A-LIGN

A-LIGN.com

Type 2 SOC 3

Prepared for:
Centric Software, Inc.

Year:
2025

CentricSoftware™

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

January 1, 2025 to December 31, 2025

Table of Contents

SECTION 1

ASSERTION OF CENTRIC SOFTWARE, INC. MANAGEMENT

ASSERTION OF CENTRIC SOFTWARE, INC. MANAGEMENT

January 5, 2026

We are responsible for designing, implementing, operating, and maintaining effective controls within Centric Software, Inc.'s ('Centric Software' or 'the Company') Centric PLM, Centric Visual Boards, Centric Planning, Centric Pricing & Inventory and Centric Market Intelligence Services throughout the period January 1, 2025 to December 31, 2025, 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*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Centric Software, Inc.'s Description of Its Centric PLM, Centric Visual Boards, Centric Planning, Centric Pricing & Inventory and Centric Market Intelligence Services throughout the period January 1, 2025 to December 31, 2025" and identifies the aspects of the system covered by our assertion.

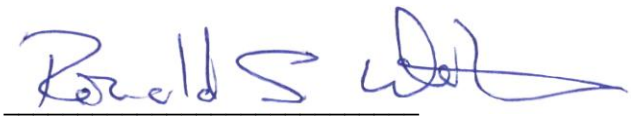
We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that Centric Software's service commitments and system requirements were achieved based on the trust services criteria. Centric Software'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 "Centric Software, Inc.'s Description of Its Centric PLM, Centric Visual Boards, Centric Planning, Centric Pricing & Inventory and Centric Market Intelligence Services throughout the period January 1, 2025 to December 31, 2025".

Centric Software uses Amazon Web Services ('AWS'), Microsoft Azure ('Azure'), and Google Cloud Platform ('GCP') to provide cloud hosting services and Digital Realty to provide data center colocation services (collectively, the 'subservice organizations'). 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.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Centric Software'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 Centric Software'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, 2025 to December 31, 2025 to provide reasonable assurance that Centric Software'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 Centric Software's controls operated effectively throughout that period.



Ronald Watson
CISO
Centric Software, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Centric Software, Inc.:

Scope

We have examined Centric Software, Inc.'s ('Centric Software' or 'the Company') accompanying assertion titled "Assertion of Centric Software, Inc. Management" (assertion) that the controls within Centric Software's Centric PLM, Centric Visual Boards, Centric Planning, Centric Pricing & Inventory and Centric Market Intelligence Services were effective throughout the period January 1, 2025 to December 31, 2025, 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*, in AICPA *Trust Services Criteria*.

Centric Software uses AWS, Azure, and GCP to provide cloud hosting services and Digital Realty to provide data center colocation 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 also provided the accompanying assertion (Centric Software assertion) about the effectiveness of controls within the system. When preparing its assertion, Centric Software 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

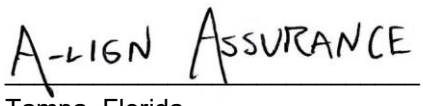
In our opinion, management's assertion that the controls within Centric Software's Centric PLM, Centric Visual Boards, Centric Planning, Centric Pricing & Inventory and Centric Market Intelligence Services were suitably designed and operating effectively throughout the period January 1, 2025 to December 31, 2025, 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, if complementary subservice organization controls and complementary user entity controls assumed in the design of Centric Software's controls operated effectively throughout that period.

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 and Saas Services during some or all of the period January 1, 2025 to December 31, 2025, business partners of Centric Software subject to risks arising from interactions with the PLM and Saas 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.



Tampa, Florida
January 5, 2026

SECTION 3

CENTRIC SOFTWARE, INC.'S DESCRIPTION OF ITS PLM AND SAAS SERVICES SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2025 TO DECEMBER 31, 2025

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. Centric innovations shorten the time to market, boost product innovation and reduce costs. Centric Software is majority-owned by Dassault Systèmes (Euronext Paris: #13065, DSY.PA).

Description of Services Provided

Centric Software's Centric PLM, Centric Visual Boards, Centric Planning, Centric Pricing & Inventory and Centric Market Intelligence Services consist of the following offerings:

- 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 Visual Boards pivot actionable data in a visual-first orientation to ensure robust, consumer-right assortments and product offers.
- Centric Planning is an innovative, cloud-native, Artificial Intelligence (AI) solution delivering end-to-end planning capabilities to maximize retail and wholesale business performance.
- Centric Pricing & Inventory leverages AI to drive margins and boost revenues by up to 18% via price and inventory optimization from pre-season to in-season to season completion.
- Centric Market Intelligence is an AI-driven market insight platform for data-informed decision-making on competitor offers and pricing as well as consumer trends and buying behavior.

The solution enables processing of the following tasks related to PLM:

- 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 the 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, 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 following solutions as:

- Permanent License
- Subscription License
- Software as a Service (SaaS)

The solution can be:

- Hosted by customers in their own environment.
- Hosted by Centric in either Standard Service or Premium and Premium High Availability (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 PLM themselves to having 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 services meet those expected by Customers' Information Technology (IT) organizations.

Components of the System

Infrastructure

Primary infrastructure used to provide Centric Software's Centric PLM, Centric Visual Boards, Centric Planning, Centric Pricing & Inventory and Centric Market Intelligence Services includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Firewalls	Palo Alto Next-Generation Firewalls	Filter traffic into and out of the private network as well as segment 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 ESXi Virtualization Software that hosts Web Servers, Application Servers, Database Services, Centric proprietary Servers and Centric PLM Application Servers
Network Attached Storage (NAS) Devices	Quality Network Appliance Provider (QNAP) Synology	NAS 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 Centric PLM, Centric Visual Boards, Centric Planning, Centric Pricing & Inventory and Centric Market Intelligence Services include 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 Datadog	Linux	Live Monitoring and notification of Internal IT systems infrastructure as well as Operations infrastructure for Standard and Cloud services
Endpoint Detection and Prevention, Security Information and Event Management, Tanium Patch Management, DataDog Monitoring, Office365 DLP	Security solutions	Leverage in class security solutions to help monitor assets for any internal/external threats to Centric Software or Customer information
OKTA	Identity Access Management	Act as the single source of truth for access management for assets and applications
Active Directory	Identity Access Management	Act as the single source of truth for access management for assets and applications
OPSWAT MetaDefender	SaaS appliance	Allow Centric employees remote access to Centric Corporate and Operations networks
Remote Desktop Gateway Servers	Microsoft Windows Server 2022	Provide Centric employees to remote desktop into specific IT and Operations servers for Administrative activities
Veeam	Microsoft Windows Server 2022	Backs up Images of key Corporate and Operations servers
Backups	Automated through cloud service provider modules	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 1300 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 its 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 AWS, Azure, or GCP
- 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, Washington, Campbell, California, 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 by the company's Product Council
- Information Security: The team is responsible for ensuring the safety of physical and digital assets globally. The dedicated team works with business units to understand and strengthen the overall security footprint and ensure compliance with regulatory requirements
- 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 a web interface. Integration with upstream and downstream business systems can be set up to allow import/export of data to/from the Centric PLM system. This is done using batch jobs or through triggered requests via the Centric PLM 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 requests.

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 (SFTP), 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. 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.

Physical Security

The in-scope system and supporting infrastructure are hosted by AWS, Azure, GCP, and Digital Realty. As such, AWS, Azure, GCP, and Digital Realty are responsible for the physical security controls for the in-scope system. Please see the "Subservice Organizations" section below for a detailed listing of controls owned by AWS, Azure, GCP, and Digital Realty.

Logical Access

Centralized access management is key to ensuring that the correct Centric Software employees have access to the correct data and systems and at the correct level. Centric Software access controls are guided by the principle of least privilege and need-to-know. These controls apply to information and information processing systems at the application and operating system layers, including networks and network services. Ensuring only people who require access to a system or service receive access helps improve Centric Software's overall security posture by limiting the number of accounts with access and reducing the overall likelihood of an account being compromised. Provisioning is based on predetermined roles with business justification and management approval. Role-based authentication is used whenever possible to make this control easier and to segregate out this function from that of other system functions.

Centric Software's IT compiles Role-Based Entitlement templates that are used during the onboarding process and throughout the employment tenure of a Centric Software employee. Access required as part of the employee's onboarding is requested using the New Hire/Departure Form.

The Human Resources Management system sends a notification to relevant personnel, or system, in the event of a termination or a job transfer of an information system user. Notification can be manual or automated. Logical access that is no longer required in the event of a termination or a transfer is documented, communicated to management, and revoked.

On at least an annual basis, collect the current access listings of systems and correlate them against a list of active employees derived from data originating in Automatic Data Processing (ADP), human resources management software. If any users are found to have active system access that are not current, Centric Software employees open an access removal ticket to begin the access de-provisioning process.

Access to a system is reviewed based on the job roles and departments, a system owner determines which roles/departments have access to their system. These reviews occur on an annual basis. If a job role is deemed to be not applicable to have access to a system, a secondary review is submitted by the team member's manager to determine if access is required.

Access is reviewed by a team member's manager for each system they have access for continued validation. These reviews occur on an annual basis or when a system owner identifies out-of-scope access, and a secondary review is required.

Where and only if applicable, appropriate, and technically feasible, and with the understanding that Centric Software is a cloud-native, Multifactor Authentication (MFA) will be enabled on user accounts accessing internal systems. A virtual private network (VPN) will be used to ensure that network traffic from the teleworker client to organization servers is encrypted to organization standards. A secure Remote Desktop Gateway requiring domain authentication is also employed to keep internal remote sessions secure.

The single source of truth for user accounts is the Active Directory Domain Controller. Employees and contractors are to sign in using their provided Centric Software credentials. Any MFA linked applications on-premises and in cloud are tied to the same complexity, security settings and account configurations that stem from the Active Directory environment whenever possible.

Computer Operations - Backups

Centric Software uses the software Veeam Backup and Replication 10.0 to create backup jobs for each production Virtual Machine (VM) on the Nutanix Production Cluster. Each VM Backup is encrypted and stored on the Synology NAS. The backup job is using either Veeam Agent or direct VMware vCenter to create the backups, which are then stored onto the Synology.

There are 3 SLAs that production servers follow:

- Every Hour for 24 Hours
- Every Day for 7 Days
- Every Week for 5 Weeks

To encrypt data blocks in backup files and files archived to tape, Veeam Backup and Replication uses the 256-bit Advanced Encryption Standard (AES) with a 256-bit key length in the Cipher Block Chaining (CBC) mode. To generate a key based on a password, Veeam Backup and Replication uses the Password-Based Key Derivation Function (PKCS) #5 version 2.0. Veeam Backup and Replication uses 10,000 keyed-hashing for message authentication (HMAC-SHA1) iterations and a 512-bit salt.

Centric Software restores any VM per request by either any active account manager or support team including the customer themselves. The time frame ranges based on the size of the VM, but in most fair conditions, a VM can be restored as fast as 30 minutes but can take up to 6 hours.

Computer Operations - Availability

Security Incident Response policies exist that provide a concise overview of how Centric Software will respond to an incident affecting its information security, describe the facilities that are in place to help with the management of the incident, define how decisions will be taken with regard to the response to an incident and explain how communication within the organization and with external parties will be handled.

Centric Software monitors the capacity and utilization of the infrastructure that runs internal systems and customer instances. By using internal tools, Centric evaluates the need for additional infrastructure to meet growth and compute demands. Capacity Monitoring includes:

- Disk Storage
- Random Access Memory (RAM) and Central Processing Unit (CPU) usage
- Network bandwidth

- Virtual Private Cloud provisioning

Centric Software has a responsibility to uphold the confidentiality, integrity and availability of the data held on its IT systems on and off site which includes systems and services supplied by third-parties. Centric has an obligation to provide appropriate and adequate protection of IT assets whether it is IT systems on premise, in the Cloud or systems and services supplied by third-parties. Effective implementation of the patch management policy reduces the likelihood of compromise which may come from a malicious threat actor or threat source. Security patches should be up to date for IT systems which are being designed and delivered by third-party suppliers prior to going operational. Third-party suppliers much be prepared to provide evidence of up-to-date patching before IT systems are accepted into service and thus become operational.

The in-scope system and supporting infrastructure is hosted by AWS, Azure, GCP, and Digital Realty. As such, AWS, Azure, GCP, and Digital Realty are responsible for the availability controls for the in-scope system. Please see the “Subservice Organizations” section below for a detailed listing of controls owned by AWS, Azure, GCP, and Digital Realty.

Change Control

Centric Software maintains a repository of documented policies and procedures to guide personnel in implementing application and infrastructure changes. Centric Software change control procedures include change request and initiation processes, documentation requirements, development practices, QA testing requirements and required approval procedures.

Jira, a ticketing system, is utilized to document the change control requests and the results of those requests. Procedures for changes in the application and implementation of new changes are driven by Development and QA (for C8 changes) and by Hosting for hosted customer infrastructure changes. QA testing results are documented by the Centric QA team. Development and testing are performed in an environment that is logically separated from customer and internal production environments. Changes are approved by the QA team prior to the deployment to any production environment and documents those approvals within the QA documentation system.

Infrastructure changes for hosted customer environments are driven by the Hosting organization. These changes are tested and proven in internal, non-customer, non-production environments before they can be deployed for customers.

Infrastructure changes for internal resources are driven by the IT organization. These changes are tested and validated in internal non-production environments before they can be deployed to production environments. The IT department requests approval from the Hosting department in advance for changes to internal resources that impact hosted customers. These requests are documented in e-mail or the internal ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to release to the customer’s production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers. Version updates and changes are tracked through the QA Team’s ticketing system.

Centric Software has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Centric Software reviews proposed operating system patches and updates to determine whether the patches are applied. Centric is 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. When patches are required, the Centric Hosting staff validates that the patches have been installed and if applicable that reboots have been completed. The installation of patches is tracked in the Hosting ticketing system.

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. Network Address Translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

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.

Dynamic Application Security Testing (DAST) and vulnerability scanning are conducted to measure the security posture of the Centric PLM Application by a third-party vendor. The third-party vendor simulates a disgruntled/disaffected insider and exploits threats based on Open Web Application Security Project (OWASP) identified threats.

Authorized employees may access the system from the Internet through the use of VPN technology.

Boundaries of the System

The scope of this report includes the Centric PLM, Centric Visual Boards, Centric Planning, Centric Pricing & Inventory and Centric Market Intelligence Services performed in the Campbell, California facility.

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

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Centric Software's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Centric Software's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

Centric Software's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- If a gap in skills is identified, training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

Centric Software's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is briefed on regulatory and industry changes affecting the services provided e.g., introduction of GDPR for European entities and California Consumer Privacy Act.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole. These include board meetings and Operations reviews that rotate between the different executive departments - Sales and Marketing, Finance/HR, RandD/IT/Hosting Operations/Security, Services and Support.

Organizational Structure and Assignment of Authority and Responsibility

Centric Software's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Centric Software's assignment of authority and responsibility activities includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Centric Software's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensure the service organization is operating at maximum efficiency. Centric Software's human resources policies and practices relating to employee hiring, orientation, training, evaluation, counselling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

Risk Assessment Process

Centric Software's risk assessment process identifies and manages risks that could potentially affect Centric Software's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Centric Software identifies the underlying sources of risk, measures the impact to the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Centric Software and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

Centric Software addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meet the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Centric Software's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Centric Software's Centric PLM, Centric Visual Boards, Centric Planning, Centric Pricing & Inventory and Centric Market Intelligence Services; as well as the nature of the components of the system result in risks that the criteria will not be met. Centric Software addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meet the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Centric Software's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication are an integral component of Centric Software's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, IT. At Centric Software, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, all-hands meetings are held to provide staff with updates on the firm and key issues affecting the organization and its employees. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Centric Software personnel via e-mail messages and are available to read at any time through the internal website.

Specific information systems used to support Centric Software's system are described in the Description of Services section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Centric Software's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored.

On-Going Monitoring

Centric Software's management conducts QA monitoring regularly, and additional training is provided based upon results of monitoring procedures.

Management's close involvement in Centric Software's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Centric Software's personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common Criteria/Security, Availability, and Confidentiality criteria were applicable to Centric Software's Centric PLM, Centric Visual Boards, Centric Planning, Centric Pricing & Inventory and Centric Market Intelligence Services.

Subservice Organizations

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

Subservice Description of Services

AWS provides flexible, scalable and secures IT infrastructure to businesses of various sizes around the world. With AWS, customers can deploy solutions on a cloud computing environment that provides computing power, storage, and other application services over the Internet as their business needs demand. AWS offers businesses 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 data centers. 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 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.

Digital Realty delivers comprehensive space, power, and interconnection solutions that enable its customers and partners to connect and service their 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 IT 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 sub service 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 sub service organization controls should be implemented by AWS, Azure, GCP, 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, CC7.2	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.
		Electronic intrusion detection systems (IDS) are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
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.
		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, 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, CC7.2	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.
		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 - GCP		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	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 from 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 - Digital Realty		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Physical access controls are in place to restrict access to and within the data center facilities that include the following: • MFA 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 always required an escort
		Physical access request is documented and require the approval of the site manager.
		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.

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 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 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 systems 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.