



ACCESS CIG, LLC

INDEPENDENT SERVICE AUDITOR'S SOC 3 + HITRUST REPORT

FOR THE UNIFY SYSTEM

FOR THE PERIOD OF MARCH 1, 2022, TO AUGUST 31, 2022

Attestation and Compliance Services



Proprietary & Confidential

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

INDEPENDENT SERVICE AUDITOR'S REPORT

To Access CIG, LLC:

Scope

We have examined Access CIG, LLC's ("Access") accompanying assertion titled "Assertion of Access CIG, LLC Service Organization Management" ("assertion") that the controls within Access' Unify System ("system") were effective throughout the period March 1, 2022, to August 31, 2022, to provide reasonable assurance that Access' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity and confidentiality (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria* and the controls set forth in the HITRUST CSF version 9.3 that are applicable to Access' Unify System required for a HITRUST CSF Security Assessment ("applicable HITRUST CSF criteria")).

Access uses various subservice organizations for cloud hosting, monitoring, and physical security services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Access, to achieve Access' service commitments and system requirements based on the applicable trust services criteria and HITRUST CSF criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Access is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Access' service commitments and system requirements were achieved. Access has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Access is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and HITRUST CSF criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and systems requirements were achieved based on the applicable trust services criteria and HITRUST CSF criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve Access' service commitments and system requirements based on the applicable trust services criteria and HITRUST CSF criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Access' service commitments and system requirements based on the applicable trust services criteria and HITRUST CSF criteria.

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

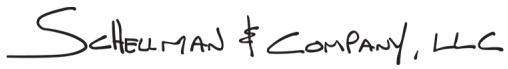
Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that Access' service commitments and system requirements were achieved based on the applicable trust services criteria and HITRUST CSF criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Access' Unify system were effective throughout the period March 1, 2022, through August 31, 2022, to provide reasonable assurance that Access' service commitments and system requirements were achieved based on the applicable trust services criteria and HITRUST CSF criteria is fairly stated, in all material respects.

The signature is handwritten in black ink and reads "SCHEELMAN & COMPANY, LLC". The first letter 'S' is significantly larger and more stylized than the rest of the text.

Columbus, Ohio
February 2, 2023

ASSERTION OF ACCESS SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Access CIG, LLC's ("Access") Unify system ("system") throughout the period March 1, 2022, to August 31, 2022, to provide reasonable assurance that Access' service commitments and system requirements relevant to security, availability, processing integrity and confidentiality were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period March 1, 2022, to August 31, 2022, to provide reasonable assurance that Access' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity and confidentiality (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*), and the controls set forth in the HITRUST CSF version 9.3 that are applicable to Access' Unify System required for a HITRUST CSF Security Assessment ("applicable HITRUST CSF criteria"). Access' objectives for the system in applying the applicable trust services criteria and HITRUST CSF criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria and HITRUST CSF criteria. The principal service commitments and system requirements related to the applicable trust services criteria and HITRUST CSF criteria are presented below.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period March 1, 2022, to August 31, 2022, to provide reasonable assurance that Access' service commitments and systems requirements were achieved based on the applicable trust services criteria and HITRUST CSF criteria.

DESCRIPTION OF THE BOUNDARIES OF THE UNIFY SYSTEM

Company Background

Headquartered in Woburn, Massachusetts, Access CIG, LLC (Access) provides records and information management services to organizations ranging from small and mid-sized business to the heavily regulated enterprise. The company has strong expertise providing physical and electronic record keeping services through an extensive network of physical and digital delivery resources located throughout the Americas.

Description of Services Provided

The services and supporting technology which make up the Unify System scope are as follows:

Records and Non-records Storage:

Access provides full service, off-site secure storage for business records for any media type. Value added services enable customers to manage the entire information lifecycle in compliant and legally defensible manner. Access operates physical record storage facilities to accommodate real assets and virtual private cloud storage facilities to accommodate electronic assets.

Conversion Services and Documentation Scanning:

Physical record storage facilities also operate commercial imaging equipment to provide physical media conversion to electronically scanned or captured information. Using standardized operating procedures, records facility operations personnel are able to image customer content and securely deliver the electronic material to the Unify ingestion pipeline for further processing, storage, and lifecycle management.

Electronic Records Management and Governance:

Electronic records are stored, accessed, and managed in a purpose-built cloud native platform solely designed to support rigorous information management requirements. The latest design principles in dev-sec-ops have been utilized to produce secure software with high degrees of automation and scale. With a comprehensive API design, customers have the option of connecting to the Unify platform using their information management tools of choice while Access maintains a secure data processing environment for every asset under lifecycle management control.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principal Service Commitments and System Requirements

Access designs its processes and procedures to meet its objectives based on the service commitments made to its customers. Security, availability, and confidentiality commitments to customers are documented and communicated in standardized contracts.

Security, availability, and confidentiality commitments are standardized and include, but are not limited to, the following:

- Access' systems are protected against unauthorized access, use, or modification.
- The Access systems are available for operation and use and monitored as committed or agreed.
- Information designated as confidential is protected and retained until its disposal is requested by the customer. Access maintains retention and destruction policies in accordance with data protection

requirements. Personnel perform retention and disposal activities according to company policy. Physical and electronic records are securely managed until destruction is authorized by the customer/owner.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

Access utilizes cloud computing platform services from Amazon Web Services (AWS). Access does not own or maintain hardware located in AWS data centers. Access and AWS operate under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure (i.e. physical infrastructure, geographical regions, availability zones, edge locations, operating, managing and controlling the components from the host operating system, virtualization layer and storage) and Access is responsible for securing the software solution built on top of AWS platform resources (i.e. customer data, customer facing features, identity access management, virtual firewall configurations, network traffic security, server-side and database encryption). Production workloads and customer facing applications are logically and physically segmented from Access' internal corporate information systems.

Access Unify is supported by internal Access team members and external vendors in the following manner:

- Production infrastructure is deployed and run in the AWS cloud service. Underlying facilities and virtualized software are managed by AWS.
- Access personnel are responsible for the 24x7 operation of the Unify environment with targeted assistance from third-party vendors.
- Unify software is predominantly written in Java and is run as containerized workloads on Linux powered AWS elastic cloud compute (EC2) services.
- Software Development Life Cycle (SDLC) is managed in Microsoft Azure Dev Ops.
- Electronically Stored Information (ESI) i.e., customer assets are stored and encrypted in AWS Simple Storage Service (S3) to support business services.
- Application metadata is stored and encrypted MongoDB (AWS managed service) to support business services.
- Monitoring and alerting services are provided by eSentire, a third-party managed security service provider (MSSP).
- Integrated identity access management (IAM) for customer users and systems provided by Auth0; internal IAM for Access users and systems provided by Microsoft Azure AD.
- Log aggregation and security information and event management (SIEM) services are provided by MSSPs.
- Privileged Access Management (PAM) is provided by CyberArk.

The in-scope infrastructure consists of systems, platforms, and databases, as shown in the table below:

Primary Infrastructure			
Production System	Business Function Description	Platform	Physical Location
Unify Application	Primary inventory management application for record tracking, management, and business records storage.	Docker Containers	AWS US East
AWS ECS	Architecture that supports the in-scope services.		AWS CAN Central

Primary Infrastructure			
Production System	Business Function Description	Platform	Physical Location
Databases & Data Storage	System data storage for the in-scope applications.	S3 and MongoDB on AWS	AWS US East AWS CAN Central
WAF and Security Groups	Front-end security groups protect the network perimeter based on rule-based access control lists and back-end security groups segregate the database servers from internal traffic. Web Application Firewalls protect the underlying applications from abusive inbound internet traffic.	AWS	
eSentire, Lambda, Cloudtrail, Guard Duty and WAF	Managed Security Service Provider that ingests AWS logs, reviews events 365/24/7 and blocks inbound traffic deemed as malicious or abusive; additional escalation of events for Access InfoSec review that violate best practices or represent suspicious activity.		
Azure AD single sign on (SSO) & Virtual Private Network (VPN)	Provides access control, endpoint security, and authentication and authorization services to production environments.	Azure	
CyberArk	Privileged Access Management limits, authorizes and records any access to production environments and data to authorized agents performing pre-authorized (service ticket) based work.	Linux	

People

The personnel that contribute to the operation of the system include the following:

- Executive management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Information technology (IT) department – manages, monitors, and supports user entities' information and systems from unauthorized access and use while maintaining integrity and availability.
- Accounting department – performs reconciliations related to services provided to user entities and provides financial and regulatory reporting and operational quality assurance (QA) and compliance.
- Conversion services department – responsible for the retrieving, indexing, scanning, and delivering of clients' document images.
- Customer support and service desk – responsible for responding to customer inquiries and issues.
- Client services – responsible for fulfilling client needs.

Procedures

Access, Authentication and Authorization

Documented information security policies and procedures are in place to define the requirements for secure access to the Access information systems. Access to the production environments is governed by the domain group policy object (GPO), which enforces network authentication credentials (i.e., username and password) and the authentication password policy configurations (i.e., password minimum length, history, age, and complexity). Access' network users are required to authenticate via a user account and password before being granted access to the network domains and are configured to enforce the GPOs' password policies.

Authentication to the remote access tool, AWS, Azure, production server operating systems, production databases, and Unify application are granted based on the user's production domain credentials. Authentication controls (e.g., password minimum lengths, expiration intervals, etc.) for these systems are governed by the primary domain controller's security policies. The network domain is configured to require users to authenticate via a unique user account and password. The Unify application is configured to require external users to authenticate via a unique user account and password. Internal Unify administrative users are authenticated to the Unify account provisioning system via a user account and password configured to enforce the following password controls:

Administrator access within the in-scope network domain, AWS, Azure, production server operating systems, production databases, and application is restricted to user accounts accessible by authorized personnel.

Access employs a documented data transmission policy to prohibit the transmission of sensitive information over the internet or other public communication paths unless it is encrypted. Data within the Unify application databases is encrypted via the standards of the Access information security policy.

Privileged Access Management Tool

Prior to authenticating to infrastructure supporting the Unify application, a user is required to request temporary elevated access via the PAM tool. Privileged access management access requests require IT management personnel approval prior to privileged access being granted. Privileged access management access sessions are recorded and are reviewed monthly. If unauthorized changes are discovered during the privileged access management access session review, IT security personnel investigate and resolve the issue. If a change is required to be made, a ticket is created, and the change management process is followed.

Access Requests and Access Revocation

Access requests for employees, contractors, and third parties are formally documented by operations personnel in a request form through the ticketing system. Access requests for employees, contractors, and third parties to the Access infrastructure and application are granted based on individual job responsibilities and require approval from IT personnel. A termination checklist is completed as part of the employee termination process, which includes employees, contractors and third parties. System administrators revoke user privileges to in-scope systems upon notification from human resources (HR) or operations personnel of a termination or pending termination. On a monthly basis, security personnel perform a review of terminated employees to help ensure terminated user accounts are deleted / disabled at the AD level, and to verify that current production AD access for employees, contractors, and third parties is still appropriate. If changes are required as a result of the review, corrective action is taken, as necessary.

Physical Security

An inventory of assets and services is maintained, and media handling and disposal policies and procedures are in place to guide personnel in performing sanitization procedures to help ensure data and software is unrecoverable prior to retiring the physical asset. Laptops are encrypted and configured with screen saver timeout to automatically lock user sessions after 15 minutes of inactivity.

Network Security

Remote access to the Unify production environment requires users to authenticate to the production network via encrypted remote access tool. The remote access tool requires a remote user to have a corporate network AD account and password to successfully authenticate. The ability to modify the remote access tool configurations is restricted to user accounts accessible by authorized IT personnel.

Access maintains redundant, high-availability web application firewall (WAF) systems within the AWS environment to provide failover services in the event of primary WAF failure and to protect the network infrastructure from unauthorized external sources. The WAF utilizes security groups to filter unauthorized inbound network traffic from the internet and are configured to deny any type of network connection that is not explicitly authorized by a firewall rule. The ability to modify WAF configurations is restricted to authorized personnel. WAF rulesets are reviewed by a network operations personnel on an annual basis to help ensure the access rules are configured to AWS best practices. Additionally, an intrusion detection and prevention system (IDPS) is utilized within the AWS environment to monitor, analyze, and respond to the in-scope systems for possible or actual security breaches.

Vulnerability scans are performed on at least a monthly basis. In addition, a third-party specialist performs an external penetration test on an annual basis. Action items to address vulnerabilities identified within the vulnerability scans and external penetration tests are researched and monitored by senior IT management through resolution. Application web servers utilize transport layer security (TLS) encryption for web communication sessions.

Antivirus / Endpoint Detection and Response (EDR)

Artificial intelligence (AI) antivirus software is utilized on production servers and workstations in order to detect and eliminate data or files that contain viruses or malicious programs recognized by the software. It is configured to monitor for updates to definitions and update registered clients on at least a daily basis. Real time scans occur on registered clients and the software is configured to auto-terminate any known threats. Additionally, the software is configured to scan all registered files upon access or modification based on hash values. Access operations personnel are notified via e-mail of potential viral activity that requires investigation and remediation. Additionally, group policies are in place to prevent installation of unapproved software on workstations to prevent the introduction of malicious software.

Change Management

IT management maintains documented change control procedures to guide personnel in application development, maintenance, and documentation activities. These procedures include topics such as change request types and classifications, coding standards, required documentation, client contact, and development lifecycle management.

The Product and Engineering teams meet on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the system.

Prior to the start of development activities, the Product team documents the requirements for application changes. These requirements involve the functional and technical specifications that a feature must meet prior to implementation into the production environment. This process guides the development activities by defining the requirements an application change must meet.

Development and testing activities are performed in distinct environments that are logically separate from production in order to help ensure that changes made within the test environment do not affect the production environment.

Version control software is utilized to log and track application and infrastructure change as well as manage versions of source code. The software allows development personnel to check out different versions of the code and to store it locally on their computer. Once users are ready to update the code repository, they check the code back in. Changes to source code result in the creation of a new version of the application code. The version control software provides rollback capabilities in the event application code needs to be restored to a previous version. The ability to modify source code within the version control software is restricted to authorized IT and development personnel. Users are authenticated via a user account and password before being granted access to the application code in the version control software.

The version control software is configured to enforce a manual code review from an individual independent of the code development prior to final code commit into the master code branch. Following approval of the code review, automated and manual testing are performed on application and infrastructure changes with user acceptance testing (UAT) performed in a mirrored production environment. All changes require final approval by management prior to implementation into the production environment. The ability to implement changes into the production environment is restricted to authorized personnel.

Data Backup and Disaster Recovery

Policies and procedures are established to define the requirements for data backup, the protection of backup media, and contingency plans to recover information systems in the event of a failure. IT personnel meet to discuss system availability as compared to system commitments, scheduled maintenance, and current projects on a weekly basis. Access utilizes backup systems to perform automated backups of production systems. The backup systems are configured to perform daily, weekly, and monthly snapshots of production system data based on predefined schedules. The backup systems are also configured to send e-mail notifications to IT personnel in the event of a backup job failure. The data replication tool is configured to replicate production data to a geographically separate data center facility on at least a daily basis. The ability to retrieve the backup data is restricted to authorized members of the IT department.

Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. IT personnel perform a restoration of backup files on an annual basis to ensure that backups are readable as part of the disaster recovery test. Further, disaster recovery plans are reviewed and tested on an annual basis.

Incident Response

Documented escalation procedures for reporting security, availability, and confidentiality incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints. Additionally, incident handling procedures are implemented for security, availability, and confidentiality incidents that include detection, analysis, containment, eradication, and recovery. IT personnel utilize an automated ticketing system to manage system incidents, response, and resolution.

System Monitoring

An enterprise monitoring console is utilized to monitor the performance and availability of production servers and network devices. In the event that predefined conditions are triggered, or thresholds are exceeded on the monitored devices, the monitoring tool is configured to automatically respond based on defined rules and alert IT personnel via e-mail. When an alert is sent, IT personnel investigate and resolve the issue, if necessary. If a change is required to be made, a ticket is created, and the change management process is followed. Additionally, IT personnel meet to discuss system availability as compared to system commitments, scheduled maintenance, and current projects on a weekly basis.

Data

The Unify application platform is used to store and retrieve digital images. Clients can securely request, manage, and track services via a secure web interface. Access typically does not know the nature of the client data that Access stores; therefore, all client data is treated as highly confidential and subject to privacy laws and regulations in jurisdictions in which Access operates.

The following table describes the information used and supported by the system:

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
Scan-on-demand images	Customer requested electronic scans of physical records	Confidential
Active file services	Digital client record storage, retrieval, and work order management	

Subservice Organizations

Data center hosting services are provided by AWS, the infrastructure monitoring and alerting services for the IDPS, WAF, malware, and incidents and their respective configurations are provided by eSentire. Access Operations is responsible for restricting physical access to the record center facilities.

The aforementioned cloud hosting service provider is responsible for providing the physical safeguarding of the IT infrastructure to help ensure that unauthorized access to the IT infrastructure does not occur, as well as providing environmental safeguards (e.g., power supply, temperature control, fire suppression, etc.) against certain environmental threats.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, eSentire, Access Operations, alone or in combination with controls at Access, and the types of controls expected to be implemented at AWS, eSentire, and Access Operations to achieve Access' service commitments and system requirements based on the applicable trust services criteria.

Control Activity Expected to be Implemented by AWS, eSentire, and Access Operations	Applicable Trust Services Criteria
eSentire is responsible for the monitoring of configuration changes and events of systems that reside within the AWS infrastructure.	CC2.1, CC7.1, CC7.2, A1.1, A1.2
eSentire is responsible for collecting data from system infrastructure components and endpoint systems to monitor system security performance, potential security vulnerabilities, resource utilization and alerting the information security team upon detection of unusual system activity or service requests.	CC2.1, CC4.2, CC7.1, CC7.2, A1.1, A1.2
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Access systems reside.	CC6.1, CC6.2, CC6.3, CC6.5, CC6.6
AWS is responsible for restricting physical access to data center facilities, offline storage and backup media, and other system components such as firewalls, routers, and servers.	CC6.4, CC6.5
Access Operations is responsible for restricting physical access to the record center facilities.	
eSentire is responsible for the configuration and monitoring of the WAF to filter unauthorized inbound network traffic from the internet, deny any type of network connection that is not explicitly authorized by a firewall rule, and ensure network address translation (NAT) functionality of the firewall systems is configured to manage internal internet protocol (IP) addresses, and prevent suspicious activity or anomalies.	CC6.6
eSentire is responsible for the configuration and monitoring of the IPS to prevent suspicious activity or anomalies on the network.	
AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Access systems reside.	CC6.7
eSentire is responsible for implementing controls to prevent, detect, and respond to the introduction of unauthorized or malicious software.	CC6.8
AWS is responsible for monitoring any changes to the logical access controls system for the underlying network, virtualization management, and storage devices where the Access systems reside.	CC7.1
AWS is responsible for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC7.2
AWS is responsible for monitoring the logical access control systems for the underlying network, virtualization management, and storage devices for the cloud hosting services where the Access systems reside.	
AWS is responsible for ensuring the data center facilities are equipped with environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.	A1.2

Complementary Controls at User Entities

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the Unify System.

HITRUST CSF Criteria Not Applicable to the In-Scope System

The HITRUST CSF criteria presented below, are not applicable to the Unify System within the scope of this examination. As a result, an associated control activity is not required to be in place at the service organization for the omitted applicable HITRUST CSF criteria. The following table presents the HITRUST CSF criteria that are not applicable for the Unify System at Access. The not applicable HITRUST CSF criteria are also described within Section 4.

Criteria #	Reason for Omitted Criteria
09.x Electronic Commerce Services	Not applicable – No electronic commerce is performed as part of the Unify application or services.
09.y On-line Transactions	
10.I Outsourced Software Development	Not applicable – Access does not utilize outsourced software development as part of the provisioning of application services for the Unify system.