Centric Software, Inc.
Type 2 SOC 3
2020

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

October 1, 2020 To December 31, 2020

Table of Contents

SECTION 1

ASSERTION OF CENTRIC SOFTWARE, INC. MANAGEMENT

ASSERTION OF CENTRIC SOFTWARE, INC. MANAGEMENT

January 22, 2021

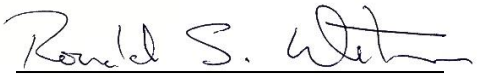
We are responsible for designing, implementing, operating, and maintaining effective controls within Centric Software, Inc.'s ('Centric Software' or 'the Company') Product Lifecycle Management (PLM), Software as a Services (SaaS) System throughout the period October 1, 2020 to December 31, 2020, to provide reasonable assurance that Centric Software's service commitments and system requirements relevant to Security, Availability and Confidentiality (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "Centric Software, Inc.'s Description of its PLM, SaaS System throughout the period October 1, 2020 to December 31, 2020" 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 October 1, 2020 to December 31, 2020, to provide reasonable assurance that Centric Software's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy* (AICPA, *Trust Services Criteria*). Centric Software's objectives for the system in applying 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 "Centric Software, Inc.'s Description of Its PLM, SaaS System throughout the period October 1, 2020 to December 31, 2020".

Centric Software uses Amazon Web Services ('AWS'), Microsoft Azure ('Azure'), Google Cloud Platform ('GCP'), and IBM Cloud Computing ('IBM') to provide cloud hosting services and Digital Realty to provide data center hosting services (collectively, 'the subservice organization'.) The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Centric Software, to achieve Centric Software's service commitments and system requirements based on the applicable trust services criteria. The description presents Centric Software's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Centric Software's controls. The description does not disclose the actual controls at the subservice organizations.

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 October 1, 2020 to December 31, 2020 to provide reasonable assurance that Centric Software's service commitments and system requirements were achieved based on the applicable trust services criteria.



Centric Software, Inc. Management

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Centric Software, Inc.

Scope

We have examined Centric Software, Inc.'s accompanying description of PLM, SaaS System titled "Centric Software, Inc.'s Description of Its PLM, SaaS System throughout the period October 1, 2020 to December 31, 2020" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2020 to December 31, 2020, to provide reasonable assurance that Centric Software's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Centric Software uses AWS, Azure, GCP, and IBM to provide cloud hosting services and Digital Realty to provide data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Centric Software, to achieve Centric Software's service commitments and system requirements based on the applicable trust services criteria. The description presents Centric Software's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Centric Software's controls. The description 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.

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

Centric Software 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 Centric Software's service commitments and system requirements were achieved. Centric Software has provided the accompanying assertion titled "Assertion of Centric Software, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Centric Software is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- 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 the description is presented in accordance with the description criteria
- 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
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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

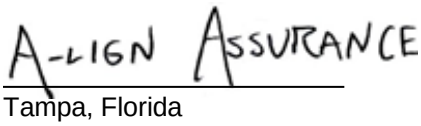
In our opinion, management's assertion that the controls within Centric Software's PLM, SaaS System were suitably designed and operating effectively throughout the period October 1, 2020 to December 31, 2020, to provide reasonable assurance that Centric Software's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on Centric Software'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 Centric Software, user entities of Centric Software's PLM, SaaS Services during some or all of the period October 1, 2020 to December 31, 2020, business partners of Centric Software subject to risks arising from interactions with the PLM, SaaS Services, and those who have sufficient knowledge and understanding of the complementary user entity controls and complementary subservice organization 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.



Tampa, Florida
January 22, 2021

SECTION 3

CENTRIC SOFTWARE, INC.'S DESCRIPTION OF ITS PLM, SAAS SYSTEM THROUGHOUT THE PERIOD OCTOBER 1, 2020 TO DECEMBER 31, 2020

OVERVIEW OF OPERATIONS

Company Background

From its headquarters in Silicon Valley, Centric Software provides a Digital Transformation Platform for companies in fashion, retail, footwear, luxury, outdoor, consumer goods and home décor. All Centric innovations shorten time to market, boost product innovation and reduce costs.

Centric Software is majority-owned by Dassault Systèmes (Euronext Paris: #13065, DSY.PA), well known in 3D design software, 3D Digital Mock Up and PLM solutions.

Description of Services Provided

Centric Software's flagship PLM platform, Centric 8, delivers enterprise-class merchandise planning, product development, sourcing, quality and collection management functionality tailored for fast-moving consumer industries. Centric provides innovative PLM technology and key industry learnings for emerging brands. Centric Visual Innovation Platform ('VIP') offers a new fully visual and digital experience for collaboration and decision-making and includes the Centric Buying Board to transform internal buying sessions and maximize retail value and the Centric Concept Board for driving creativity and evolving product concepts.

The solution enables processing of the following tasks related to Product Lifecycle Management:

- Defining Seasonal Product Plans by Company, By Brand, By Department Collection
- Creating/Editing/Managing Products
- Creating/Editing/Managing Materials
- Creating/Editing/Managing Agents, Suppliers and Vendors
- Creating/Editing/Managing Bills of Materials in context of Product/Material
- Creating /Editing/Managing other information necessary for a supplier/vendor to be able to source and produce the product
- Manage and do what-if analysis for sample products and their associated costs
- Present Collections of Products to allow Merchandizing decisions such as:
    - Good, Better, Best product positioning
    - Add / Drop product
    - Margin Analysis
    - Revenue Analysis
    - Store Deliveries
    - This year / Last year comparison
    - Order management

Principal Service Commitments and System Requirements

Centric Software offers the solution as:

- Permanent License
- Subscription License and
- SaaS

The solution can be:

- Hosted by customers in their own environment
- Hosted by Centric in either Standard Service or Premium and Premium HA Service
- Defined service level agreements ('SLAs') describe and indicate to customers what the services cover

Over the past two to three years there has been a strong growth in interest from customers to move from hosting Centric 8 themselves to have Centric provide the service for them. Currently a third of customers choose Centric to provide the service. Centric Software is currently in the process of ensuring all services meet those expected by Customers' information technology ('IT') organizations this includes ISO27001:2013 certification, SOC2 Attestation and as a company that does a large portion of its business in Europe GDPR compliance.

Components of the System

Infrastructure

Primary infrastructure used to provide Centric Software's PLM, SaaS System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Firewalls	Netgate XG-1541 pfSense2.4.5 Appliances	Filter traffic into and out of the private network as well as segments internal traffic supporting corporate services (Finance, Development, Quality Assurance ('QA'), Support, Client Services, Sales, and Cloud Operations)
Switches	Aruba 3810M Aruba 5406R-zl2 CiscoSG300-10 NetGear GS748T EDIMAX Pro GS-5008PL Dell Power Connect 2724	Connects devices on the Corporate and Operations networks
Virtual Server Hosts	Dell PowerEdge Nutanix Hyperconverged Server	Act as VMWare ESXiVirtualization Software that host Web Servers, Application Servers, Database Services, Centric proprietary Servers Centric 8 Application Servers
Network Attached Storage ('NAS') Devices	Quality Network Appliance Provider ('QNAP') Synology	Network Attached Storage to serve as backup drives for various Centric servers and applications
Phone System	Dell Optiplex	Hosts Asterisk Voice over Internet Protocol ('VOIP') Phone System provides Headquarters and Home Offices access to the Public Switched Telephone Network ('PSTN')

Software

Primary software used to provide Centric Software's PLM, SaaS System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Atlassian JIRA	Cloud Provider	Trouble Ticketing System for internal IT support Trouble Ticketing System for internal Cloud Operations support
Nagios XI Enterprise	Linux	Live Monitoring and notification of Internal IT systems infrastructure as well as Operations infrastructure for Standard and Cloud services
Open Virtual Private Network (VPN) Remote Access Server	FreeBSD running on Netgate pfSenseAppliances	Allow Centric employees remote access to Centric Corporate and Operations networks
Remote Desktop Gateway Servers	Microsoft Windows 2012 R2	Provide Centric employees to remote desktop into specific IT and Operations servers for Administrative activities
Veeam	Windows 2016	Backs up Images of key Corporate and Operations servers
BACKUPS	FreeBSD and Batch	Backs up Customer Data to storage server for disaster recovery. Backup Logs are created as each job runs

People

Centric Software has a staff of just over 400 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, these individuals are responsible for ensuring the growth of the company is executed in a way that allows strategic goals to be balanced with operational goals
- Sales/Pre-Sales: Sales / Pre-Sales organization is a globally distributed team operating out of three primary regions The Americas, Europe, Middle East, Africa and Russia ('EMEAR'), and Australia, New Zealand, China, Japan, Hong Kong, Singapore, Sri Lanka, S. Korea, India, Vietnam, etc. ('AsiaPAC'). This organization is responsible for promoting and selling Centric Software's products and solutions
- Marketing: The Centric Marketing team is a global organization responsible for developing, communicating and promoting awareness of Centric and it's solutions in a global arena. This includes running seminars, webinars, on-line events and ultimately driving leads for the sales organization
- Client Services: Client Services is a global organization split into two groups one focused on EMEAR and South America and the other focused on North America and AsiaPAC. These two groups are responsible for ensuring the Centric Products and Solutions are delivered, configured and taken to operational use by Customers. The teams provide ongoing services to those Customers looking to expand their use of the solutions
- Global Support: The Global Support Team operates out of three regions EMEAR, North America and AsiaPAC. This team provides maintenance services to support customers based on either Silver, Gold or Platinum support contacts. Customers work via a support portal (based on Atlassian Jira) to pose questions, log and track defects or browse the solution knowledge base

- Hosting Operations: The Hosting Operations organization is a globally distributed team tasked with providing the hosting services required to run Centric Software's Application solutions for hosted customers. This organization installs, runs and monitors each server and associated software necessary to ensure Centric meets/exceeds the posted SLA targets. Hosted Services are provided out of Centric Software's managed data center or via one of the Premium partners Amazon AWS, Microsoft Azure, IBM Cloud or Google Cloud Platform
- Research and Development ('R&D'): The R&D organization is responsible for developing, testing and releasing new versions of the Centric portfolio of products. The development team is a distributed team with developers in Seattle, WA, Campbell, CA, Montreal, Canada, and Chennai, India. This team also works with contractors based in Pune, India to help extend development capacity when required. This team utilizes an Agile software development methodology based on 2 week sprints. 2 Major and 2 minor releases are planned per year, but it typically ends up being 3 major and 4 minor releases
- Product Management: The Product Management organization is responsible for driving the company's product roadmap. The roadmap is balanced between Customer, Competitive and Strategic feature drivers. Roadmaps are reviewed once per month by the company's Product Council
- IT: IT Service desk, IT infrastructure, IT networking, IT system administration, company application support, information security, and IT operations personnel manage electronic interfaces and business implementation support and telecom:
    - The IT Service desk provides technical assistance to the Centric Software employees
    - The infrastructure, networking, and systems administration staff supports Centric Software's IT infrastructure, which is used by employees to conduct their day-to-day activities
    - The IT security staff monitor internal and external security threats and maintain current antivirus software
    - The IT staff maintains the inventory of IT assets

Data

Data, as defined by customers of Centric Software constitutes the following:

- Transaction data
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

Users login to the system and create data in the system through web interface. Integration with upstream and downstream business systems can be set up to allow import/export of data to/from the Centric 8 PLM system. This is done using batch jobs or through triggered requests via the Centric 8 representational state transfer ('REST') application programming interface ('API'). Data stored in the system can be encrypted at rest but this is only done based on Customer request.

Output reports are available in electronic portable document format ('PDF'), comma-delimited value file exports, or electronically from the application website. The availability of these reports is limited by job function. Reports delivered externally are sent using a secure method—encrypted e-mail, secure file transfer protocol ('FTP'), or secure websites or over connections secured by trusted security certificates. Centric Software uses hypertext transfer protocol secure ('HTTPS') with transport layer security ('TLS') 1.2 for interaction with the system.

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 Centric Software policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Centric Software team member.

Boundaries of the System

The scope of this report includes the PLM, SaaS System performed in the Campbell, California facilities.

This report does not include the cloud hosting services provided by AWS, Azure, GCP and IBM at their multiple facilities and the data center hosting services provided by Digital Realty at the Santa Clara, California.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common Criteria/Security, Availability, and Confidentiality criterion were applicable to the Centric Software's PLM, SaaS System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS, Azure, GCP and IBM at their multiple facilities and the data center hosting services provided by Digital Realty at the Santa Clara, California.

Subservice Description of Services

AWS provides flexible, scalable and secure IT infrastructure to businesses of all sizes around the world. With Amazon Web Services, customers can deploy solutions on a cloud computing environment that provides compute power, storage, and other application services over the Internet as their business needs demand. AWS affords business the flexibility to employ the operating systems, application programs, and databases of their choice.
Azure is a cloud computing platform for building, deploying and managing applications through a global network of Microsoft and third-party managed datacenters. It supports both Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) cloud service models and enables hybrid solutions that integrate cloud services with customers' on-premises resources.

GCP provides IaaS and PaaS cloud service models, allowing businesses and developers to build and run any or all of their applications on Google's Cloud infrastructure. Customers can benefit from performance, scale, reliability, ease of-use, and a pay-as-you-go cost model.

IBM provides on-demand IaaS to its customers, allowing them to create scalable bare metal server, virtual server, or hybrid computing environments, via IBM Cloud Computing Customer Portal, leveraging global data centers and points of presence.

Digital Realty delivers comprehensive space, power, and interconnection solutions that enable its customers and partners to connect with each other and service their own customers on a global technology and real estate platform. Digital Realty is a leading global provider of data center, colocation and interconnection solutions for customers across a variety of industry verticals ranging from cloud and information technology services, social networking and communications to financial services, manufacturing, energy, healthcare, and consumer products.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by AWS, Azure, GCP, IBM and Digital Realty 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	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.
		Electronic intrusion detection systems (IDS) are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		S3-Specific - S3 performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.
		S3-Specific - When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
		S3-Specific - Objects are stored redundantly across multiple fault-isolated facilities.
		S3-Specific - The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
		RDS-Specific - If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.
		Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.
Availability	A1.2	Datacenter Management team maintains datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.
		Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.
		Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses.
		Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities.
		Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
		Customer data is automatically replicated within Azure to minimize isolated faults.
		Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.
		Backup restoration procedures are defined, and backup data integrity checks are performed through standard restoration activities.
		Offsite backups are tracked and managed to maintain accuracy of the inventory information.
		Production data is encrypted on backup media.
		Azure services are configured to automatically restore customer services upon detection of hardware and system failures.

Subservice Organization - Google Cloud		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	Data center server floors network rooms and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval form authorized personnel and is controlled via badge access readers, biometric identification mechanism, and/or physical locks.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel through the use of real time video surveillance and/or alerts generated by security systems.
Availability	A1.2	Data centers are equipped with sensors to monitor temperature and humidity.
		Secure areas are equipped with fire detection alarms and protection equipment.
		Network rooms are connected to an UPS system and emergency generator power is available for at least 24 hours in the event of a loss of power.
		Shutoff valves are accessible, working properly, and known to key personnel.
		Data center power and network lines are protected against interception and damage.
		Data centers are equipped with redundant air con systems.
		Data centers are equipped with redundant network connections via different physical connections.
		Google performs and records routine preventative and regular maintenance.

Subservice Organization - IBM Cloud		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	SoftLayer's access to controlled areas is restricted (e.g. through the use of a card access or biometric systems) to authorized personnel only and requires documented approval from management. All individuals without authorized access to the controlled areas must sign in and be escorted by an individual with approved controlled area access.
		SoftLayer's levels of access rights to controlled areas are fully revalidated on a quarterly basis. A quarterly revalidation is performed to determine that a business need for access still exists.
		Terminated SoftLayer access to controlled areas is revoked within five business days of termination.
Availability	A1.2	Data centers are protected against environmental factors such as fire, water, and heat through the following: • Fire alarms • Fire extinguishers • Smoke alarms and • Fire suppression and extinguishing systems • Maintenance is performed on a periodic basis
		Power Distribution Units (PDU) and electrical panels exist in the data centers. Data center facilities are protected against power disruptions of failures through Uninterruptible Power Supply (UPS) or Emergency Power Supply (EPS) systems. Maintenance is performed on a periodic basis.
		Heating and cooling (HVAC) mechanisms exist, such as CRAC/CRAH units, air handlers and Chillers, in the data center to monitor and control temperature and humidity. Maintenance is performed on a periodic basis.

Subservice Organization - Digital Reality		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	Physical access controls are in place to restrict access to and within the data center facilities that include the following: • Two-factor authentication system for access to the data centers and suites • Personnel entering the data center facility were required to wear badges identifying them as visitor, employee, contractor or strategic partner • Visitor logs recorded visitor access to the data center facility • Visitors required an escort at all times
		Physical access request are documented and require the approval of the site manager.

Subservice Organization - Digital Reality		
Category	**Criteria**	**Control**
		A review of Digital Realty employees and contractors with physical access to customer suites is performed on a quarterly basis and unnecessary access is identified, modified and removed as necessary.
		A termination notification ticket is completed by HR and physical access is revoked by the corporate security team for Digital Realty employee and contractor terminations within one business day of termination.
		Visitors are required to surrender their badges upon exit. Access badges for visitors that do not require an escort are configured to expire at the end of the day.
		Surveillance cameras are in place to monitor and record access within the data centers. Surveillance cameras are located along the building perimeters and within the data centers.
		Digital surveillance systems are configured to retain video footage for the data centers for a minimum of 90 days.
Availability	A1.2	The data centers are equipped with the following environmental protection equipment: • Fire detection and suppression equipment • UPS systems • Generators • CRAC/CRAH units
		Management retains the inspection report received from third-party specialists evidencing completion of inspection and maintenance of the following according to a predefined schedule: • Fire detection and suppression equipment • UPS systems • Generators • CRAC/CRAH units
		Site security personnel are assigned daily operational procedures and tasks that include environmental system monitoring.
		Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.

Centric Software management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as SLAs. In addition, Centric performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling SOC2, ISO27001 reports
- Holding periodic discussions with vendors and subservice organizations
- Making regular site visits to Digital Realty subservice organizations' facilities but relying on SOC2 and ISO27001 certification/Attestation for Amazon AWS, Microsoft Azure, IBM Cloud and Google GCP subservices
- Reviewing attestation reports over services provided by vendors and subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

Centric Software'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 Centric Software's services to be solely achieved by Centric Software control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Centric Software'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 Centric Software.
2. User entities are responsible for notifying Centric Software 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 Centric Software 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 Centric Software services.
6. User entities are responsible for providing Centric Software with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Centric Software of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security, Availability, and Confidentiality Categories)

Security refers to the protection of

i. information during its collection or creation, use, processing, transmission, and storage and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability

Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.