Service & Security Data Sheet

Updated November 16, 2023

This document has been provided by iManage for evaluating the use of the iManage Cloud. The information provided is confidential and should not be duplicated or distributed without written permission from iManage.

The information provided is subject to change without notice.

iManage Cloud Overview

The iManage Cloud is a comprehensive cloud service (SaaS) for the delivery of iManage's best-in-class cloud platform for knowledge work.

Since 1995, thousands of professional organizations have licensed and benefited from iManage's industry-leading cloud platform for knowledge work. Now, as these organizations look to the cloud to help them eliminate complicated on-premises enterprise software deployments, streamline operations, and improve ROI, they can subscribe to the iManage Cloud. Here, they will have access to the powerful and familiar iManage solutions without the need for in-house implementation of back-office infrastructure. In addition, customers subscribing to the iManage Cloud achieve a level of service that would have been cost-prohibitive to implement on their own, with increased security, service resilience, and performance.

The iManage Cloud makes the powerful iManage Cloud platform for knowledge work available to new customers. These are customers of all sizes, including those for whom an on-premises software deployment may not be feasible. With a subscription to the iManage Cloud, they reap the benefits of the industry-leading solution for knowledge work, with the security, scalability, and performance typically available only to large organizations with big IT departments.

The iManage Cloud service is a scalable multi-tenant solution built on a secure, high-availability, modern platform architecture. A shared infrastructure provides core services like metadata storage and management, file services, preview, and OCR, while the application architecture provides logical separation of data.

Access to the iManage Cloud is available via an HTTPS connection using a lightweight HTML5 web application, with optional desktop and mobile apps that provide for integration with key desktop productivity applications for Windows and iOS, such as Microsoft Office. In addition, the mobile application can be further secured with a mobile device management solution (MDM).

This data sheet provides details about the architecture of the iManage Cloud. It is intended to assure you that data stored in the iManage Cloud is highly secured and complies with modern industry security standards.

TABLE OF CONTENTS

iManage Cloud Overview

Service Offerings

Data Centers
- Data Domicile
- Disaster Recovery

Certification and Compliance

Physical Access Controls

Network Security
- Application Access
- System Network Access
- Security Information & Event Management
- Secure Activities within the SDLC

Data Ownership

Data Encryption

Data Segregation

Data Safeguarding Practices
- Personnel Access Controls
- Access Authorization Management
- System Logs
- Application Access Controls
- Administrative Access Controls
- Data Access Levels
- Application Logs
- Business Continuity and Disaster Recovery

Data Retention
- Journaling
- Backup

Service Offerings

The iManage Cloud offers a suite of products centered around our core knowledge work platform, iManage Work.

Additional iManage Cloud products may be provisioned to address specific security requirements.

While specific products may utilize different architectures, a common iManage Cloud Security Framework is detailed in the certification and compliance section below.

Additional products include, but are not limited to:

- **iManage Security Policy Manager:** An iManage Cloud Service allows for the creation of ethical walls that can be applied to the iManage Work repository.
- **iManage Threat Manager**: An iManage Cloud Service that uses machine learning to detect and alert administrators to suspicious activity within the iManage Work repository, which may suggest a data breach or theft.
- **iManage Insight+:** iManage's knowledge search and management solution, native to the iManage Cloud ecosystem.
- **iManage Share:** An iManage Cloud Service for the collaborative sharing of content that originates in the iManage Work repository. A security data sheet for content stored within iManage Share is available upon request.
- **iManage Records Manager:** An iManage Cloud Service governing paper records and electronic content stored with the iManage Work Repository.
- **Business Intake Manager:** An iManage Cloud Service to simplify and accelerate a compliant client intake process with powerful and flexible business intake software.
- **Conflicts Manager:** An iManage Cloud Service delivering a sophisticated conflicts check solution that provides firms with a 360-degree view of ethical and business conflicts, optimizing loss prevention efforts and increasing revenue.
- **iManage Tracker:** a matter-centric task-management system that empowers organizations to action documents and emails, improve team visibility, and reduce risk.

Data Centers

The iManage Cloud is available in eight geographical regions across the globe. Each regional implementation is hosted in a primary and secondary Microsoft Azure availability zone-enabled region.

Geography	Primary Region	Secondary Region	Data Center Owner
United States	East US 2 (Virginia)	Central US (Iowa)	Microsoft Azure
	Central US (Iowa)	East US 2 (Virginia)	
Canada	Central Canada (Toronto)	Canada East (Quebec)	
Brazil	Brazil South (São Paulo)	South Central US (San Antonio, TX)	
Continental Europe	West Europe (Netherlands)	North Europe (Ireland)	
United Kingdom	UK South (London)	UK West (Cardiff)	
Australia	Australia East (Sydney)	Australia Southeast (Melbourne)	
Asia Pacific	Southeast Asia (Singapore)	East Asia (Hong Kong)	
Japan	Japan East (Tokyo)	Japan West (Osaka)	
United Arab Emirates	UAE North	UAE Central	

To ensure resiliency, a minimum of three separate availability zones are present in all availability zone-enabled regions. Azure availability zones (data centers) are physically separate locations within an Azure region that provide discrete power, networking, and cooling and are tolerant to local failures such as fire, floods, or earthquakes. They are connected through a dedicated regional low-latency network, ensuring Azure services offer the best possible performance and security within any region. All infrastructure is managed and deployed via code. All services are containerized and managed based on the Azure Kubernetes (AKS) container orchestration platform. All iManage cloud services are distributed across availability zones to ensure that iManage can continue to provide service even if up to two zones are compromised. Microsoft does not have access to the iManage Cloud or the customer data in the iManage Cloud.

IManage Operations and Security Personnel have thoroughly vetted all facilities and cloud services to ensure they meet necessary security and redundancy standards.

All iManage Cloud data centers are validated against the SOC 2 criteria and ISO 27001 controls. In addition, data center certification documents are available and can be provided for the data centers of interest. You can request these documents from your account representative if they still need to be provided.

Data Domicile

The data associated with a specific customer account will be hosted within a designated geographical region, ensuring the data's domicile is clear. The customer account and its associated data (including backups) will remain within the geographical region defined within the agreement unless the customer requests a change of venue. Customer content is automatically and asynchronously replicated to a paired Azure region via Azure's Geo-Zone Redundant Storage (GZRS) service.

Disaster Recovery

Each Azure region offers a region pair within the same geography (such as Europe or Asia). In the unlikely event of a catastrophic disaster sufficient to render all three Availability Zones in the primary region unavailable, iManage would programmatically redeploy all cloud services to the paired secondary region and resume services within the contractual RTO. Customer data is asynchronously replicated between regional pairs, and iManage can restore access to customer data within the contractual RPO.

Certification and Compliance

iManage Cloud annual SOC 2/SOC 2+/SOC 3, CSA Star, and ISO 27001 audits are conducted in the first quarter of each calendar year to ensure continued compliance with these standards. The independent third-party certification confirms that iManage Cloud has the controls and safeguards to host and process customer data securely.

Each audit includes an assessment of the control objectives and activities set forth by these standards, including controls over information technology and related processes.

These audits cover the management, operation, and maintenance of the information assets and information systems that support the iManage Cloud, providing confidentiality, availability, privacy, security, and integrity of iManage customer data during storage, processing, and delivery.

The iManage security and compliance program is certified and independently audited to the following standards and frameworks.

ISO 27001 CERTIFIED by schellman

ISO 27001 Certified

STAR LEVEL TWO: THIRD-PARTY AUDIT — STAR LEVEL TWO — SECURITY TRUST ASSURANCE & RISK

CSA STAR

AICPA SOC — aicpa.org/soc4so — SOC for Service Organizations

SOC 2 Type II Report

- ISO 27001
- ISO 27701
- ISO 27017
- ISO 27018
- ISO 22301
- SOC 2 Type 2 (All Trust Principles: Security, Availability, Confidentiality, Integrity & Privacy)
- SOC 2+ (includes select NIST 800-171 controls)
- SOC 3
- CSA STAR Level 2 (Gold Level)

Refer to http://imanage.com/security for the most current list of certifications.

Network Security

Application Access

Access to the iManage Cloud Services is provided via a secure HTTPS connection. Data is protected in transit using the TLS v1.2 protocol for authenticated and encrypted communication and is strictly enforced. The encrypted communications utilize an RSA-2048 key exchange.

Industry-standard best practices are implemented to restrict access to backend components and ensure that public-facing web servers maintain the highest security ratings. These practices include, but are not limited to:

- Implementation of firewalls and proxies with monitoring to detect hostile activity
- Internal segmentation utilizing standard application security methodology
- Separation between production, development, and testing environments
- Full segregation between iManage Cloud and iManage corporate networks

In addition to regular internal monitoring, iManage conducts annual penetration tests through an independent third party. Testing occurs in the first quarter of each calendar year and is based on NIST SP 800-115 and NIST 800-53 standards. An executive summary of the scope and the testing results can be provided on request.

System Network Access

The iManage Cloud services are delivered on a dedicated, independent network isolated from all other networks, including those used for development, testing, and iManage internal IT networks. Access to the production network for each regional implementation uses a VPN connection via a bastion host (Jumpbox). Additionally, it requires 2-factor authentication from an iManage-owned device with a valid digital certificate.

Access to the production iManage Cloud network is restricted to individuals tasked with operating and deploying the production services. Authentication with a unique user ID is required, and all access to the production iManage Cloud network is logged to our enterprise SIEM. Once authenticated, access to the services is determined based on the user role and provided on a "need to know" basis.

Security Information and Event Management (SIEM)

The iManage Cloud utilizes Splunk Enterprise for data and asset inventory, compliance monitoring and reporting, collection and analysis of security events, threat detection, and unified log management and analysis. Machine Analytics with Host Forensics is also included. Logs are maintained for one year.

Host system event logs (e.g., system event logs, non-iManage application logs, and network logs) are ingested and analyzed to detect potential threats and an extensive range of early indicators of compromise, enabling rapid response and mitigation.

Secure Activities within the SDLC

iManage uses a secure software development lifecycle (SDLC) when developing new applications and creating new features in existing applications. The SDLC process provides a consistent risk-based approach to systems development that delivers quality solutions to meet business needs. Business needs such as confidentiality, integrity, and availability are implemented in all iManage applications by leveraging the following activities as early as possible in the SDLC process.

- Secure system architecture design and analysis
- Static Application Security Testing (SAST)
- Software Composition Analysis (SCA)
- Dynamic Application Security Testing (DAST)
- Infrastructure as Code (IaC) Analysis
- Container Analysis
- Automated pen testing of hosted application
- Manual Penetration Testing (MPT)
- Manual pen testing of the hosted application. Independent certifications are performed yearly in addition to internal red team testing.

All alerts discovered in the SDLC are verified for risk and then prioritized and remediated per the risk calculation.

iManage uses industry-leading application security tools and processes to assess the SDLC.

Data Ownership

With the iManage Cloud, the customer retains sole and exclusive data ownership. The iManage Cloud Services Agreement (a sample is available here) specifies the terms governing the ownership and handling of confidential data unless superseded by an alternative agreement between iManage and the Customer. In addition, the customer-managed encryption key (CMEK) service discussed in the Data Encryption section below allows additional ownership control by enabling the customer to control the encryption key(s) used to encrypt their data.

Data Encryption

The iManage Cloud encrypts all iManage Work documents at rest using AES 256-bit encryption. At rest, encryption is mandatory for all document storage, including storage volumes supporting operating systems, backup, and recovery systems. In addition, the encryption is validated to Federal Information Processing Standards (FIPS) 140-2 level 2.

All customer content in the iManage Cloud is encrypted by default. At a minimum, data at rest is encrypted via volume-level encryption. However, content stored in iManage Work provides higher levels of encryption, ensuring that every version of every file stored in Work is *individually* encrypted at rest with a randomly generated encryption key. And that each encryption key is securely wrapped with a higher-level key, thereby providing a highly granular encryption model for added data security. iManage Work additionally provides an add-on option that lets customers assume ownership of the primary encryption key ("CMEK") used to encrypt their content. It also allows the customer to revoke the CMEK, ensuring that their data stored in the iManage Cloud cannot be decrypted.

With CMEK, the customer has complete and exclusive control of the primary key. The customer in a third-party key management service sets up the key. iManage never receives or stores a copy of the customers' encryption key. The supported third-party service provider is Microsoft Azure Key Premium Vault, which supports HSM-backed keys and is FIPS 140-2 Level 2 compliant. Customers will configure their iManage Cloud environment to connect to this third-party service provider using their company-specific private credentials. A data sheet on CMEK is available for customers interested in learning more about this option. Please inquire with your Account Representative.

Data Segregation

iManage Cloud Services are delivered by a shared infrastructure, but various access controls and validation mechanisms logically separate customer data:

- Implementation of zero-trust network architecture principles within the iManage Work environment.
- Logical content segregation of iManage Work content via unique per-customer encryption key hierarchy in accordance with NIST best practices
- Logical metadata segregation by customer ID for metadata storage
- Independent tenant administrative functions
- Containment Security Model
  - Highly granular security model with independent security access down to the document version level
  - Ability to require the filing of documents and emails to a container
  - Refiling service to ensure document and email access aligns to the container where required
  - Users outside of the schema/library with access to content are easily recognized and can be blocked
  - Integration with iManage Security Policy Manager to govern access by client or matter/engagement by policy
  - Integration with iManage Share to provide a clear distinction between content shared with external collaborators and that which is visible to internal collaborators

Data Safeguarding Practices

User accounts used to access the iManage Cloud contain only the following information about the user:

- User First Name
- User Last Name
- User Email Address (required)
- Location (optional)
- IP Address

No other Personally Identifiable Information (PII) is necessary for access to the iManage Cloud

HIPPA
Compliance

iManage Cloud can support your obligations required by HIPAA at the product, platform, and organization level in a variety of ways including, but not limited to:

- Strict employee security policies and procedures in alignment with ISO 27001 requirements
- Restricted physical access to production servers
- Formally defined breach notification policy
- Encryption of data in transit
- Encryption of data at rest
- Built-in application access controls like account lockout
- Ability to grant/deny access to documents
- Multiple optional folder access rights to provide granular user access to folders
- Audit trail of account activities on both users and content

- Restricted employee access to customer data files
- Defined disaster recovery procedures in alignment with ISO 22301 requirements
- Company (account) level limitations for those within the account who can create and manage user accounts.
- The ability for company (account) level administrators to revoke user accounts.
- User account level limitations for who can grant the ability to access, modify, and delete content
- User synchronization from an LDAP repository to ensure timely revocation of user accounts.
- Group synchronization from an LDAP repository to the alignment of access to content to job function
- Support for SAML 2.0 Single Sign-on and OpenID Connect to ensure user identity and enforce central administration of users.
- Built-in functionality to provide reasonable assurance that confidential user content is not compromised, including but not limited to refile services, multi-tier encryption key management, and role restrictions

Personnel Access Controls

iManage controls ensure that all employees involved in processing customer data through the iManage Cloud Services are authorized personnel who need to access the system resources and data, are bound by appropriate confidentiality obligations, and have undergone appropriate training on an annual basis regarding the protection of personal data. Personnel are subject to background checks.

Should any affiliate or third-party subcontractor become involved in processing customer data through the iManage Cloud Services, iManage will ensure that the third party enters into a written agreement with iManage by which they are subject to these same obligations. As of the publication of this document, there are no such third-party processors.

Access Authorization Management

All iManage personnel delivering iManage Cloud Services are subject to iManage policies and standards for secure user identification and authentication protocols, which require unique access IDs. This applies to both system access and application access.

System Logs

Access to system and network logs is provided on a need-to-know basis for operating and supporting the iManage Cloud Services. Only iManage personnel who deliver iManage Cloud Services can access the production network where the logs reside. In addition, access is restricted based on each user's job function (e.g., DBA has access to database logs, web administrator to web server logs, system administrator to system event logs, etc.)

Application Access Controls

SAML 2.0 Single Sign-on

The most common user authentication method for iManage Cloud is via a SAML 2.0-compliant identity provider (IDP). This provides the highest security and convenience for users and administrators with centralized user management. It also enables enhanced account and password restrictions and additional security capabilities like multi-factor authentication. iManage Cloud is certified with ADFS, PingFederate, and Azure ADFS identity providers. However, it has been configured with various other providers, which are also SAML 2.0 compliant. When configured, users log in to an iManage Cloud endpoint, which redirects the user to the IDP configured in

their iManage Cloud company account. When the user's identity is confirmed via authentication to the IDP, a SAML token is sent back to the iManage Cloud endpoint to allow entry to the iManage Cloud as the associated user. When using Single Sign-on (SSO), user administration (creation and suspension) is done via the Identity Provider.

Enabling the SSO option will require all users in the company library to be authenticated against the specified IDP to gain access to the iManage Cloud. Since a SAML 2.0 IDP may only be an option for some customers, particularly those onboarding, the following additional authentication options are supported:

OpenID Connect (OIDC)

Customers are increasingly adopting SSO authentication via OpenID Connect, a modern authentication standard based on OAuth 2.0. OIDC is generally easier to configure and support than SAML 2.0. It can be configured by exchanging two URLs and requires no certificates to manage and no complex metadata files to exchange. OIDC is supported by all commonly used IDP vendors, including Microsoft (ADFS, Azure AD), Okta, and PingFederate.

Directory Synchronization

Customers who utilize Azure AD as their IDP can use the iManage Users and Groups Sync solution to automatically push users and groups from Azure AD to iManage Work in the iManage Cloud. This leverages the standardized System for Cross-Domain Identity Management (SCIM) protocol and obviates the need for a customer to utilize a standalone directory synchronization tool.

Other customers utilizing an LDAP-based IDP have access to a utility that will synchronize users and groups from the company's LDAP directory to the iManage Cloud user directory. The Directory Services Sync Utility (DSSync) can be downloaded and installed on any server within the company's domain, where it will run as a Microsoft Windows service. It will communicate to the iManage Cloud over a secure connection and will be subject to the authentication requirements set up by the company administrator for the service account.

A configuration interface is included with the utility, which allows the company administrator to configure the connection, the user accounts, and users and groups to be synchronized. In addition, extensive filtering options allow a subset of the users in the LDAP directory to synchronize to the iManage Cloud, including filtering by OU, group, or user attribute.

The DSSYNC utility also allows for the synchronization of groups and group membership to the iManage Cloud directory, enabling group management within the LDAP directory services. In addition, this lightweight utility can be run continuously to provide near real-time alignment of users and groups.

Administrative Access Controls

A role-based security model allows granular control of the administrative capabilities, such that helpdesk agents who need to manage users can be limited. Higher-level administrative accounts can have access to run company reports or set up integration policies (for example, mobile integration). Finally, these role assignments can be specified at the library level, such that you can choose separate administrators for each library (e.g., your organization has merged with another)

Data Access Levels

Access to the content uploaded to iManage Work in the iManage Cloud is governed by access control lists assigned to the specific object, the object being a version of a document or email. Access can be granted to a user or a group of users with the following access levels:

- No Access
- Read Only
- Read/Write
- Full Access (includes the ability to modify the access control list)

Security can be defaulted based on the container to which the object is filed. In addition, an optional refile service will ensure that all filed objects adhere to the security set at the container to which they are filed.

Optional Client and Project/Matter based access levels

iManage Security Policy Manager is an optional service available within the iManage Cloud that allows access to objects and content based on the client or project/matter to which the content pertains. Frequently referred to as an ethical wall, the governance rules defined by iManage Security Policy manager will ensure that only users who are explicitly allowed access to client-related or project-related content can access the content. It also provides for explicit denial of access to any content pertaining to a client or project/matter. It applies to both existing content and any content created in the future.

User Activity Auditing

iManage Work in the cloud maintains audit trail logs for the following activities:

- Last login date/time
- Document activity

Only persons with access to the content can view the document activity. Each document activity entry captures the IP Address, date/time, User ID, the object being accessed, and the action taken or the result.

Document activity logs are maintained for the life of the subscription and are only deleted when the customer library is deleted).

Activity log entries are immutable and are retained indefinitely for objects (i.e., users, documents).

Business Continuity and Disaster Recovery

iManage performs annual business continuity testing and validation of high availability. The primary focus for iManage is to ensure the reliability and availability of the iManage Cloud services. However, there may be incidents and events outside iManage's control, and iManage has invested in the resources and defined processes to ensure business continuity and timely recovery of the services in the event of a disaster.

Disaster recovery capability is included within the iManage Cloud services. The iManage Cloud disaster recovery services include replicating customer data in encrypted form to a secondary Azure region maintained in the event of a disaster. Secondary Azure regions are located far enough away from the primary region to avoid the impact of a large-scale regional catastrophe. In addition, a global network of iManage support and operations resources ensures that in the event of a disaster, communications are maintained, and the technical resources required to recover are available.

iManage maintains a business continuity program compliant with and certified against the ISO 22301 standard to guide the development, implementation, and management of business continuity in the event of a disaster impacting iManage business operations. The iManage Business Continuity Management System (BCMS) is documented and part of the iManage Information Security Management System. The iManage Head of Security is responsible for the maintenance of the BCMS with oversight from the iManage Governance Board, a board consisting of iManage executive management. The iManage BCMS is reviewed, at minimum, annually. In addition, employees directly involved in implementing the BCMS are trained by participating in tabletop exercises and reviewing the appropriate procedure and process documentation.

Data Retention

iManage Work documents and deleted emails are retained in the tenant-level Trash, where the tenant administrator can further manage them. An administrator can restore or purge documents in Trash from Trash with the required access level using the iManage Control Center.

Journaling

Each time a document/object is modified in the system, a copy of the original is written to a journal. This provides a complete history of every revision to a document. Any user with access rights to the document can view and recover one of the prior entries maintained in the Journal. In addition, documents written to the Journal are retained indefinitely, or until explicitly purged, to allow customers to recover replaced or overwritten documents. Additional details on journaling and document recovery are provided in the *Document Recovery Data Sheet for iManage Cloud Customers*. Please inquire with your Account Representative for a copy.

Backup

iManage maintains the ability to recover all modified or deleted data objects for up to 90 days. This capability is intended for system recovery purposes only. Customers who require recovery of individual documents may recover documents from the Journal as noted above.

Return to Top