Report on Siemens Industry Software, Inc.'s Cloud Application Services (CApS) SaaS Operations and Managed Services offerings Relevant to Security, Availability, and Confidentiality Throughout the Period June 1, 2024 to May 31, 2025

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

SIEMENS

Table of Contents

Section 1

Independent Service Auditor's Report 3

Section 2

Assertion of Siemens Industry Software, Inc. Management 6

Attachment A

Siemens Industry Software, Inc.'s Description of the Boundaries of Its Cloud Application Services (CApS) SaaS Operations and Managed Services offerings 9

Attachment B

Principal Service Commitments and System Requirements 20

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Siemens Industry Software, Inc. ("Siemens")

Scope

We have examined Siemens' accompanying assertion titled "Assertion of Siemens Industry Software, Inc. Management" (assertion) that the controls within Siemens' Cloud Application Services (CApS) SaaS Operations and Managed Services offerings (system) were effective throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that Siemens' 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 (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*.

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

Siemens uses subservice organizations to provide data center colocation and managed services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Siemens, to achieve Siemens' service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Siemens' controls. 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.

Siemens' CApS offerings and Managed Services uses Siemens' SISW Xcelerator Services (SXS) Enterprise Core to provide enterprise and governance control activities. The description of the boundaries of the system indicates that complementary corporate-level controls of Siemens' SXS Enterprise Core that are suitably designed and operating effectively are necessary, along with controls at Siemens' CApS offerings and Managed Services, to achieve Siemens' service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary corporate-level controls assumed in the design of Siemens' CApS offerings and Managed Services controls. Our examination did not include such complementary corporate-level controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Siemens 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 Siemens' service commitments and system requirements were achieved. Siemens has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Siemens 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 American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

Our examination included:

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

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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Siemens' Cloud Application Services (CApS) SaaS Operations and Managed Services offerings were effective throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that Siemens' service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls, complementary user entity controls, and complementary corporate-level controls assumed in the design of Siemens' controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Greenwood Village, Colorado
July 29, 2025

Section 2

Assertion of Siemens Industry Software, Inc. Management

SIEMENS

Assertion of Siemens Industry Software, Inc. ("Siemens") Management

We are responsible for designing, implementing, operating and maintaining effective controls within Siemens' Cloud Application Services (CApS) SaaS Operations and Managed Services offerings (system) throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that Siemens' 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 (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

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

Siemens uses subservice organizations for data center colocation and managed services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Siemens, to achieve Siemens' service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Siemens' controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

Siemens' CApS offerings and Managed Services uses Siemens' SISW Xcelerator Services (SXS) Enterprise Core to provide enterprise and governance control activities. The description of the boundaries of the system indicates that complementary corporate-level controls of Siemens' SXS Enterprise Core that are suitably designed and operating effectively are necessary, along with controls at Siemens' CApS offerings and Managed Services, to achieve Siemens' service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary corporate-level controls assumed in the design of Siemens' CApS offerings and Managed Services controls. The description of the boundaries of the system does not disclose the actual controls at Siemens' SXS Enterprise Core.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that Siemens' service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls, complementary user entity controls, and complementary corporate-level controls assumed in the design of Siemens' controls operated effectively throughout that period. Siemens' 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 attachment B.

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 June 1, 2024 to May 31, 2025, to provide reasonable assurance that Siemens' service commitments and system requirements were achieved based on the applicable trust services criteria.

Siemens Industry Software, Inc.

Attachment A

Siemens Industry Software, Inc.'s Description of the Boundaries of Its Cloud Application Services (CApS) SaaS Operations and Managed Services offerings

Type of Services Provided

Siemens Industry Software, Inc. (“SISW” or “the Company”) is a global innovator focusing on digitization and automation for process and manufacturing industries. Though headquartered in Plano, Texas, United States, SISW has thousands of employees globally. SISW's Cloud Application Services (CApS) and Managed Services is a service organization whose operations team extends Teamcenter X (TcX), Polarion X, and Capital X services to customers as a cloud-hosted option for traditionally on-premises applications, expanding on the scalability and availability of these enterprise solutions. CApS is responsible for the deployment and maintenance operations of all three solutions on the SISW cloud, transferring the responsibilities for continued monitoring, patching, and disaster recovery preparedness from customer operations teams to SISW.

The boundaries of the system in this section details CApS SaaS Operations and Managed Services offerings for Teamcenter and Polarion (“CApS SaaS Operations and Managed Services offerings” or “the system”). Any other Company services are not within the scope of this report.

CApS Offerings

TcX is a single tenant or multitenant offering that is packaged as TcX Essentials, TcX Standard, TcX Advanced, or TcX Premium that provides varying levels of product management lifecycle solution enabling organizations to access product information; build a bill of materials (BOM); and manage 3D designs, documents, and software. Polarion X is an integrated application lifecycle management system enabling individuals to collaborate, design, build, and test software systems. Capital X is a software suite that enables the engineering of electrical systems for large platforms such as cars, aircraft, and sophisticated machines.

Teamcenter System Managed Services

The Teamcenter user interface helps people across the organization take part in the product development process by taking control of product data and processes, including 3D designs, electronics, embedded software, documentation, and BOM. Organizations can use Teamcenter by leveraging product information across more domains and departments, such as manufacturing, quality, cost engineering, compliance, service, and supply chain.

Teamcenter features include the following: Capacity Asset Lifecycle Management, Adaptable Product Lifecycle Management (PLM) Foundation, BOM Management, Change Management and Workflow, Document Management and Publishing, Electrical Design Management, Environment Compliance and Product Sustainability, Manufacturing Data and Process Management, Mechanical Design Management, Model-Based Systems Engineering, Product Configuration, Product Cost Management, Product Requirements Engineering, Program Planning and Project Execution, Search and Analytics, Simulation Management, Software Design and Asset Management, Sourcing and Supplier Integration, Streamline Service Operations, Visualization, Digital Mockup, and Virtual Reality. Some of Teamcenter’s additional services include, but are not limited to:

- Computer-aided design (CAD) integration
- Flexible support window
- Automated backup and disaster recovery
- Minimum one-year contract and monthly invoicing
- 24x7 cloud infrastructure support
- Business solution, user, and application support

- Access to a secure ticketing system
- Service-level agreement management
- Review plan meeting
- HTTPS connectivity
- Minor enhancements
- Proactive monitoring and alerting for servers and resources
- Windows system, security, and software event log monitoring

Polarion System Managed Services

Polarion is a unified application lifecycle management solution where users can define, build, test, and manage complex software systems in a unified, 100% browser-based solution that serves small teams or thousands of users. Polarion features include the following: Polarion Application Lifecycle Management (ALM) Solution, Polarion Requirements Management, Polarion Quality Assurance (QA) Solution, Add-on Variants for Industry-Leading Technology and Integrations, Polarion Pro for Unified Change Management, Polarion Reviewer for External Reviews, e-signatures and approvals, and software-as-a-service (SaaS) offerings.

The Boundaries of the System Used to Provide the Services

The boundaries of CApS SaaS Operations and Managed Services offerings are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of CApS SaaS Operations and Managed Services offerings.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

The Company utilizes AWS and Azure to provide the resources to host CApS SaaS Operations and Managed Services offerings. The Company leverages the experience and resources of AWS and Azure to quickly and securely scale as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the individual services' architecture within AWS and Azure to ensure the availability, security, and resiliency requirements are met.

The Company also leverages Auth0's authentication services platform to provide external identity management services, taking advantage of Auth0's global footprint to provide the required scalability and resiliency demanded by global customers. All CApS offerings within the scope of this description support the use of SISW's deployment of Auth0 services to provide for a consistent authentication mechanism across the portfolio.

SISW is a wholly owned subsidiary of Siemens AG and relies on Siemens Corporate IT services for providing redundant, secure infrastructure services for development environments, based out of Siemens data centers across the globe.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Infrastructure	
Production Tool	**Business Function**
Amazon Relational Database Service (Amazon RDS)	Customer data storage
Amazon Elastic Compute Cloud (Amazon EC2)	Application servers
AWS Identity and Access Management (IAM)	Identity and access management
Amazon CloudFront	Content distribution network
Amazon Simple Storage Service (Amazon S3), Amazon FSx, Amazon Elastic Block Store (Amazon EBS)	Cloud storage
Amazon RDS	Customer data storage
Cloud Custodian	Policy management
Siemens Corporate Public Key Infrastructure (PKI) services	Identification and authentication services
Azure SQL MI	Customer data storage
Virtual machine (VM)	Application servers
IAM	IAM
Azure Gateway	Proxy, load balancer
Blob Storage	Cloud storage
Azure NetApp files	Cloud storage

Software

Software consists of the programs and software that support CApS SaaS Operations and Managed Services offerings operations (operating systems [OSs]), middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor CApS SaaS Operations and Managed Services offerings include the following business functions, as shown below:

- Deployment image building
- Help desk ticketing systems
- Logging and monitoring tools
- Change management tools
- Source code and orchestration tool
- Privileged access management (PAM) tool
- Infrastructure orchestration and automation
- User directory services
- File storage

- Container images
- Security monitoring
- Security monitoring, infrastructure and application event monitoring, capacity logging and monitoring
- Software testing and component vulnerability scanning tools

People

The Company develops, manages, and secures CApS SaaS Operations and Managed Services offerings via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Human Resources (HR)	Responsible for onboarding new personnel, defining the roles and positions of new hires, performing background checks, and facilitating the employee termination process.
CApS Operations	Responsible for the deployment and maintenance of Polarion X, Capital X, and TcX and Managed Services.
Cloud Security Operations (CSO)	Responsible for managing operations and the security of the production cloud environments.
Capital, Polarion, and Teamcenter Software Development	Software development teams that produce the core software and requisite cloud-specific configuration kits to operate the software on the cloud infrastructure.
Services Engineering	Responsible for the development, testing, deployment, and maintenance of new code for CApS offerings for the Polarion System.
Services Delivery	Responsible for delivery, support, incident management, backup, and restoration of CApS offerings for Polarion System service delivery.
Security and Compliance Practice	Responsible for access control, vulnerability scans, penetration tests, remediation plans, certifications, risk assessments, annual self-assessments, BCP/DRP planning and testing, third-party assessments, policies, procedures, processes, and overall security posture of the production environment.
Product Management	Responsible for overseeing the product lifecycle, including adding new product functionality.
Global HR	Responsible for HR functions including termination and offboarding actions for employees.
Information Security Management	Responsible for documenting information about the security program and its supporting policies.

Procedures

Procedures include the automated and manual procedures involved in the operation of CApS SaaS Operations and Managed Services offerings. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, IT, and HR. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of CApS SaaS Operations and Managed Services offerings:

Procedures	
Procedure	**Description**
Logical Access	How the Company restricts logical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical security deviations.
Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.
Vulnerability Management	How the Company identifies, evaluates, and remediates vulnerabilities stemming from hardware and software that are essential for the operation of the system.
Personnel Management	How the Company recruits, develops, and promotes skilled personnel who are essential for the continued operation of the system.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the user interface and application programming interface (API), the customer or end user defines and controls the data they load into and store within each application's specific production network, within a specifically defined database schema, or within a virtual storage volume. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Encryption is enabled for data stores housing sensitive customer data.

The following table details the types of data contained in the production application for CApS SaaS Operations and Managed Services offerings:

Data	
Production Application	**Description**
Capital X, Polarion X	The Company stores core product information, basic user information required to access or use the product, and customer tenancy operational information.
TcX	The Company stores core product information, basic user information required to access or use the product, and customer tenancy operational information.
Log Information	The Company logs information about customers and their users, including Internet Protocol (IP) addresses. Log files are immutable records of computer events about an OS, application, or user activity, which form an audit trail. These records may be used to assist in detecting security violations, performance problems, and flaws in applications.
Teamcenter Managed Services	The Company keeps track of user activity in relation to the types of services customers and their users use, the configuration of their computers, and performance metrics related to their use of the services.
	The Company logs information about customers and their users, including IP addresses. Log files are immutable records of computer events about an OS, application, or user activity, which form an audit trail. These records may be used to assist in detecting security violations, performance problems, and flaws in applications.
Polarion Managed Services	The Company keeps track of user activity in relation to the types of services customers and their users use, the configuration of their computers, and performance metrics related to their use of the services.
	The Company logs information about customers and their users, including IP addresses. Log files are immutable records of computer events about an OS, application, or user activity, which form an audit trail. These records may be used to assist in detecting security violations, performance problems, and flaws in applications.

Complementary User Entity Controls (CUECs)

The Company's controls related to CApS offerings and Managed Services cover only a portion of overall internal control for each user entity of CApS offerings and Managed Services. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls, taking into account the related CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls
CC2.1	• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames. • Controls to provide reasonable assurance that the Company is notified of changes in: – User entity vendor security requirements – The authorized users list
CC2.3	• It is the responsibility of the user entity to have policies and procedures to: – Inform their employees and users that their information or data is being used and stored by the Company. – Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
CC6.1	• User entities grant access to the Company's system to authorized and trained personnel. • Controls provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the company. • User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.
CC6.2	• User entities request access to the Company's system for authorized and trained personnel via the CApS offerings function. • User entities must inform immediately the Company's CApS offerings function via approved communication channels of any change in access for its users or consumers of the Company's TcX product.

Complementary Corporate-Level Controls

The Company relies on the SISW Xcelerator Services (SXS) Enterprise Core enterprise and governance controls. SXS Enterprise Core controls are performed and monitored by corporate functions. Therefore, each user entity's internal control must be evaluated in conjunction with SISW's controls, taking into account the related controls expected to be implemented at SXS Enterprise Core as described below.

Criteria	Complementary Corporate-Level Controls
CC1.1 CC1.5	• SXS Enterprise Core is responsible for ensuring that the code of conduct describes employee responsibilities and expected behavior regarding data and information system usage. • SXS Enterprise Core is responsible for ensuring that the confidentiality agreement prohibits the disclosure of information and other data to which the employee has been granted access. • SXS Enterprise Core is responsible for ensuring that new personnel that are offered employment are subject to verification checks prior to their start dates, conforming to the organization's policy on eligibility verifications. • SXS Enterprise Core is responsible for ensuring that there are documented disciplinary actions in a formalized sanctions policy for employees and contractors who violate the code of conduct.

Criteria	Complementary Corporate-Level Controls
CC1.2 CC1.4	• SXS Enterprise Core is responsible for ensuring that the Board of Directors provides written consent to approve actions annually and that the Board of Directors includes directors that are independent from management. • SXS Enterprise Core is responsible for ensuring that the Board of Directors has documented oversight responsibilities relative to internal control.
CC1.3 CC2.2	• SXS Enterprise Core is responsible for ensuring that management has established defined roles and responsibilities to oversee the implementation of the security and control environment. • SXS Enterprise Core is responsible for ensuring that job descriptions are documented for employees supporting the service including authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.
CC1.4 CC2.2	• SXS Enterprise Core is responsible for ensuring that managers are required to complete performance appraisals for direct reports at least annually. • SXS Enterprise Core is responsible for ensuring that employees complete security awareness training upon hire and annually thereafter.
CC2.2	• SXS Enterprise Core is responsible for ensuring that a formalized whistleblower policy is established and an anonymous communication channel is available for employees to report potential security issues or fraud concerns.
CC2.3	• SXS Enterprise Core is responsible for ensuring that formal information sharing agreements are in place with critical vendors and subservice organizations. These agreements include confidentiality commitments applicable to that entity.
CC3.1 CC3.2 CC3.3 CC3.4 CC5.1 CC5.2 CC5.3 CC9.1	• SXS Enterprise Core is responsible for ensuring that a documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. • SXS Enterprise Core is responsible for ensuring that risk objectives are specified in its annual risk assessment to enable the identification and assessment of risk related to the objectives.
CC5.3	• SXS Enterprise Core is responsible for ensuring that the information security policies and procedures are documented, define the information security rules and requirements for the service environment, and are reviewed at least annually and updated as needed. • SXS Enterprise Core is responsible for ensuring that formal procedures are documented that outline requirements for vulnerability management and system monitoring and that the procedures are reviewed at least annually. • SXS Enterprise Core is responsible for ensuring that a vendor management program is in place. • SXS Enterprise Core is responsible for ensuring that a formal policy is in place that includes change management roles and responsibilities; criteria for risk assessment, categorization, and prioritization of changes; approvals for implementation of changes; requirements for the performance and documentation of tests, including rollback plans; requirements for segregation of duties during development, testing, and release of changes; and requirements for the implementation and documentation of emergency changes. • SXS Enterprise Core is responsible for ensuring that a formal security and software development life cycle (SDLC) methodology is in place that governs the project planning, design, acquisition, testing, implementation, maintenance, and decommissioning of information systems and related technologies.

Criteria	Complementary Corporate-Level Controls
CC6.5 C1.2	• SXS Enterprise Core is responsible for ensuring that electronic media containing confidential information is purged or destroyed and that evidence of the purging or destruction is retained for each device destroyed.
CC6.7	• SXS Enterprise Core is responsible for ensuring that a mobile device management system is in place to centrally manage mobile devices supporting the service. • SXS Enterprise Core is responsible for ensuring that portable and removable media devices are encrypted when used.
CC6.8	• SXS Enterprise Core is responsible for ensuring that anti-malware technology is deployed for environments commonly susceptible to malicious attack and is configured to be updated routinely, logged, and installed on all relevant production servers and endpoints.
CC7.3	• SXS Enterprise Core is responsible for ensuring that security events are logged, tracked, resolved, and communicated to affected parties by management according to the Company's security incident response policies and procedures. All events are evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives.
CC9.2	• SXS Enterprise Core is responsible for ensuring that a third-party attestation report review or vendor risk assessment is performed at least annually for all TcX and CApS offerings critical vendors and subservice organizations. Exceptions noted in the reports or risk assessments are evaluated to determine their impact on the service. • SXS Enterprise Core is responsible for ensuring that a third-party attestation report review or vendor risk assessment is performed at least annually for all Teamcenter Managed Services critical vendors and subservice organizations. Exceptions noted in the reports or risk assessments are evaluated to determine their impact on the service. • SXS Enterprise Core is responsible for ensuring that a third-party attestation report review or vendor risk assessment is performed at least annually for all Polarion System Managed Services critical vendors and subservice organizations. Exceptions noted in the reports or risk assessments are evaluated to determine their impact on the service.
A1.1	• SXS Enterprise Core is responsible for ensuring that production system capacity is evaluated continuously, and system changes are implemented to help ensure that processing capacity can meet demand.
CC5.3 C1.1	• SXS Enterprise Core is responsible for ensuring that a data classification policy is documented to help ensure that confidential data is properly secured and restricted to authorized personnel. • SXS Enterprise Core is responsible for ensuring that confidential or sensitive customer data is prohibited by policy from being used or stored in non-production systems or environments.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS and Azure as subservice organizations for data center colocation and managed services. The Company’s controls related to CApS SaaS Operations and Managed Services offerings cover only a portion of the overall internal control for each user entity within the CApS SaaS Operations and Managed Services offerings portfolio.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place at the organizations related to:

- Physical security controls to protect the data environment from loss of confidentiality, tampering, and availability threats
- Environmental protection to mitigate the risk of fires, power loss, climate, and temperature variabilities
- Backup, recovery, and redundancy controls related to availability

Through its operational activities, Company management monitors the services performed by the subservice entities to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreements, stay informed of changes planned at the hosting facilities, and relay any issues or concerns to AWS and Azure management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to CApS SaaS Operations and Managed Services offerings to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls, taking into account the related CSOCs expected to be implemented at AWS and Azure as described below.

Criteria	Complementary Subservice Organization Controls
CC6.1	• AWS and Azure are responsible for encrypting databases in its control.
CC6.4	• AWS and Azure are responsible for restricting data center access to authorized personnel. • AWS and Azure are responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5 C1.2	• AWS and Azure are responsible for securely decommissioning and physically destroying production assets in their control.
CC7.2 A1.2	• AWS and Azure are responsible for the installation of fire suppression and detection and environmental monitoring systems at their data centers. • AWS and Azure are responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS and Azure are responsible for overseeing the regular maintenance of environmental protections at their data centers.
CC6.6 CC6.8 CC7.2	• AWS is responsible for patching infrastructure as a part of routine maintenance and as a result of identified vulnerabilities in the App.
CC2.1 CC7.1 CC7.2 CC7.3	• AWS is responsible for performing internal and external network vulnerability scans and remediating all critical and high vulnerabilities identified during the scans.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of CApS SaaS Operations and Managed Services offerings. Commitments are communicated through the Universal Customer Agreement, Cloud Support and Service Level Framework, Data Privacy Terms, and Statements of Work.

System requirements are specifications regarding how CApS SaaS Operations and Managed Services offerings should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to CApS offerings include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• The Company will implement appropriate technical safeguards to protect client data, based on the International Standard for Organization (ISO) 27001 Information Security framework. • The Company will restrict employee access based on job role and business need. • The Company will implement authentication mechanisms to protect service and administrative consoles. • The Company will enable timely modification, revocation, and deprovisioning of employee access. • The Company will log and monitor all access and administrative activities within CApS. • The Company will ensure logical segregation of production and non-production environments. • The Company will implement formal processes to control and perform changes to developed applications.	• Information security standards • Logical access standards • Access review standards • Employee provisioning and deprovisioning standards • Risk and vulnerability management standards • Change management standards • Incident handling and response standards • Firewall standards • System hardening standards
Availability	• The Company will ensure the system is available for use 98% (Standard), 99.5% (Enhanced), and 99.95% (Maximum) of the time, monthly, for the Company's standard cloud support deployments. • The Company will use commercially reasonable efforts to notify customers at least 24 hours prior to the occurrence of scheduled downtime for CApS offerings. • The Company shall, in the event of a continuity event, recover services: – Within 24 hours (recovery time objective of less than 24 hours) and ensure data restoration to be at a point within 24 hours (recovery point objective of less than 24 hours) at the Standard service level tier	• System logging and monitoring standards • Backup and recovery standards • Incident handling and response standards • Business continuity standards

Trust Services Category	Service Commitments	System Requirements
	– Within 12 hours (recovery time objective of less than 12 hours) and ensure data restoration to be at a point within 12 hours (recovery point objective of less than 12 hours) at the Enhanced service level tier – Within 2 hours (recovery time objective of less than 2 hours) and ensure data restoration to be at a point within 2 hours (recovery point objective of less than 2 hours) at the Maximum service level tier	
Confidentiality	• The Company will disclose confidential information only to those employees and third parties that are bound by confidentiality agreements. • The Company will use reasonable care to protect against unauthorized use and disclosure of customer information. • The Company will encrypt customer data at rest and transmitted over public networks. • The Company will irretrievably erase data or destroy storage media before disposing of or reusing IT systems.	• Data classification and handling standards • Encryption standards • Information sharing standards

The Company's principal service commitments and system requirements related to Managed Services include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• The Company will ensure that system access is granted to authorized personnel only. • The Company will secure the information system from unauthorized access, use, modification, disclosure, destruction, threats, or hazards. • The Company will notify the customer without undue delay in the event the Company becomes aware of a security incident.	• Access control policies and procedures • Password policies and procedures • Deployment and maintenance of Amazon Web Services (AWS) and Microsoft Azure (Azure) • Patch management policies and procedures • Network segmentation • Firewall standards • Vendor policies and procedures • Protection of data in transit • Monitoring and logging

Trust Services Category	Service Commitments	System Requirements
Availability	• The Company will use commercially reasonable efforts to functionally maintain the cloud services 24 hours per day, 7 days per week, except for planned downtime and any unavailability caused by circumstances beyond the Company's reasonable control. • The Company will provide the ability to recover and restore customer data. • The Company will ensure that the system is available 98% of the time for standard cloud support deployments.	• Backup and recovery policies and procedures • Business continuity plans (BCPs) and disaster recovery plans (DRPs) and testing • Multi-location strategy for the production environment • System capacity evaluation and planning
Confidentiality	• The Company will prevent the disclosure and protect the confidentiality of customer unrestricted information. • The Company will ensure that personnel engaged in providing the services maintain the confidentiality of customer data. • The Company will maintain all customer data as confidential and will not disclose information to any unauthorized parties without written consent. • Upon termination or expiration of services, the Company will delete or destroy customer data.	• Data classification policies and procedures • Data retention and disposal policies and procedures