Iron Mountain incident response policy. Access to administer the SIEM devices, which includes any changes to configurations within the tool, is restricted to explicitly authorized and appropriate personnel.

Iron Mountain performs vulnerability assessments over the infrastructure (e.g. network, servers) and applications are performed on at least a quarterly basis. The vulnerabilities noted within both quarterly scans are documented within tickets and tracked to resolution.

Anti-Virus Management

In order to protect the systems hosted by the IT Infrastructure and Application Hosting Service from computer viruses, malicious codes and unauthorized software, Iron Mountain utilizes industry-standard solutions and tools, which are installed on the servers as part of the process where technically feasible or exempted. The solutions are centrally administered and updates are pushed out to the agents installed on the production machines. Iron Mountain configures a scan schedule to detect computer viruses, malicious codes, or unauthorized software. In the event that a potential incident is discovered, it will follow the standard incident response process.

Customer Access

Customer access to the in-scope applications for Iron Mountain Customers is provided through the IMConnect application and SecureSync applications. The IMConnect application serves as the authentication point for customer access to SKP, DMS (Imaging on Demand) and IPM. DMS (DRCi/ DRC@) customers are assigned a unique URL in order to access the data within the application.

The customer has the ability to (and is responsible for) self-administering their own accounts at the application layer. The Customer is responsible for user administration (e.g. add, delete) activities with respect to their own users within these applications.

Application Development and Maintenance

Changes to the in-scope systems consist of upgrades, maintenance changes, data changes, vendor patches or configuration changes. All changes follow a common change management process. Requests for changes ("RFC"), including emergency changes, are submitted in the centralized enterprise ticketing system (Assyst). The change management ticket includes information about the changes, including proposed modification needed, the requester, and priority. Submitted tickets are then sent to the owners from the impacted areas for review and authorization.

Once the request has been authorized, an implementation timeline is determined and the change(s) are assigned to a system developer/ programmer or infrastructure engineer.

After the changes have been configured in the development environment, they are stored, backed up, and unit tested by the programmers. A segregated development and testing environment is in place that uses configurations from production and old historical data to accurately reflect the production environment. Access to the development and testing environments are restricted to authorized Iron Mountain personnel to maintain the security and confidentiality of data.

Once unit testing is completed, the programs are promoted to the system testing stage. After system testing is performed and results are acceptable, user acceptance testing is conducted by the business requester to validate user requirements (as required). In addition, regression testing is performed to verify that core application functions and processes continue to perform as expected after the changes have been introduced to the production environment. The results of testing are documented and reviewed and changes or unexpected results are communicated and addressed within the RFC ticket system or e-mail. The Database Manager participates in the overall process to validate that the database design is not adversely impacted and will continue to support the business objectives.

Upon completion of required testing and final sign-off on the change by the business, the changes are documented on the monthly Change Control Process list for movement to production during the next monthly Change Process. A Change Approval Board ("CAB") meeting is held weekly to determine which changes are ready for deployment into the production environment. The meetings are attended by representatives from Infrastructure, IS Application Development and various business units to review pending and recent changes. Depending on the nature of the change, CAB meetings may include regional or global members. The group reviews each change to understand the issue, teams or departments involved, the proposed resolution, any outage impacts, time schedule for implementation, and back-out plans.

Once all changes have been approved, the 'Monthly Release Form' is signed and dated by the Release Manager, DBA, and the IT Director. Then the list of approved changes is sent to the appropriate resource for deployment of patch / change from the test environment to the production environment.

System Backup and Recovery

Incremental and full backups are performed on a regularly scheduled basis for the in-scope systems using the CommVault backup utility and the status of backups is reported on a monthly scorecard. As part of the server build process, backup software is installed by default, unless Management has exempted the server from the backup process. The following components are included in the backup process for each of the in-scope systems:

- IMConnect: Application programs, data files, production servers and production databases
- SKP: Application programs, data files, production servers and production databases
- SecureBase/SecureSync: Application programs, data files, production servers and production databases
- DMS: Application programs, data files, CMOD application, Iron Mountain secure FTP site, Iron Mountain extranet site programs, production servers and production databases
- IPM: Application data/configuration files, production servers and production databases

Iron Mountain uses its Offsite Data Protection service for the off-site storage of physical tape media. Backups of production data are encrypted to prevent unauthorized individuals from being able to access the content of the backups. In the event that backup fails, the job failure would follow Iron Mountain's incident management process.

Access to the backup job schedulers is restricted to authorized and appropriate personnel. Access requests and modifications would follow Iron Mountain's standard access administration process.

In addition to the periodic backups, the Progress databases used for the SKP application are automatically replicated to the secondary datacenter using OpenEdge replication.

Business Continuity and Disaster Recovery

Iron Mountain has developed a business continuity plan, which is designed to provide an overall management process as well as the underlying foundational structure that enables the appropriate level of response and recovery to an incident and potential crisis situation. The plan identifies the organization response structure and provides guidance on the activities that may occur to assess the situation, decide whether to activate the appropriate teams, escalate the situation, or decide whether to activate the Business Continuity Plans (BCP) and manage and monitor response activities throughout the life cycle of the situation. This BCP is made available to Iron Mountain employees via the Iron Mountain intranet and is tested on an annual basis. As part of the disaster recovery plan, IT Systems restoration tests are performed on at least an annual basis.

Incident Management and Monitoring

Iron Mountain's Incident Management Program was developed with a tactical and business strategy, including governance, industry standard and best practices. The program provides a framework to support successful incident response, including:

- Triage, investigate, and escalate the event to internal support resources;
- Mitigate the event and its impact;
- Coordinate notifications in compliance with legal, regulatory and contractual requirements;
- Notify appropriate insurance partners;
- Develop trending and reporting; and
- Develop processes and procedures to help prevent recurring events.

If an event may threatens the security, availability and confidentiality of personal data or customer information, it is Iron Mountain's policy that the incident is reported through established escalation protocols, which are designed to help streamline the incident reporting process and enabling Iron Mountain personnel to register vital incident information quickly, thoroughly, and efficiently about events that occurs at Iron Mountain. Once an incident is reported, the appropriate Iron Mountain team is alerted to begin researching the matter. If the incident resolution requires further action and/or changes to the system, a change request will be opened and flow through the Iron Mountain change management process. The incident is then tracked until a resolution is reached and documented within the ticket. As necessary, Iron Mountain response team members coordinate customer notifications in accordance with laws, regulations and customer agreements. Additionally, Iron Mountain personnel perform analysis to identify of trends, and develop processes and procedures to proactively prevent reoccurring events.

Iron Mountain also utilizes automated tools to monitor the production IT environment to detect events that impact the security, availability or confidentiality of data. When such events are identified, a ticket is generated and routed to the appropriate response team for triage and resolution.

On at least a quarterly basis, Iron Mountain Management meets to monitor the IT Infrastructure and Application Hosting environment, review information related to incident volume and response time, and incident breakdown's by service.

Subservice Organizations

Iron Mountain utilizes CenturyLink (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

Complementary User Entity Controls

In designing the System, Iron Mountain has contemplated that certain controls would be implemented by user entities to achieve the applicable trust services criteria supporting the System, which were communicated to user entities through the contract acceptance process. The complementary user entity controls presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities.

- 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)

Criteria and Controls

The controls that achieve the applicable trust services criteria are listed in the accompanying Description of Criteria, Controls, Tests and Results of Tests, which is considered an integral part of the Description.

Description of Criteria, Controls, Tests and Results of Tests

Controls to Meet the Trust Services Criteria

On the pages that follow, the controls to meet the applicable trust services criteria have been specified by, and are the responsibility of, Iron Mountain. The testing performed by Ernst & Young LLP and the results of tests are the responsibility of the service auditor.

The full text of the trust services criteria for the security (also referred to as 'common criteria'), availability, and confidentiality principles and are contained in tables above the testing tables for each criterion. This section describes the controls at Iron Mountain that achieve the applicable trust services criteria.

Procedures for Assessing the Completeness and Accuracy of Information Produced by the Entity (IPE)

For tests of controls requiring the use of Information Produced by the Entity (IPE), procedures were performed to assess the reliability of the information, including completeness and accuracy of the data or reports, to determine whether the information can be relied upon in the examination procedures. This includes IPE used by Iron Mountain management in performance of controls (i.e., periodic review of user listings), and IPE used in the performance of our examination procedures.

Based on the nature of the IPE, a combination of the following procedures were performed to address the completeness and accuracy of the data or reports used: (1) inspect source documentation relating to the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) agree data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing.

Criteria, Controls, Tests and Results of Tests

Common Criteria Related to Organization and Management

Criteria	Criteria Description
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, monitoring, and maintenance, of the system enabling it to meet its commitments and system requirements as they relate to security, availability, and confidentiality.
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, monitoring, maintaining, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, monitoring, and maintaining the system affecting security, availability, and confidentiality and provides resources necessary for personnel to fulfill their responsibilities.
CC1.4	The entity has established employee conduct standards, implemented employee candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security, availability, and confidentiality.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
CC1.1	Iron Mountain has defined organizational structures, reporting lines, authorities and responsibilities for employees that support the design, development, implementation, operation, maintenance and monitoring over the in-scope services provided to customers.	Inquired of Iron Mountain personnel and inspected the Iron Mountain organizational diagram to determine that Iron Mountain has defined organizational structures, reporting lines, authorities and responsibilities for employees that support the design, development, implementation, operation, maintenance and monitoring over the in-scope services provided to customers.	No deviations noted.
CC1.2	The Iron Mountain CIO and/or Information Security Group are responsible for and have defined, documented and communicated policies related to the security, availability and confidentiality of data within the	Inspected the Iron Mountain policies to determine that Iron Mountain has defined, documented and communicated policies related to the security, availability and confidentiality of data within the in-scope System and to approve exceptions to approved policies.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
	systems. Responsibilities for security, availability and confidentiality of data are assigned to Iron Mountain personnel. Exceptions to approved policies are approved by Iron Mountain management.	Inspected the following policies to determine that the policies were periodically reviewed by Iron Mountain Management: • Information Security Organization Policy • Communication and Operations Management Policy • Information Classification and Handling Policy & Procedures • Global Facility Policy • Access Control Policy • Acceptable Use Policy • Authorized Devices Policy • IT System Logging and Log Monitoring Policy • Intrusion Detection and Prevention Policy	No deviations noted.
		Inquired of Iron Mountain personnel to determine that Iron Mountain personnel, including the CIO and Information Security Group, have been assigned and were aware of responsibilities related to the security, availability and confidentiality of data.	No deviations noted.
	Documented job descriptions exist which address the security, availability, and confidentiality obligations and commitments of authorized users and are communicated at the time of hire.	For a sample of open job positions, inspected job descriptions to determine that job responsibilities and requirements are set forth by Iron Mountain and communicated during the hiring process.	No deviations noted.
CC1.3	IT Management develops Strategic Plans to align business and IT objectives as well as communicate current IT concerns and environmental changes to the business lines and to determine whether employees have the resources to fulfill their job responsibilities. This plan is presented periodically to IT personnel during meetings held by the CIO.	Inspected the semi-annual IT Strategy Meeting Minutes to determine that the CIO held meetings to align business and IT objectives, as well as communicated current IT concerns and environment changes to the business lines and whether employees have the resources to fulfill their job responsibilities.	No deviations noted.
	Management allocates finances for training events for IT personnel to attend various training events throughout the year.	Inspected the annual IT budget to determine that financial resources were allocated to training.	No deviations noted.
		Inspected the annual training course completion log to determine that employees have completed necessary training courses.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
	Documented job descriptions exist which address the security, availability, and confidentiality obligations and commitments of authorized users and are communicated at the time of hire.	For a sample of open job positions, inspected job descriptions to determine that job responsibilities and requirements are set forth by Iron Mountain and communicated during the hiring process.	No deviations noted.
	Performance assessments are performed on an annual basis for Iron Mountain employees.	For a sample of employees, inspected the performance assessment results to determine that the annual performance assessment was completed, discussed and any areas for improvement were communicated to the employee.	No deviations noted.
CC1.4	Documented procedures and job descriptions exist which address the security, availability, and confidentiality obligations and commitments of authorized internal users and are communicated and acknowledged at the time of hire.	For a sample of positions, inspected job descriptions to determine that job responsibilities and requirements are set forth by Iron Mountain and communicated during the hiring process.	No deviations noted.
		For a sample of new employees and contractors, inspected HR documentation to determine that the new employees and contractors signed and acknowledged the following Iron Mountain Policies within the appropriate timeframe in accordance with Iron Mountain policy: • IM Confidentiality Agreement • IM Code of Conduct and Business Ethics Agreement • Computer Resources - Access and Use: Acceptable Use Procedures.	Deviations noted. *Refer to deviation number 1 within the 'Results of Tests and Deviation Information' section below for further details and Management's response.*
		Inspected the IM Code of Conduct and Business Ethics Agreement and the Acceptable Use Procedures document and validated that enforcement procedures are documented within the policies that are signed by new employees and contractors.	No deviations noted.
	New employees are offered employment subject to background checks and reference validation to enable Iron Mountain to meet its commitments and requirements as they relate to security, availability, and confidentiality of data.	For a sample of new employees, inspected the background check form to determine that the employee was offered employment subject to completion of a background check and reference validation to enable Iron Mountain to meet its commitments and requirements as they relate to security, availability, and confidentiality of data.	No deviations noted.
	Performance assessments are performed on an annual basis for Iron Mountain employees.	For a sample of employees, inspected the performance assessment results to determine that the annual performance assessment was completed, discussed and any areas for improvement were communicated to the employee.	No deviations noted.

Common Criteria Related to Communication

Criteria	Criteria Description
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.
CC2.2	The entity's security, availability, and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.
CC2.4	Information necessary for designing, developing, implementing, operating, monitoring, and maintaining controls, relevant to the security, availability, and confidentiality of the system, is provided to personnel to carry out their responsibilities.
CC2.5	Internal and external users have been provided with information on how to report security, availability, and confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security, availability, and confidentiality are communicated to those users in a timely manner.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
CC2.1	Documented IT Policies exist and have been communicated to internal users, which address the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation.	Inspected the related security, availability and confidentiality policies to determine that the policies addressed the design and operation of the system and its boundaries have been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation exist and have been communicated to internal users.	No deviations noted.
	A network diagram is maintained by Iron Mountain and includes information of the boundaries of the system.	Inspected the Iron Mountain Network Diagram to determine that it includes information related to the boundaries of the system.	No deviations noted.
		Inspected the Iron Mountain Network Diagram to determine that Iron Mountain uses multiple-tiers architecture for customer-facing web applications.	No deviations noted.
	Iron Mountain has established formal contractual agreements with vendors supporting the service documenting the security, availability and confidentiality requirements for material service providers.	For a sample of vendors where signed agreements are required based upon Iron Mountain policy and procedures, inspected the Iron Mountain Vendor Agreement to determine that Iron Mountain has established a standard confidentiality agreement with its Vendors and went through a formal acceptance process, which includes signing of the agreement.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
	Iron Mountain has documented confidentiality policies, procedures, and security/availability obligations (i.e., commitments) for external users, which is communicated at the time of contract acceptance.	For a sample of new customers, inspected the Customer Agreements to determine that the security and availability commitments for external users are documented in the document and signed by the customer.	No deviations noted.
CC2.2	Documented procedures and job descriptions exist which address the security, availability, and confidentiality obligations and commitments of authorized internal users and are communicated and acknowledged at the time of hire.	For a sample of new employees and contractors, inspected HR documentation to determine that the new employees and contractors signed and acknowledged the following Iron Mountain Policies within 14 days of hire in accordance with Iron Mountain policy: • IM Confidentiality Agreement • IM Code of Conduct and Business Ethics Agreement • Computer Resources - Access and Use: Acceptable Use Procedures.	Deviations noted. *Refer to deviation number 1 within the 'Results of Tests and Deviation Information' section below for further details and Management's response.*
	Iron Mountain has established formal contractual agreements with vendors supporting the service documenting the security, availability and confidentiality requirements for material service providers.	For a sample of vendors where signed agreements are required based upon Iron Mountain policy and procedures, inspected the Iron Mountain Vendor Agreement to determine that Iron Mountain has established a standard confidentiality agreement with its Vendors and went through a formal acceptance process, which includes signing of the agreement.	No deviations noted.
	Iron Mountain has documented confidentiality policies, procedures, and security/availability obligations (i.e., commitments) for external users, which is communicated at the time of contract acceptance.	For a sample of new customers, inspected the Customer Agreements to determine that the security and availability commitments for external users are documented in the document and signed by the customer.	No deviations noted.
CC2.3	The Iron Mountain CIO and/or Information Security Group are responsible for and have defined, documented and communicated policies related to the security, availability and confidentiality of data within the systems. Responsibilities for security, availability and confidentiality of data are assigned to Iron Mountain personnel. Exceptions to approved policies are approved by Iron Mountain management.	Inspected the Iron Mountain policies to determine that Iron Mountain has defined, documented and communicated policies related to the security, availability and confidentiality of data within the in-scope System and to approve exceptions to approved policies.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
	Policies over security, availability and confidentiality are reviewed and approved by the Iron Mountain CIO and/or the Security Compliance group who have the responsibility and accountability over these policies (including making the necessary updates). Only approved policies are posted on the internal systems (e.g., Archer Tool Policy repository or the SharePoint) where they are made readily available to company personnel.	Inspected the IT Policies over the security, availability and confidentiality of the System to determine that they were reviewed and approved by the Iron Mountain CIO and/or Security Compliance group.	No deviations noted.
		Observed that only approved policies are made available on the internal systems (e.g. Archer or SharePoint).	No deviations noted.
	Documented procedures and job descriptions exist which address the security, availability, and confidentiality obligations and commitments of authorized users and are communicated and acknowledged at the time of hire.	For a sample of new employees and contractors, inspected HR documentation to determine that the new employees and contractors signed and acknowledged the following Iron Mountain Policies within 14 days of hire in accordance with Iron Mountain policy: • IM Confidentiality Agreement • IM Code of Conduct and Business Ethics Agreement • Computer Resources - Access and Use: Acceptable Use Procedures.	Deviations noted. *Refer to deviation number 1 within the 'Results of Tests and Deviation Information' section below for further details and Management's response.* .
	Iron Mountain has documented confidentiality policies, procedures, and security/availability obligations (i.e., commitments) for external users, which is communicated at the time of contract acceptance.	For a sample of new customers, inspected the Customer Agreements to determine that the security and availability commitments for external users are documented in the document and signed by the customer.	No deviations noted.
	Iron Mountain has established formal contractual agreements with vendors supporting the service documenting the security, availability and confidentiality requirements for material service providers	For a sample of vendors where signed agreements are required based upon Iron Mountain policy and procedures, inspected the Iron Mountain Vendor Agreement to determine that Iron Mountain has established a standard confidentiality agreement with its Vendors and went through a formal acceptance process, which includes signing of the agreement.	No deviations noted.
CC2.4	IT Management develops Strategic Plans to align business and IT objectives as well as communicate current IT concerns and environmental changes to the business lines.	Inspected the semi-annual IT Strategy Meeting Minutes to determine that the CIO held meetings to align business and IT objectives, as well as communicated current IT concerns and environment changes to the business lines and whether employees have the resources to fulfill their job responsibilities.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
	Policies are reviewed and approved on a regular basis by the Iron Mountain CIO and/or Information Security to help ensure that policies include appropriate requirements, commitments and updates over security availability and confidentiality. Only approved policies are posted on the internal systems (e.g., Archer Tool Policy repository or the SharePoint) where they are made readily available to company personnel.	Inspected the IT Policies over the security, availability and confidentiality of the System to determine that they were reviewed and approved by the Iron Mountain CIO and/or Security Compliance group.	No deviations noted.
		Observed that only approved policies are made available on the internal systems (e.g. Archer or SharePoint).	No deviations noted.
	Documented procedures and job descriptions exist which address the security, availability, and confidentiality obligations and commitments of authorized users and are communicated and acknowledged at the time of hire.	For a sample of new employees and contractors, inspected HR documentation to determine that the new employees and contractors signed and acknowledged the following Iron Mountain Policies within 14 days of hire in accordance with Iron Mountain policy: • IM Confidentiality Agreement • IM Code of Conduct and Business Ethics Agreement • Computer Resources - Access and Use: Acceptable Use Procedures.	Deviations noted. *Refer to deviation number 1 within the 'Results of Tests and Deviation Information' section below for further details and Management's response.*
	Management allocates finances for training events for IT personnel to attend various training events throughout the year.	Inspected the annual IT budget to determine that financial resources were allocated to training.	No deviations noted.
		Inspected the annual training course completion log to determine that employees have completed necessary training courses.	No deviations noted.
	Iron Mountain has documented confidentiality policies, procedures, and security/availability obligations (i.e., commitments) for external users, which is communicated at the time of contract acceptance.	For a sample of new customers, inspected the Customer Agreements to determine that the security and availability commitments for external users are documented in the document and signed by the customer.	No deviations noted.
CC2.5	A documented process exists for submitting, logging, identifying, and appropriately escalating security and related system availability, and confidentiality issues, breaches, or complaints. Processes are	Inspected Iron Mountain Incident Management policies and procedures to determine that a process exists for submitting, logging, identifying and escalating security, availability and/or confidentiality issues, breaches, or complaints.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
	communicated to internal users through Iron Mountain's internal sites and external users through the signed Customer Agreements.	Observed that the Iron Mountain Incident Management policies and procedures are made available to internal users of the system through the internal sites (e.g. Archer or SharePoint).	No deviations noted.
		Observed that Iron Mountain provides customers with the ability to submit questions and complaints within the Iron Mountain websites and applications.	No deviations noted.
		For a sample of customers, inspected the Customer Agreements and Customer User Guides to determine that the commitments and obligations for users are documented in the document and signed by the customer.	No deviations noted.
CC2.6	Management uses a defined systems development lifecycle (SDLC) and Change Control Process and Procedure to control when/how modifications are introduced into the enterprise and has representation at weekly change control meetings to validate success/failure of modifications in the enterprise and determine the timing of implementation. These policies and procedures, along with the method for submitting change control requests, are posted to the Corporate Intranet for access by areas affected by the process.	Inspected policies and procedures related to changes to in-scope systems to determine that they existed and included requirements around the authorization, development, testing, approval, and communication of changes.	No deviations noted.
		Observed that policies and procedures related to changes to in-scope systems are posted on the Corporate Intranet site.	No deviations noted.
	Changes to systems and/or network devices impacting end users (e.g., internal) are communicated through email indicating date, length of time, affected system, and relevant change ticket (internally specific) and/or made available to external users through release notes and alerts.	Observed that internal (e.g. Iron Mountain Employees) system users receive notification of changes to the system through email, which includes change date, length of time, affected system and change ticket.	No deviations noted.
		Observed release notes and alerts made available to external users for notification of a change that may impact the Security, Confidentiality, or Availability of the in-scope systems.	No deviations noted.

Common Criteria Related to Risk Management and Implementation of Controls

Criteria	Criteria Description
CC3.1	The entity (1) identifies potential threats that could impair system security, availability, and confidentiality commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
CC3.1	On at least an annual basis, Iron Mountain performs a risk assessment. As part of this process, threats to the System are identified and the risks from these threats are formally assessed. Processes and procedures are then revised by management, as needed.	Inspected the most recent Risk Assessment to determine that the following: • Risk assessment of the System was completed; • Threats and risks to the Security, Confidentiality or Availability of the system were identified, including risks arising from the use of vendors and customers with access to IM systems; • Environmental, regulatory, and technological changes were identified; • Identified risks and changes were analyzed for significance and potential impact to internal controls; • Risk owners were assigned for identified threats and risks; • Action plans and risk mitigation strategies were developed and documented; and • Relevant policies and procedures were updated, as necessary.	No deviations noted.
	Business continuity management and disaster recovery procedures are documented and made available through the intranet for Iron Mountain personnel.	Inspected the Business Continuity Management System (BCMS) Policy to determine that business continuity management and disaster recovery procedures are clearly documented.	No deviations noted.
		Observed that the Business Continuity Management System (BCMS) is made available through the intranet for Iron Mountain personnel.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
	IT Management develops Strategic Plans to align business and IT objectives as well as communicate current IT concerns and environmental changes to the business lines. This plan is presented periodically to IT personnel during meetings held by the CIO.	Inspected the semi-annual IT Strategy Meeting Minutes to determine that the CIO held meetings to align business and IT objectives, as well as communicated current IT concerns and environment changes to the business lines and whether employees have the resources to fulfill their job responsibilities.	No deviations noted.
	As part of the on-boarding process, Iron Mountain determines the level of risk and potential threats associated with the vendor to determine the necessary legal agreements required and level of on-going monitoring required.	For a sample of new vendors, validated that the vendor questionnaire assessment was completed to identify the appropriate risk level of the vendor and the need for on-going monitoring.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
CC3.2	Policies are reviewed and approved by the Iron Mountain CIO and/or Information Security to help ensure that policies include appropriate requirements, commitments and updates over security, availability and confidentiality. Approved policies are posted on the internal systems (e.g., Archer Tool Policy repository or the SharePoint) where they are made readily available to company personnel.	Inspected the IT Policies over the security, availability and confidentiality of the System to determine that they were reviewed and approved by the Iron Mountain CIO and/or Security Compliance group.	No deviations noted.
		Observed that only approved policies are made available on the internal systems (e.g. Archer or SharePoint).	No deviations noted.
	IT Management develops Strategic Plans to align business and IT objectives as well as communicate current IT concerns and environmental changes to the business lines and to reassess the suitability of the design and deployment of control activities.	Inspected the semi-annual IT Strategy Meeting Minutes to determine that the CIO held meetings to align business and IT objectives, as well as communicated current IT concerns and environment changes to the business lines and whether employees have the resources to fulfill their job responsibilities.	No deviations noted.
	A Third Party Risk Assessment Program has been developed that contains vendor requirements for compliance with confidentiality commitments and requirements and corrective action, if necessary.	Inspected the Vendor Risk Policies and procedure documents to determine that the policies and procedures were reviewed and approved by the Iron Mountain CIO and/or Information Security group to determine that the documents included matters related to vendor compliance requirements.	No deviations noted.
	Existing vendors are assessed periodically in accordance with Iron Mountain policy to validate whether the Vendor is in compliance with relevant Iron Mountain security, availability and confidentiality commitments and requirements.	Observed that Iron Mountain has a Third Party tool to continuously monitor medium and low risk vendors and assesses whether they need to be reclassified based on risk.	No deviations noted.
		For a sample of vendors classified as high risk by Iron Mountain management, inspected the annual review of high risk vendors to validate Vendors are in compliance with relevant Iron Mountain security, availability, and confidentiality commitments and requirements.	No deviations noted.

Common Criteria Related to Monitoring of Controls

Criteria	Criteria Description
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security, availability, and confidentiality, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
CC4.1	Network and host-based vulnerability assessments, which includes determining whether IP addresses and names are not displayed on server banners, are performed by a Third Party on a quarterly basis and identified risks are communicated and resolved accordingly.	For a sample of quarters, inspected supporting documentation to determine that a vulnerability assessment was performed and identified risks were communicated and resolved accordingly to remain consistent with system commitments and requirements as they relate to security, availability and confidentiality.	No deviations noted.
		For a sample of quarters, inspected the supporting documentation to determine that the vulnerability assessment included determining whether IP address and names are not displayed on server banners.	No deviations noted.
	Iron Mountain engages a third-party vendor to perform an annual penetration test to help identify potential risks and vulnerabilities to the customer-facing web applications and infrastructure.	Inquired of Iron Mountain management to determine that the penetration test is performed on an annual basis.	No deviations noted.
		For the most recent annual penetration test, inspected the supporting documentation to determine that the test included the following components: • Cross Site Scripting (XSS) • Injection Flaws • Remote File Inclusion/ Command Injection • Insecure Direct Object Reference • Cross Site Request Forgery (CSRF) • Information Leakage and Improper Error Handling • Broken Authentication and Session Management • Insecure Cryptographic Storage • Insecure Communications • Allow directory transversal	No deviations noted.
	Iron Mountain utilizes periodic meetings with management and scorecards to monitor the IT Infrastructure and Application Hosting environment and to assess the environment against security, availability, and confidentiality commitments and requirements.	Inspected supporting documentation to determine that periodic management meetings were held to discuss and scorecards were used to monitor the IT Infrastructure and Application Hosting environment and to assess the environment against security, availability, and confidentiality commitments and requirements.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
		For a sample of quarters, inspected the meeting minutes CIO scorecard to determine that the meeting was held, that scorecard was created and that the scorecard contained incident volume and resolution.	No deviations noted.
	A Security Information and Event Management (SIEM) tool is installed to log and monitor suspicious activity. Access to the SIEM tool is limited to authorized and appropriate personnel.	Inquired of Iron Mountain Management to determine that the centralized log system is in place for logging and monitoring of suspicious activities.	No deviations noted.
		Observed that the SIEM tool is in place and actively monitoring servers within the production environment real-time and that activity logs are stored within the system.	No deviations noted.
		Inspected the system generated listing of users with access to the SIEM tool to determine that access is limited to authorized and appropriate individuals.	No deviations noted.
		Observed that the SIEM tool is configured to alert Iron Mountain personnel when suspicious activity is detected.	No deviations noted.

Common Criteria Related to Logical and Physical Access Controls

Criteria	Criteria Description
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.
CC5.6	Logical access security measures have been implemented to protect against unauthorized security, availability, and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security, availability, and confidentiality.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
CC5.1	Logical access to IT computing resources is appropriately restricted by the implementation of individual identification, authentication, and authorization mechanisms.	Inspected the related security, availability and confidentiality policies to determine that procedures exist to restrict access to confidential information.	No deviations noted.
		Observed that users first authenticate through Active Directory to gain access to the in-scope systems.	No deviations noted.
	Customers are restricted to their own production environment through the use of username and password authentication.	Observed an Iron Mountain associate login with a test customer user ID and password to determine access was restricted to the respective customer's information.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
	Network (Active Directory) passwords comply with Iron Mountain security requirements, including password complexity and forced password change upon initial login.	Inspected the Active Directory password configuration to determine that passwords comply with Iron Mountain security requirements, including password complexity and forced password change upon initial login.	No deviations noted.
	Non-display passwords are used for web-based Iron Mountain applications to help restrict system access to authorized personnel.	Observed that non-display passwords are used for Iron Mountain web-based applications.	No deviations noted.
	Iron Mountain secures the transmission of private and confidential data to its internal and external facing networks through the use of encryption (at least 256-bit) via VPN and SSL encryption respectively.	Inspected the VPN connection configuration to determine that encryption (at least 256-bit) is used.	No deviations noted.
		For a sample transmission, inspected the transmission file to determine that SSL encryption is used.	No deviations noted.
	Build Checklists are used for each new Windows and UNIX server install to help ensure systems put into production meet the minimum standards for ensuring appropriate operating system level security.	For a sample of new Windows and UNIX servers, inspected the Build Checklists to determine that the servers put to into production meet minimum standards for ensuring appropriate operating system level security.	No deviations noted.
		For a sample of existing Windows and UNIX servers, inspected the OS and DB security settings to determine that the servers were configured in accordance with Iron Mountain's standards.	No deviations noted.
	A Security Information and Event Management (SIEM) tool is installed to log and monitor suspicious and unauthorized activity. Access to the SIEM tool is limited to authorized and appropriate personnel.	Inquired of Iron Mountain Management to determine that the centralized log system is in place for logging and monitoring of suspicious and unauthorized activities.	No deviations noted.
		Observed that the SIEM tool is in place and actively monitoring servers within the production environment real-time and that activity logs are stored within the system.	No deviations noted.
		Inspected the system generated listing of users with access to the SIEM tool to determine that access is limited to authorized and appropriate individuals.	No deviations noted.
		Observed that the SIEM tool is configured to alert Iron Mountain personnel when suspicious activity is detected.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
CC5.2	Individual accounts (including privileged access) to the in-scope systems are added and/or modified in a timely manner and require approval by the authorizing manager. Access rights are granted in accordance with the request and appropriate for the individual's job responsibilities.	For a sample of users granted/modified access to the in-scope systems, inspected the access requests to determine that the requests were appropriately documented and approved and that access was provisioned in accordance with the request.	No deviations noted.
		For a sample of users granted access to the in-scope production systems, inspected the access granted and inquired of Management to determine that the access is appropriate based upon the individuals' job responsibilities.	No deviations noted.
	Individual accounts on the in-scope systems are inactivated/deleted by IT in a timely manner upon notification from HR.	For a sample of terminated users, inspected user listings from the in-scope systems to determine that accounts were inactivated or deleted in a timely manner following termination.	Deviations noted. *Refer to deviation number 3 within the 'Results of Tests and Deviation Information' section below for further details and Management's response.*
CC5.3	Logical access to IT computing resources is appropriately restricted by the implementation of individual identification, authentication, and authorization mechanisms.	Inspected the related security, availability, and confidentiality policies to determine that procedures exist to restrict access to confidential information.	No deviations noted.
		Observed that users first authenticate through the Windows Domain to gain access to the in-scope systems.	No deviations noted.
	Customers are restricted to their own production environment through the use of username and password authentication.	Observed an Iron Mountain associate login with a test customer user ID and password to determine access was restricted to the respective customer's information.	No deviations noted.
CC5.4	Individual accounts on the in-scope systems are inactivated/deleted by IT in a timely manner upon notification from HR.	For a sample of terminated users, inspected user listings from the in-scope systems to determine that accounts were inactivated or deleted in a timely manner following termination.	Deviations noted. *Refer to deviation number 3 within the 'Results of Tests and Deviation Information' section below for further details and Management's response.*
	IT management reviews and revalidates privileged accounts to the in-scope applications at least quarterly.	For a sample of quarters, inspected evidence to determine that the review and revalidation of privileged access to the in-scope applications was completed.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
	Access to the RADIUS server is restricted through the use of two-factor authentication.	Observed a user access the RADIUS server to determine that access to the RADIUS server is restricted through the use of two-factor authentication.	No deviations noted.
CC5.5	A documented procedure exists to restrict physical access to the data centers and offline storage media (including backup tapes and storage arrays) via access card. A list of personnel with access to the data center facilities are reviewed by the Data Center Manager quarterly.	Inspected the Data Center Physical Security policy to determine that a policy exist to control physical access to the data centers and offline storage media.	No deviations noted.
		Observed that access to the Iron Mountain production data centers and offline storage media is restricted via access card.	No deviations noted.
		For a sample of quarters, inspected the Data Center Access Reviews to determine that physical access to the data centers was reviewed on a quarterly basis.	No deviations noted.
	Access to the in-scope data centers and surrounding facilities and sensitive areas within the facilities is restricted through the use of badge scanners.	Observed that access to the in-scope data centers and surrounding facilities and sensitive areas within the facilities is restricted through the use of badge scanners.	No deviations noted.
	Access to the in-scope data centers and surrounding facilities is approved by authorized individuals.	For a sample of access requests to the in-scope data centers and surrounding facilities, inspected the access request documentation to determine that the access request was approved by authorized individual.	Deviation noted. *Refer to deviation number 2 within the 'Results of Tests and Deviation Information' section below for further details and Management's response.*
	Employee access to the in-scope data centers and surrounding facilities is removed upon termination.	For a sample of terminated employees, inspected the system generated access listings for the in-scope data centers and surrounding facilities to determine that access was revoked upon termination.	No deviations noted.
	Visitors to the in-scope data centers and surrounding facilities are required to present a government issued ID, sign the visitor log, are issued a guest badge and are escorted by Iron Mountain personnel.	Observed that visitors to the in-scope data centers and surrounding facilities are required to present a government issued ID, sign the visitor log, issued a guest badge and escorted by Iron Mountain personnel.	No deviations noted.
	A 24 hour, 7 days a week security guard presence is established to monitor, detect and follow-up on unauthorized activity at the facility.	Inquired of Iron Mountain Management to determine that a 24 hour, 7 days a week security guard is present to monitor, detect and follow-up on unauthorized activity at the facility.	No deviations noted.
	Surveillance cameras have	Observed that a security guard is present at the facility.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
	been positioned at key locations both inside and outside surrounding facilities.	Observed that surveillance cameras have been positioned at key locations both inside and outside surrounding facilities.	No deviations noted.
	Hardware stored within the in-scope data centers is physically restricted based on Iron Mountain and customer requirements.	Observed that hardware stored within the in-scope data centers is physically restricted in accordance with Iron Mountain and Customer requirements.	No deviations noted.
	Access to the in-scope data centers is monitored by surveillance cameras that have been positioned at key entry and exit points of the data centers.	Observed that access to the in-scope data centers is monitored by surveillance cameras that have been positioned at key entry and exit points of the data centers.	No deviations noted.
	Physical access to the in-scope data centers and surrounding facilities is reviewed and approved by management on a quarterly basis. Exceptions are documented and resolved.	For a sample of quarters, inspected the quarterly review documentation to determine that access to in-scope data centers and surrounding facilities was reviewed and approved by management and exceptions were documented and resolved.	No deviations noted.
	The security system responsible for the administration of access cards for the Iron Mountain datacenters is located within a locked room.	Observed that the security system responsible for the administration of access cards for data centers is located within a locked room.	No deviations noted.
	Iron Mountain maintains oversight of the CenturyLink co-location by obtaining and reviewing independent attestation reports, performing periodic visits and restricting to the ability to request access to colocation space at CenturyLink to authorized and appropriate individuals.	Inspected evidence of Iron Mountain Management's most recent review of the CenturyLink attestation report to determine that management reviewed the attestation report and evaluated whether the controls described within the report are effective and are sufficient to confirm with the applicable Trust Services criteria and are applicable to the CenturyLink data centers supporting the system.	No deviations noted.
		Inquired of Iron Mountain Management and noted that Iron Mountain performs regular site visits to CenturyLink to confirm existence of and adherence with the adequacy of the physical controls (i.e., locked cage, secure access).	No deviations noted.
		Inspected a system generated listing of individuals with the ability to request access to CenturyLink co-location space to determine the ability to request access is limited to authorized and appropriate Iron Mountain individuals.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
CC5.6	An Intrusion Detection system is in place over critical network points and monitored for unusual activity within or against the Iron Mountain Network.	Inspected the IT Infrastructure Diagram to determine that IDS agents are located at the network entry points between firewalls and routers.	No deviations noted.
		For a sample of alerts, including IDS alerts, inspected supporting documentation to determine that unusual activity is monitored, documented, reviewed and remediated in a timely manner.	No deviations noted.
		Inspected the IDS systems to determine that the tool is configured to send log to the centralized SIEM tool for monitoring.	No deviations noted.
	Firewalls are implemented at externally facing networks points to help prevent unauthorized network access and data leakage. Administration over the firewalls is restricted to authorized Iron Mountain personnel.	Inspected the IT Infrastructure Diagram to determine that externally facing firewalls are in place.	No deviations noted.
		Inspected the system user listings within the firewall management console to determine that privileged access to firewall devices is restricted to appropriate and authorized Iron Mountain personnel.	No deviations noted.
		Inspected the firewall management console to determine that the following settings are in place to help prevent unauthorized network access and data leakage: • Split tunneling is disabled • Web filtering is enabled to help restrict the access to external email or messaging sites	No deviations noted.
	Firewall rulesets are monitored by FireMON and any changes to the rulesets, including port usage, are approved.	Observed that FireMON is used for monitoring and reviewing the firewall rulesets.	No deviations noted.
		Inquired of Iron Mountain management and observed the process for approving changes to the firewall rulesets, including port usage.	No deviations noted.
	Logical access to IT computing resources is appropriately restricted by the implementation of individual identification, authentication, and authorization mechanisms.	Inspected the related security, availability, and confidentiality policies to determine that procedures exist to restrict access to confidential information.	No deviations noted.
		Observed that users first authenticate through the Windows Domain to gain access to the in-scope systems.	No deviations noted.
	Remote desktop connection is restricted to authorized personnel.	Observed a remote desktop connection to determine that the remote connection is limited to authorized personnel.	No deviations noted.
	Iron Mountain secures the transmission of private and confidential data to its internal	Inspected the VPN connection configuration to determine that encryption (at least 256-bit) is used.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
	and external facing networks through the use of encryption (at least 256-bit) via VPN and SSL encryption respectively.	For a sample transmission, inspected the transmission file to determine that SSL encryption is used.	No deviations noted.
CC5.7	Backups are encrypted prior to being sent offsite to restrict access to data.	Observed that production backups are encrypted prior to being sent offsite.	No deviations noted.
	Iron Mountain secures the transmission of private and confidential data to its internal and external facing networks through the use of encryption (at least 256-bit) via VPN and SSL encryption respectively.	Inspected the VPN connection configuration to determine that 3DES encryption (256-bit) is used.	No deviations noted.
		For a sample transmission, inspected the transmission file to determine that SSL encryption is used.	No deviations noted.
CC5.8	Build Checklists are used for each new Windows and UNIX server install to help ensure systems put into production meet the minimum standards for ensuring appropriate operating system level security.	For a sample of new Windows and UNIX servers, inspected the Build Checklists to determine that the servers put to into production meet minimum standards for ensuring appropriate operating system level security.	No deviations noted.
		For a sample of existing Windows and UNIX servers, inspected the OS and DB security settings to determine that the servers were configured in accordance with Iron Mountain's standards.	No deviations noted.
	Anti-virus is installed and configured on applicable servers for automatic virus definition and scan engine updates, unless exempted by Management.	For a sample of in-scope systems, inspected anti-virus tools configurations to determine that anti-virus has been configured to automatically install virus definition and scan engine updates, unless exempted by Management.	No deviations noted.

Common Criteria Related to System Operations

Criteria	Criteria Description
CC6.1	Vulnerabilities of system components to security, availability, and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.
CC6.2	Security, availability, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
CC6.1	An Intrusion Detection system is in place over critical network points and monitored for unusual activity within or against the Iron Mountain Network.	Inspected the IT Infrastructure Diagram to determine that IDS agents are located at the network entry points between firewalls and routers.	No deviations noted.
		For a sample of alerts, including IDS alerts, inspected supporting documentation to determine that unusual activity is monitored, documented, reviewed and remediated in a timely manner.	No deviations noted.
	Operations support personnel monitor operating systems and databases for availability and system uptime statistics.	Observed that operations personnel monitor operating systems and databases for availability and system uptime statistics through a monitoring tool.	No deviations noted.
		For a sample of servers, inspected the server configurations to determine that monitoring tools are installed to actively monitor the server for availability and system uptime statistics.	No deviations noted.
	Anti-virus is installed and configured on applicable servers for automatic virus definition and scan engine updates, unless exempted by Management.	For a sample of in-scope systems, inspected anti-virus tools configurations to determine that anti-virus has been configured to automatically install virus definition and scan engine updates, unless exempted by Management.	No deviations noted.
	Iron Mountain engages a third-party vendor to perform an annual penetration test to help	Inquired of Iron Mountain management to determine that the penetration test is performed on an annual basis.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
	identify potential risks and vulnerabilities to the customer-facing web applications and infrastructure.	For the most recent annual penetration test, inspected the supporting documentation to determine that the test included the following components: • Cross Site Scripting (XSS) • Injection Flaws • Remote File Inclusion/ Command Injection • Insecure Direct Object Reference • Cross Site Request Forgery (CSRF) • Information Leakage and Improper Error Handling • Broken Authentication and Session Management • Insecure Cryptographic Storage • Insecure Communications • Allow directory transversal	No deviations noted.
CC6.2	A documented process exists for submitting, logging, identifying, and appropriately escalating security and related system availability, and confidentiality issues, breaches, or complaints. Processes are communicated to internal users through Iron Mountain's internal sites and external users through the signed Customer Agreements.	Inspected Iron Mountain Incident Management policies and procedures to determine that a process exists for submitting, logging, identifying and escalating security and/or confidentiality issues, breaches, or complaints.	No deviations noted.
		Observed that the Iron Mountain Incident Management policies and procedures are made available to internal users of the system through the internal sites (e.g. Archer or SharePoint).	No deviations noted.
		Observed that Iron Mountain provides customers with the ability to submit questions and complaints within the Iron Mountain websites and applications.	No deviations noted.
		For a sample of customers, inspected the Customer Agreements and Customer User Guides to determine that the commitments and obligations for users are documented in the document and signed by the customer.	No deviations noted.
	Production incidents impacting the security, availability or confidentiality of the system are documented, researched and resolved in accordance with Iron Mountain's Incident Management Policy.	For a sample of production incidents, inspected documentation to determine that the incident was documented, researched and resolved in accordance with Iron Mountain's Incident Management Policy.	No deviations noted.

Common Criteria Related to Change Management

Criteria	Criteria Description
CC7.1	The entity's commitments and system requirements, as they relate to security, availability, and confidentiality, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security, availability, and confidentiality.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security, availability, and confidentiality commitments and requirements.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
CC7.1	.Management uses a defined systems development life cycle (SDLC) and Change Control Process and Procedure to address security, availability and confidentiality commitments and requirements during the development, acquisition, implementation and maintenance of information systems. These policies and procedures are posted to the Corporate Intranet for access by all areas affected by the process.	Inspected policies and procedures related to changes to in-scope systems to determine that they existed and included requirements around the authorization, development, testing, approval, and communication of changes.	No deviations noted.
		Observed that policies and procedures related to changes to in-scope systems are posted on the Corporate Intranet site.	No deviations noted.
	Changes are appropriately approved by the Change Approval Board and the impact on the security, availability or confidentiality of data within the system is assessed before being migrated to production.	For a sample of changes performed to the in-scope systems, inspected the change request tickets to determine that the changes were approved by the Change Approval Board and the impact on the security the security, availability or confidentiality of data within the system was assessed prior to deployment in production.	No deviations noted.
CC7.2	Build Checklists are used for each new Windows and UNIX server install to help ensure systems put into production meet the minimum standards for ensuring appropriate operating system level security.	For a sample of new Windows and UNIX servers, inspected the Build Checklists to determine that the servers put to into production meet minimum standards for ensuring appropriate operating system level security.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
	Policies are reviewed and approved by the Iron Mountain CIO and/or the Information Security Group to help ensure that policies include appropriate requirements, commitment and updates over security, availability and confidentiality. Only approved policies are posted on the internal systems (e.g., Archer Tool Policy repository or the SharePoint) where they are made readily available to company personnel.	Inspected the IT Policies over the security, availability and confidentiality of the System to determine that they were reviewed and approved by the Iron Mountain CIO and/or Security Compliance group.	No deviations noted.
		Observed that only approved policies are made available on the internal systems (e.g. Archer or SharePoint).	No deviations noted.
	Changes to the in-scope systems are documented within a Change Request.	For a sample of changes to the in-scope systems, inspected the Change Request to determine that the change to the system was documented.	No deviations noted.
	Network and host-based vulnerability assessments are performed by a Third Party on a quarterly basis and identified risks are communicated and resolved accordingly to remain consistent with system commitments and requirements as they relate to security, availability and confidentiality.	For a sample of quarters, inspected vulnerability assessment documentation to determine that a vulnerability assessment was performed and identified risks are communicated and resolved accordingly to remain consistent with system commitments and requirements as they relate to security, availability and confidentiality.	No deviations noted.
CC7.3	A documented process exists for submitting, logging, identifying, and appropriately escalating security and related system availability, and confidentiality issues, breaches, or complaints. Processes are communicated to internal users through Iron Mountain's internal sites and external users through the signed Customer Agreements.	Inspected Iron Mountain Incident Management policies and procedures to determine that a process exists for submitting, logging, identifying and escalating security, availability and/or confidentiality issues, breaches, or complaints.	No deviations noted.
	Network and host-based vulnerability assessments are performed by a Third Party on a quarterly basis and identified risks are communicated and resolved accordingly to remain consistent with system commitments and requirements as they relate to security, availability and confidentiality.	For a sample of quarters, inspected vulnerability assessment documentation to determine that a vulnerability assessment was performed and identified risks are communicated and resolved accordingly to remain consistent with system commitments and requirements as they relate to security, availability and confidentiality.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
CC7.4	Change requests affecting the in-scope systems are authorized by the change control administrators within the enterprise wide application Service Center.	For a sample of changes performed to the in-scope systems, inspected the change request tickets and email communications to determine that the changes were appropriately authorized by the change control administrators.	No deviations noted.
	Changes to the in-scope systems are tested (where applicable) prior to deployment in production.	For a sample of changes to the in-scope systems, inspected change request tickets and system evidence to validate the change was tested (where applicable) prior to deployment in production.	No deviations noted.
	For changes to the in-scope systems, development work is performed in a separate environment from production and development and test environments are separate from the in-scope systems.	Inspected the server listing and inquired of Iron Mountain Management to determine that separate development, testing, and in-scope systems exist.	No deviations noted.
	Emergency changes follow the standard change management procedures which include formal documentation and proper authorization.	For a sample of emergency changes performed to the in-scope systems, inspected the change request tickets to determine that the emergency change followed the standard change management procedures with supporting documentation and authorization by IT Management within the change request ticket.	No deviations noted.
	Changes are appropriately approved by the Change Approval Board and the impact on system availability, confidentiality and security is assessed before being migrated to production.	For a sample of changes performed to the in-scope systems, inspected the change request tickets to determine that the changes were approved by the Change Approval Board and the impact on system availability, confidentiality and security was assessed prior to deployment in production.	No deviations noted.

Additional Criteria for Availability

Criteria	Criteria Description
A1.1	Current processing capacity and usage are monitored, maintained, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
A1.1	IT Management develops Strategic Plans to align business and IT objectives as well as communicate current IT concerns and whether current processing capacity is sufficient to meet the availability commitments and requirements.	Inspected the semi-annual IT Strategy Meeting Minutes to determine that the CIO held meetings to align business and IT objectives, as well as communicated current IT concerns and environment changes to the business lines and whether employees have the resources to fulfill their job responsibilities.	No deviations noted.
	Iron Mountain utilizes periodic meetings with management and scorecards to monitor the IT Infrastructure and Application Hosting environment.	Inspected supporting documentation to determine that management meetings were held to discuss and reviewed incidents.	No deviations noted.
		For a sample of quarters, inspected the CIO scorecard to determine that it contained incident volume and resolution.	No deviations noted.
	Operations support personnel monitor operating systems and databases for availability and system uptime statistics.	Observed that operations personnel monitor operating systems and databases for availability and system uptime statistics through a monitoring tool.	No deviations noted.
		For a sample of servers, inspected the server configurations to determine that monitoring tools are installed to actively monitor the server for availability and system uptime statistics.	No deviations noted.
		For a sample usage alert, inspected the incident ticket to determine that the incident was researched in accordance with Iron Mountain's Incident Management Policy.	No deviations noted.
		For a sample of production incidents, inspected documentation to determine that the incident was documented, researched and resolved in accordance with Iron Mountain's Incident Management Policy.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
A1.2	Environmental systems exist and are monitored in the Iron Mountain data centers which control temperature, humidity and detect fire and water.	Observed that environmental systems exist and are monitored in the Iron Mountain data centers which control temperature, humidity and detect fire and water.	No deviations noted.
	Maintenance agreements (system specific) are in place over the environmental systems within the Iron Mountain data centers to review/check these systems on a defined frequency (e.g., Annual, monthly, quarterly).	For a sample of environmental systems within the Iron Mountain data centers, inspected maintenance agreements and reports to determine that maintenance was performed over environmental systems based on a defined frequency (e.g. Annual, monthly, quarterly).	No deviations noted.
	Redundant network devices and authentication server are installed to provide ongoing availability of the System.	Inspected the network device and authentication server configurations to determine that redundant network devices are installed.	No deviations noted.
	Iron Mountain maintains oversight of the CenturyLink co-location by obtaining and reviewing independent attestation reports, performing periodic visits and restricting to the ability to request access to colocation space at CenturyLink to authorized and appropriate individuals.	Inspected evidence of Iron Mountain Management's most recent review of the CenturyLink attestation report to determine that management reviewed the attestation report and evaluated whether the controls described within the report are effective and are sufficient to confirm with the applicable Trust Services criteria and are applicable to the CenturyLink data centers supporting the system.	No deviations noted.
		Inquired of management and noted that Iron Mountain performs regular site visits to CenturyLink to confirm existence of and adherence with the adequacy of the physical controls (i.e., locked cage, secure access) and environmental safeguards.	No deviations noted.
	Backup procedures, including escalation procedures, are documented and made available through the intranet for Iron Mountain personnel.	Inspected the Iron Mountain backup procedures to determine that the backup procedures include escalation procedures and are documented and include escalation procedures.	No deviations noted.
		Observed that the backup procedures are made available to Iron Mountain personnel through the intranet.	No deviations noted.
	Production data is backed up on a nightly basis (unless otherwise agreed to with the system owner) and sent to an alternate (offsite) location on a daily basis.	For a sample of production servers, inspected the system backup schedule to determine that the production server was configured to be backed up on a nightly basis, unless a documented exception exists.	No deviations noted.
		For a sample of servers and a sample of days, inspected system generated backup logs to determine that production data is backed up on a nightly basis.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
		For a sample of months, inspected the backup monitoring scorecard to determine that management monitored the backup process and successful completion percentage.	No deviations noted.
		Inspected available CommVault documentation and inquired of Iron Mountain Management to determine that jobs will not be written to tape prior to successfully completing.	No deviations noted.
		For a sample of days, inspected the offsite rotation logs to determine that backup tapes were rotated to an alternate location.	No deviations noted.
	The ability to add, modify and delete backup job schedules is limited to authorized Iron Mountain personnel.	Inspected the system generated user listing to determine that the ability to add, modify and delete backup job schedules is limited to authorized Iron Mountain personnel.	No deviations noted.
	Operations maintain an up-to-date backup tape inventory, within the CommVault tool, of tapes stored both on and off-site.	Observed that Operations maintains an up-to-date backup tape inventory, within the CommVault tool, of tapes stored both on and off-site.	No deviations noted.
	A documented process exists for submitting, logging, identifying, and appropriately escalating security and related system availability, and confidentiality issues, breaches, or complaints. Processes are communicated to internal users through Iron Mountain's internal sites and external users through the signed Customer Agreements.	Inspected Iron Mountain Incident Management policies and procedures to determine that a process exists for submitting, logging, identifying and escalating security and/or confidentiality issues, breaches or complaints.	No deviations noted.
		Observed that the Iron Mountain Incident Management policies and procedures are made available to internal users of the system through the internal sites (e.g. Archer or SharePoint).	No deviations noted.
		Observed that Iron Mountain provides customers with the ability to submit questions and complaints within the Iron Mountain websites and applications.	No deviations noted.
		For a sample of customers, inspected the Customer Agreements and Customer User Guides to determine that the commitments and obligations for users are documented in the document and signed by the customer.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
A1.3	Business continuity management and disaster recovery procedures are documented and made available through the intranet for Iron Mountain personnel.	Inspected the Business Continuity Management System (BCMS) Policy to determine that business continuity management and disaster recovery procedures are clearly documented and included the following attributes: a. Testing procedures b. business impact analysis c. application inbound and outbound interfaces d. staff call trees e. total facility outage f. other regional alternative work arrangements g. business and technology dependency solutions h. recovery teams roles and responsibilities i. restoration procedures j. procedures detailing how backlog work and lost data will be recovered k. client contacts l. offsite locations of plan m. process description and recovery time objective classification n. recovery strategy o. evacuation procedures	No deviations noted.
		Observed that the Business Continuity Management System (BCMS) is made available through the intranet for Iron Mountain personnel.	No deviations noted.
	Backup tapes are restored and tested annually as part of Iron Mountain's Disaster Recovery testing to determine the effectiveness of the backup process.	Inspected evidence of the most recent restoration test to determine that backup tapes are restored and tested annually as part of Iron Mountain's Disaster Recovery testing to determine the effectiveness of the backup process.	No deviations noted.

Additional Criteria for Confidentiality

Criteria	Criteria Description
C1.1	Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.
C1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.
C1.3	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.
C1.4	The entity obtains confidentiality commitments that are consistent with the entity's confidentiality requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.
C1.5	Compliance with the entity's confidentiality commitments and system requirements by vendors and others third parties whose products and services are part of the system is assessed on a periodic and as-needed basis and corrective action is taken, if necessary.
C1.6	Changes to the entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.
C1.7	The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.
C1.8	The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
C1.1	Iron Mountain classifies data within the in-scope systems in accordance with defined requirements and policies.	Inspected the Iron Mountain Information Security Policies and inquired of management to determine that procedures exist to classify data within the in-scope systems in accordance with defined requirements and policies.	No deviations noted.
	Information designated as confidential is not stored, processed, or maintained in test or development systems.	Inspected the Iron Mountain Global Communications Policy to determine that procedures are in place prohibiting the use of production data in the test and development environments.	No deviations noted.
		Inquired of Management to determine that information designated as confidential is not stored, processed, or maintained in test or development systems.	No deviations noted.
	For changes to the in-scope systems, development work is performed in a separate environment from production and development and test environments are separate from the in-scope systems.	Inspected the server listing and inquired of Iron Mountain Management to determine that separate development, testing, and in-scope systems exist.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
C1.2	Logical access to IT computing resources is appropriately restricted by the implementation of individual identification, authentication, and authorization mechanisms. Logical Access Procedures have been established to address these elements (as defined within the criteria).	Inspected the related security, availability, and confidentiality policies to determine that procedures exist to restrict access to confidential information.	No deviations noted.
		Observed that users first authenticate through the Windows Domain to gain access to the in-scope systems.	No deviations noted.
	Iron Mountain secures workstations through the use of a standard build prior to distributing to the end-users in order to help reduce the risk of data leakage.	Observed that Iron Mountain IT utilizes a global build for employee workstations.	No deviations noted.
		Inspected the standard workstation configuration to determine that full disk encryption is used and the use of removable media is disabled.	No deviations noted.
	An Intrusion Detection system is in place over critical network points and monitored for unusual activity within or against the Iron Mountain Network.	Inspected the IT Infrastructure Diagram to determine that IDS agents are located at the network entry points between firewalls and routers.	No deviations noted.
		For a sample of alerts, including IDS alerts, inspected supporting documentation to determine that unusual activity is monitored, documented, reviewed and remediated in a timely manner.	No deviations noted.
	Customers are restricted to their own production environment through the use of username and password authentication.	Observed an Iron Mountain associate login with a test customer user ID and password to determine access was restricted to the respective customer's information.	No deviations noted.
	Iron Mountain secures the transmission of private and confidential data to its internal and external facing networks through the use of encryption (at least 256-bit) via VPN and SSL encryption respectively.	Inspected the VPN connection configuration to determine that encryption (at least 256-bit) is used.	No deviations noted.
		For a sample transmission, inspected the transmission file to determine that SSL encryption is used.	No deviations noted.
	Backups are encrypted prior to being sent offsite to restrict access to data.	Observed that database server backups are encrypted prior to being written to tape and sent offsite.	No deviations noted.
	Iron Mountain classifies data within the in-scope systems in accordance with defined requirements and policies.	Inspected the Iron Mountain Information Security Policies and inquired of management to determine that procedures exist to classify data within the in-scope systems in accordance with defined requirements and policies.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
C1.3	Iron Mountain has documented confidentiality policies, procedures, and security/availability obligations (i.e., commitments) for external users, which is communicated at the time of contract acceptance.	For a sample of new customers, inspected the Customer Agreements to determine that the security and availability commitments for external users are documented in the document and signed by the customer.	No deviations noted.
	Customers are restricted to their own production environment through the use of username and password authentication.	Observed an Iron Mountain associate login with a test customer user ID and password to determine access was restricted to the respective customer's information.	No deviations noted.
	Iron Mountain secures the transmission of private and confidential data to its internal and external facing networks through the use of encryption (at least 256-bit) via VPN and SSL encryption respectively.	Inspected the VPN connection configuration to determine that encryption (at least 256-bit) is used.	No deviations noted.
		For a sample transmission, inspected the transmission file to determine that SSL encryption is used.	No deviations noted.
	Backups are encrypted prior to being sent offsite to restrict access to data.	Observed that database server backups are encrypted prior to being written to tape and sent offsite.	No deviations noted.
C1.4	Iron Mountain has established formal contractual agreements with vendors supporting the service documenting the security, availability and confidentiality requirements for material service providers.	For a sample of vendors where signed agreements are required based upon Iron Mountain policy and procedures, inspected the Iron Mountain Vendor Agreement to determine that Iron Mountain has established a standard confidentiality agreement with its Vendors and went through a formal acceptance process, which includes signing of the agreement.	No deviations noted.
C1.5	Iron Mountain maintains oversight of the CenturyLink co-location by obtaining and reviewing independent attestation reports, performing periodic visits and restricting to the ability to request access to colocation space at CenturyLink to authorized and appropriate individuals.	Inspected evidence of Iron Mountain Management's most recent review of the CenturyLink attestation report to determine that management reviewed the attestation report and evaluated whether the controls described within the report are effective and are sufficient to confirm with the applicable Trust Services criteria and are applicable to the CenturyLink data centers supporting the system.	No deviations noted.
		Inquired of management and noted that Iron Mountain performs regular site visits to CenturyLink to confirm existence of and adherence with the adequacy of the physical controls (i.e., locked cage, secure access).	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
		Inspected a system generated listing of individuals with the ability to request access to CenturyLink co location space to determine the ability to request access is limited to authorized and appropriate Iron Mountain individuals.	No deviations noted.
	Iron Mountain has established formal contractual agreements with vendors supporting the service documenting the security, availability and confidentiality requirements for material service providers.	For a sample of vendors where signed agreements are required based upon Iron Mountain policy and procedures, inspected the Iron Mountain Vendor Agreement to determine that Iron Mountain has established a standard confidentiality agreement with its Vendors and went through a formal acceptance process, which includes signing of the agreement.	No deviations noted.
		Inquired of Iron Mountain Management to determine that amendments would be made to existing contractual agreements should Iron Mountain's confidentiality requirements change.	No deviations noted.
C1.6	Iron Mountain communicates security, availability and confidentiality commitments and obligations to internal users through documented policies, procedures and acknowledgement forms that employees sign-off on as part of the hiring process.	For a sample of new employees and contractors, inspected HR documentation to determine that the new employees and contractors signed and acknowledged the following Iron Mountain Policies, which communicated their security, availability and confidentiality commitments and obligations, within 14 days of hire in accordance with Iron Mountain policy: • IM Confidentiality Agreement • IM Code of Conduct and Business Ethics Agreement • Computer Resources - Access and Use: Acceptable Use Procedures.	Deviations noted. *Refer to deviation number 1 within the 'Results of Tests and Deviation Information' section below for further details.*
	Iron Mountain has established formal contractual agreements with vendors supporting the service documenting the security, availability and confidentiality requirements for material service providers	For a sample of vendors where signed agreements are required based upon Iron Mountain policy and procedures, inspected the Iron Mountain Vendor Agreement to determine that Iron Mountain has established a standard confidentiality agreement with its Vendors and went through a formal acceptance process, which includes signing of the agreement.	No deviations noted.
C1.7	Iron Mountain classifies data within the in-scope systems in accordance with defined requirements and policies.	Inspected the Iron Mountain Information Security Policies and inquired of management to determine that procedures exist to classify data within the in-scope systems in accordance with defined requirements and policies.	No deviations noted.

Criteria	Controls specified by Iron Mountain	Testing performed	Results of testing
	Iron Mountain has established processes and procedures to help validate that electronic customer confidential information is retained in accordance with customer commitments and requirements.	Inspected the Iron Mountain Information Security Policies and inquired of management to determine that processes and procedures are in place to help ensure customer confidential information is retained in accordance with customer commitments and requirements.	No deviations noted.
		For a sample customer retention request, inspected system evidence to determine that the confidential information was retained in accordance with customer commitments and requirements.	No deviations noted.
C1.8	Iron Mountain classifies data within the in-scope systems in accordance with defined requirements and policies.	Inspected the Iron Mountain Information Security Policies and inquired of management to determine that procedures exist to classify data within the in-scope systems in accordance with defined requirements and policies.	No deviations noted.
	Iron Mountain has established processes and procedures to help validate that electronic customer confidential information is destroyed in accordance with customer commitments and requirements.	Inspected the Iron Mountain Information Security Policies and inquired of management to determine that processes and procedures are in place to ensure customer confidential information is destroyed in accordance with customer commitments and requirements.	No deviations noted.
		For a sample customer destruction request, inspected system evidence to determine that the customer confidential information was disposed of in accordance with customer commitments and requirements.	No deviations noted.
	Iron Mountain's change management process governs the de-commissioning of system components to help ensure that customer confidential data is removed prior to leaving the boundaries of the Iron Mountain system.	For a sample request to de-commission component, inspected the documentation to determine that the request proceeded through the change management process and that Management validated that any confidential data was removed prior to closing the ticket.	No deviations noted.

Results of Tests and Deviation Information

Ref #	Criteria	Deviation Information
1	CC1.4. CC2.2, CC2.3, CC2.4, C1.6	**Control specified by Iron Mountain** Documented procedures and job descriptions exist which address the security, availability, and confidentiality obligations and commitments of authorized internal users and are communicated and acknowledged at the time of hire. Iron Mountain communicates security, availability and confidentiality commitments and obligations to internal users through documented policies, procedures and acknowledgement forms that employees sign-off on as part of the hiring process. **Results of Testing performed** For 3 out of 40 employees, the employee did not complete the 'IM Confidentiality Agreement', 'Code of Conduct' and/or 'Computer Resources - Access and Use: Acceptable Use Procedures' policy. For 11 out of 40 employees, employees did not complete the 'IM Confidentiality Agreement' 'Code of Conduct' and/or 'Computer Resources - Access and Use: Acceptable Use Procedures' in a timely manner (14 days or 30 days) in accordance with Iron Mountain policy but within the period. **Management Response** For the 3 employees noted above, Management confirmed through direct conversion with the employees and the employees' Manager that they were aware of and received communication of the policies and commitments related to security, availability and confidentiality at the time of hire. In all cases, evidence has since been obtained to document acknowledgement of policies. As of February 6, 2017, Iron Mountain has invested in onboarding compliance by creating a new position and hiring an Onboarding Coordinator. This coordinator will be responsible for managing the compliance of onboarding activities and accountability for ensuring appropriate acknowledgements and training is completed in a timely manner. This coordinator will manage the daily reporting of outstanding onboarding activities and work with Iron Mountain HR to address non-compliance in a timely manner. Onboarding activities that are more than 30 days past due will be reported to our Managers of Workforce Experience who will have responsibility for addressing compliance through follow up, and if necessary, formal documentation up to and including termination. We expect this new Onboarding Coordinator position to be through their onboarding and training and fully functioning in their role by March 20, 2017.

Ref #	Criteria	Deviation Information
2	CC5.5	**Control specified by Iron Mountain** Access to the in-scope data centers and surrounding facilities is approved by authorized individuals. **Results of Testing performed** For 1 of 18 sampled new Iron Mountain employees granted access to the Boyers data center, approval was obtained from the Data Center Security Manager prior to provisioning, however documentation of the approval was not retained. Based upon inquiry of the individuals responsible for approving and provisioning data center access requests, along with inspection of the employee's job title and responsibilities, we noted that the access was authorized at the time of hire and that access appears appropriate. **Management Response** IMDC Management was aware of the new hire and understood that as a Security Officer, she would require access to all IMDC doors to effectively perform her role. While the Manager and Security team discussed her on-boarding an assigned access appropriate to her role, they did not follow the documented procedure that requires an email approval prior to issuing the new badge. The VP Security, Security Manager, Data Center Manager and Compliance Manager have reeducated users on the documentation retention procedures for data center access provisioning and have further added a requirement to input the approval email directly into the user account in the security access control system.

Ref #	Criteria	Deviation Information
3	CC5.2, CC5.4	**Control specified by Iron Mountain** Individual accounts on the in-scope systems are inactivated/deleted by IT in a timely manner as approved by the authorizing manager. **Results of testing performed** For 4 of 40 terminated users, notification of termination was not provided by HR to the IT department in a timely manner. As such, the access was not removed timely. Based upon the inspection of the user's access request ticket(s), de-provisioning ticket, last network login and SecureBase/Secure Sync user listings, it was noted that the user did not have access and/or did not inappropriately access the systems after the date of termination. **Management Response** Through management investigation, it was confirmed none of the four employees noted accessed any of the in-scope system post termination. Additionally, it was confirmed that access cards were collected timely and the terminated employees did not have the ability to physically access Iron Mountain locations. Network accounts for the identified employees were disabled in a timely manner upon receiving the termination notice from the HR system. For this reason and the below factors, Management feels the deviations do not preclude the achievement of the criteria. Iron Mountain has implemented processes to mitigate the risks of the employment status not being updated in the HR system in a timely manner. These processes include: as account disablement after 60-day of inactivity, password expiration, termination checklist for managers to follow. Beginning in December 2016, educational materials will be communicated to Managers and anyone with direct reports to reinforce their awareness of their responsibility in the timely processing of terminations. Subsequent communications will be sent out quarterly to reiterate the importance of compliance with the processing of timely terminations. Furthermore, as of June 2016, an alert functionality was enabled within the Iron Mountain HR system to trigger a 'Manager Alert' when a termination has been entered into the HR system retroactively. This alert explains the critical nature of processing terminations in a timely period, the compliance requirements and asks Management to reiterate these points to their team.