



A-LIGN

Velocity Global

Type 2 SOC 3

2024

Velocity Global



SOC 3 FOR SERVICE ORGANIZATIONS REPORT

January 1, 2024 to March 31, 2024

Table of Contents

SECTION 1 ASSERTION OF VELOCITY GLOBAL MANAGEMENT	1
SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT	3
SECTION 3 VELOCITY GLOBAL'S DESCRIPTION OF ITS EMPLOYER OF RECORD SERVICES SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2024 TO MARCH 31, 2024	7
OVERVIEW OF OPERATIONS.....	8
Company Background.....	8
Description of Services Provided.....	8
Principal Service Commitments and System Requirements.....	8
Components of the System.....	9
Boundaries of the System.....	12
Changes to the System in the Last 3 Months.....	12
Incidents in the Last 3 Months	12
Criteria Not Applicable to the System.....	12
Subservice Organizations	12
COMPLEMENTARY USER ENTITY CONTROLS.....	14

SECTION 1

ASSERTION OF VELOCITY GLOBAL MANAGEMENT

ASSERTION OF VELOCITY GLOBAL MANAGEMENT

April 8, 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within Velocity Global's ('the Company') Employer of Record Services System throughout the period January 1, 2024 to March 31, 2024, to provide reasonable assurance that Velocity Global's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Velocity Global's Description of Its Employer of Record Services System throughout the period January 1, 2024 to March 31, 2024" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2024 to March 31, 2024, to provide reasonable assurance that Velocity Global's service commitments and system requirements were achieved based on the trust services criteria. Velocity Global's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Velocity Global's Description of Its Employer of Record Services System throughout the period January 1, 2024 to March 31, 2024".

Velocity Global uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Velocity Global, to achieve Velocity Global's service commitments and system requirements based on the applicable trust services criteria. The description presents Velocity Global's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Velocity Global's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Velocity Global's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Velocity Global's controls.

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

We assert that the controls within the system were effective throughout the period January 1, 2024 to March 31, 2024 to provide reasonable assurance that Velocity Global's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Velocity Global's controls operated effectively throughout that period.

Chuck Kim

Chuck Kim
VP Cloud and Corporate Infrastructure
Velocity Global

SECTION 2
INDEPENDENT SERVICE AUDITOR'S REPORT



INDEPENDENT SERVICE AUDITOR'S REPORT

To Velocity Global:

Scope

We have examined Velocity Global's ("the Company") accompanying assertion titled "Assertion of Velocity Global Management" (assertion) that the controls within Velocity Global's Employer of Record Services System were effective throughout the period January 1, 2024 to March 31, 2024, to provide reasonable assurance that Velocity Global's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in *AICPA Trust Services Criteria*.

Velocity Global uses AWS to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Velocity Global, to achieve Velocity Global's service commitments and system requirements based on the applicable trust services criteria. The description presents Velocity Global's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Velocity Global's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Velocity Global, to achieve Velocity Global's service commitments and system requirements based on the applicable trust services criteria. The description presents Velocity Global's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Velocity Global's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Velocity Global 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 Velocity Global's service commitments and system requirements were achieved. Velocity Global has also provided the accompanying assertion (Velocity Global assertion) about the effectiveness of controls within the system. When preparing its assertion, Velocity Global is responsible for selecting, and identifying in its assertion, the applicable trust services 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 management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

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

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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 Velocity Global's Employer of Record Services System were suitably designed and operating effectively throughout the period January 1, 2024 to March 31, 2024, to provide reasonable assurance that Velocity Global's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Velocity Global's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Velocity Global's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Velocity Global, user entities of Velocity Global's Employer of Record Services during some or all of the period January 1, 2024 to March 31, 2024, business partners of Velocity Global subject to risks arising from interactions with the Employer of Record Services, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

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

A-ALIGN ASSURANCE

Tampa, Florida
April 8, 2024

SECTION 3

VELOCITY GLOBAL'S DESCRIPTION OF ITS EMPLOYER OF RECORD SERVICES SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2024 TO MARCH 31, 2024

OVERVIEW OF OPERATIONS

Company Background

In 2014, Velocity Global pioneered the industry of distributed work to make working together across the globe a reality for all. Over the years, the needs of their customers and their business have evolved. Today, Velocity Global is considered the strategic partner for companies hiring global talent to maximize their business value.

Velocity Global supports over 185 countries around the world, and their own global team is spread across 60 countries, leveraging deep domain expertise and knowledge every day to help companies reach their goals by hiring, retaining, and paying talent anywhere in the world.

Industries served by Velocity Global include but aren't limited to Financial Services, Information Technologies and Telecommunications, Legal Services, Advertising, Manufacturing, Technology, Healthcare, Retail, and Educational institutions.

Description of Services Provided

Velocity Global offers a global employment solution that simplifies how companies onboard, manage and pay talent. With unparalleled expertise in over 185 countries, Velocity Global delivers best-in-class service and innovative solutions that enable companies to feel confident breaking into new markets. Velocity Global's services include international Employer of Record, global immigration, payroll, and consulting to help companies achieve their global growth goals. Companies trust Velocity Global to ensure a compliant, efficient, and flexible global expansion.

Principal Service Commitments and System Requirements

Velocity Global designs its processes and procedures related to Information Security to meet its objectives for its Employer of Record services. Those objectives are based on the service commitments that Velocity Global makes to user entities, the laws and regulations that govern the provision of Employer of Record services, and the financial, operational, and compliance requirements that Velocity Global has established for the services.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Information Security Program that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit

Velocity Global establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Velocity Global's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Information Security Program.

Components of the System

Infrastructure

Primary infrastructure used to provide Velocity Global's Employer of Record Services System includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
AWS	Cloud	Hosts Velocity Global's Software as a Service (SaaS) Solution

Software

Primary software used to provide Velocity Global's Employer of Record Services System includes the following:

Primary Software		
Software	Operating System	Purpose
Global Work Platform	N/A	Velocity Global's Native Employer of Record platform

People

Velocity Global has a staff of 350 employees organized in the following functional areas:

- *Corporate.* Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, and human resources.
- *Operations.* Provides direct day-to-day services and management of client relationships.
- *IT.* The infrastructure, networking, and systems administration staff typically has no direct use of the Employer of Record Services System. Rather, it supports Velocity Global's IT infrastructure, which is used by the software. A systems administrator will deploy the releases of the Human Resources Software services and other software into the production environment.
- *Development.* The software development staff develops and maintains the custom software for Velocity Global. This includes the Employer of Record Services System, supporting utilities, and the external websites that interact with Velocity Global. The staff includes software developers, database administration, software quality assurance, product managers, designers, and researchers:
 - The information security staff supports the Employer of Record Services System indirectly by monitoring internal and external security threats and maintaining current antivirus software.

Data

Data, as defined by Velocity Global, constitutes the following:

- Employer of Record Services System files
- Transaction data
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Velocity Global policies and procedures that define how services should be delivered. These are located on the Company's Intranet and can be accessed by any Velocity Global team member.

Physical Security

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope system. For specific controls around the physical security measures AWS has implemented, please refer to the Subservice Organization section below.

Logical Access

Velocity Global uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, Velocity Global implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Employees and approved vendor personnel sign on to the Velocity Global network using a Single Sign-On (SSO) user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of SSO. Passwords must conform to defined password standards and are enforced through parameter settings in the SSO. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Customer employees' access Velocity Global services through the Internet using the TSL functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured in accordance with Velocity Global's configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Upon hire, employees are assigned to a position in the HR management system. Prior to the employees' start date, HR creates a ticket for employee user IDs to be created and access to be granted. The report is used by IT to create user IDs and access rules. Access rules have been pre-defined based on the defined roles. The system lists also include employees with position changes and the associated roles to be changed within the access rules.

On an annual basis, access rules for each role are reviewed by a working group composed of security, IT, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access.

On a quarterly basis, managers review roles assigned to their direct reports. Role lists are generated by IT and distributed to the managers via the event management system. Managers review the lists and indicate the required changes in the event management record. The record is routed back to the security help desk for processing. The IT manager identifies any records not returned within two weeks and follows up with the manager.

Computer Operations - Backups

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Velocity Global monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Velocity Global evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center space
- Data storage
- Network bandwidth

Velocity Global has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Velocity Global system owners review proposed operating system patches to determine whether the patches are applied. Customers and Velocity Global systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Velocity Global staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

Velocity Global maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Velocity Global. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party vendor on a monthly basis in accordance with Velocity Global policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Velocity Global. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Velocity Global system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system from the Internet through the use of leading virtual private network (VPN) technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes the Employer of Record Services System performed in the Denver, Colorado facilities.

This report does not include the cloud hosting services provided by AWS at the various facilities.

Changes to the System in the Last 3 Months

No significant changes have occurred to the services provided to user entities in the 3 months preceding the end of the review period.

Incidents in the Last 3 Months

No significant incidents have occurred to the services provided to user entities in the 3 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common/Security and Availability criteria were applicable to the Velocity Global Employer of Record Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at the various facilities.

Subservice Description of Services

AWS provides cloud hosting services, which includes implementing physical security controls to protect the housed in-scope systems. Controls include, but are not limited to, visitor sign-ins, required use of badges for authorized personnel, and monitoring and logging of the physical access to the facilities.

Complementary Subservice Organization Controls

Velocity Global’s services are designed with the assumption that certain controls will be implemented by the subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Velocity Global’s services to be solely achieved by Velocity Global control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of Velocity Global.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	Criteria	Control
Common Criteria / Security	CC6.4, CC7.2, A1.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		KMS-Specific - Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.
		KMS-Specific - Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team processes.
	CC6.5	All AWS production media is securely decommissioned and physically destroyed prior to leaving AWS Secure Zones.
		AWS provides customers the ability to delete their content. Once successfully removed the data is rendered unreadable.
		AWS retains customer content per customer agreements.

Velocity Global management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Velocity Global performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and the subservice organization
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Velocity Global's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Velocity Global's services to be solely achieved by Velocity Global control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Velocity Global's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Velocity Global.
2. User entities are responsible for notifying Velocity Global of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Velocity Global services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Velocity Global services.
6. User entities are responsible for providing Velocity Global with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Velocity Global of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.