Report on Siemens Industry Software, Inc.'s Xcelerator as a Service (XaaS) Enterprise Core Relevant to Security, Availability, and Confidentiality Throughout the Period October 1, 2022 to March 31, 2023

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

Table of Contents

Section 1

Section 2

Attachment A

Attachment B

Attachment C

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' Xcelerator as a Service (XaaS) Enterprise Core (system) were effective throughout the period October 1, 2022 to March 31, 2023, 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)* (2017 TSC).

Siemens uses a subservice organization to provide data center colocation 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 organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in attachment C, "Other Information Provided by Siemens Industry Software, Inc. That Is Not Covered by the Service Auditor's Report," is presented by Siemens' management to provide additional information and is not a part of Siemens' description of the boundaries of XaaS Enterprise Core made available to user entities during the period October 1, 2022 to March 31, 2023. Information included regarding ISO 27001, ISO 27017 and ISO 27018 has not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it.

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 service 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' XaaS Enterprise Core were effective throughout the period October 1, 2022 to March 31, 2023, 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 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
August 15, 2023

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’ Xcelerator as a Service (XaaS) Enterprise Core (system) throughout the period October 1, 2022 to March 31, 2023, 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)* (2017 TSC). Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

Siemens uses a subservice organization for data center colocation 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 organization.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2022 to March 31, 2023, 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 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 October 1, 2022 to March 31, 2023, 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 Xcelerator as a Service (XaaS) Enterprise Core

Type of Services Provided

Siemens Industry Software, Inc. (“SISW”, “the Company”) is a global company focusing on digitalization. Headquartered in Plano, Texas, SISW’s Siemens Xcelerator as a Service (XaaS) is a comprehensive and integrated portfolio of engineering software and services, as well as an application development platform and how it enhances electronic and mechanical design, system simulation, manufacturing, operations, and life cycle analytics. The XaaS suite includes the XaaS Enterprise Core that offers individuals the ability to securely collaborate, store, share, and modify files in the cloud.

The boundaries of the system in this section details the XaaS Enterprise Core. No other Company services are within the scope of this report.

The Boundaries of the System Used to Provide the Services

The boundaries of XaaS Enterprise Core 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 XaaS Enterprise Core.

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

Infrastructure

The Company utilizes Amazon Web Services (AWS) to provide the resources to host XaaS Enterprise Core. The Company leverages the experience and resources of AWS to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the XaaS Enterprise Core architecture within AWS 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, with a fully dedicated internal team responsible for implementing configurations that use Auth0’s global footprint to provide the required scalability and resiliency for global customers.

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

Infrastructure	
Production Tool	**Business Function**
Identity and access management (IAM)	IAM
Auth0	IAM
Amazon Elastic Kubernetes Service (Amazon EKS)	Container hosting environment
Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), Amazon DocumentDB	Database, data storage services
Cloud Custodian	Policy management
Amazon CloudFront	Content distribution network

Infrastructure	
Production Tool	**Business Function**
Siemens Corporate public key infrastructure (PKI) services	Identification and authentication services

Software

Software consists of the programs and software that support XaaS Enterprise Core (operating systems [OSs], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor XaaS Enterprise Core include the following applications, as shown in the table below:

Software	
Production Application	**Business Function**
GitHub, Bitbucket	Code repositories
Amazon CloudWatch, AWS CloudTrail, Amazon GuardDuty, Datadog, Splunk, PagerDuty, Grafana	Logging and monitoring software, tools, utilities
Polarion, Jira, Jenkins, Gitlab runners, Argo CD	Continuous integration/continuous delivery (CI/CD) core tools
SonarQube, Aqua, Amazon Inspector, Tanium	Software testing and component vulnerability scanning tools
Harbor, Artifactory	Software repositories
Rancher, Ansible, Cloud formation	Infrastructure orchestration and automation
TrendMicro, Malware Bytes, Microsoft Defender	Antivirus/Anti-malware tools
Pulse Secure	Corporate virtual private network (VPN)
Microsoft Office 365 software and affiliated services	Productivity tools
Confluence, Wiki, WalkMe	Document storage and productivity
Cloudability	Cost control, capacity management

People

The Company develops, manages, and secures XaaS Enterprise Core 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.

People	
Group/Role Name	**Function**
Cloud Security Operations (CSO)	Responsible for managing operations and the security of the production cloud environments.
XCICD	Responsible for the development environment for XaaS Enterprise Core.
Webkey	Responsible for managing authentication of users.
Lifecycle Services (LCS)	Responsible for providing a secure platform for data storage and exchange of information.
Mainstream/Zel-X	Responsible for developing the front-end interface of XaaS Enterprise Core.
Entitlement	Responsible for providing and managing entitlements to users of XaaS Enterprise Core.
SaaS Experience	Responsible for providing a unified access portal and usage information for XaaS Enterprise Core.
XCR KaaS	Responsible for providing secure maintenance of Kubernetes clusters on AWS.
WalkMe	Responsible for maintaining product help pages.
RunOps	Responsible for Tier 1 support services.
Siemens Corporate IT	Responsible for corporate IAM services, workstations, and corporate VPN services.

The following organization chart reflects the Company’s internal structure related to the groups discussed above:

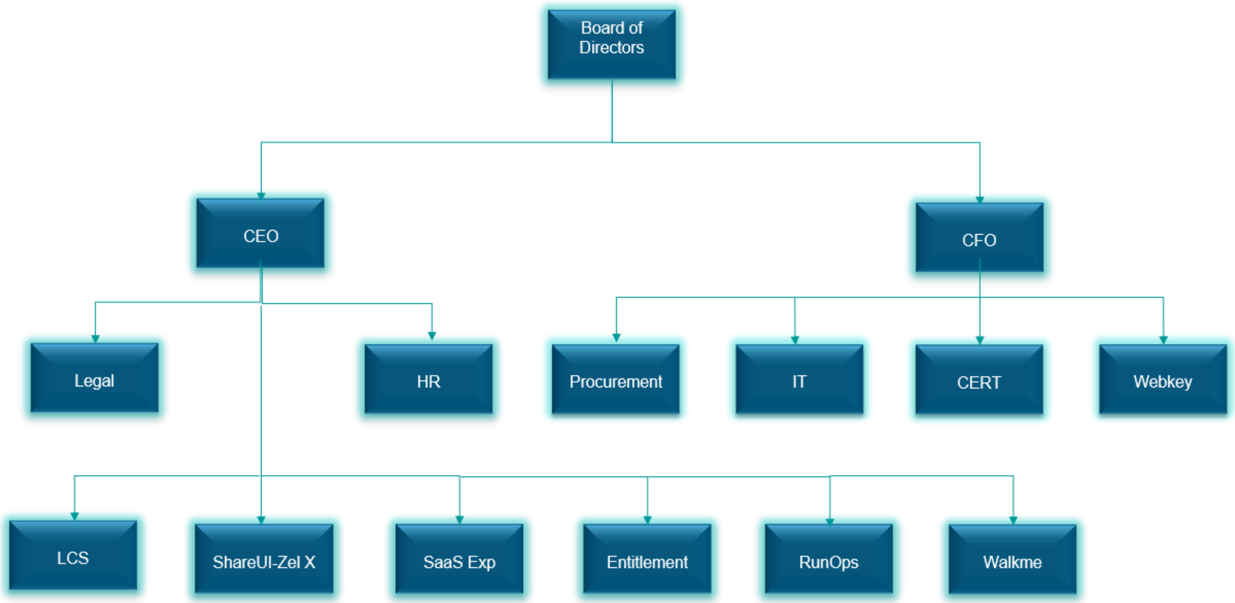

Figure 1: SISW Organization Chart

Procedures

Procedures include the automated and manual procedures involved in the operation of XaaS Enterprise Core. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (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 XaaS Enterprise Core:

Procedures	
Procedure	**Description**
Logical and Physical Access	How the Company restricts logical and physical 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 and physical 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 Management	How the Company 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.
Personnel Management	How the Company recruits, develops, and promotes skilled personnel.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the user interface (UI) and application programming interfaces (APIs), the customer or end-user defines and controls the data they load into and store in the XaaS Enterprise Core production network. 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 databases and datastores housing sensitive customer data.

The following table details the types of data contained in the production application for XaaS Enterprise Core:

Data		
Production Application	**Description**	**Data Store**
XaaS Enterprise Core application	The Company stores user-provided files within its datastores, as part of its core 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.	Amazon S3 storage services
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.	Amazon GuardDuty, Amazon CloudWatch, AWS CloudTrail, Datadog, Splunk

Subservice Organization and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS as a subservice organization for data center colocation services. The Company's controls related to XaaS Enterprise Core cover only a portion of the overall internal control for each user entity of XaaS Enterprise Core.

Although the subservice organization has 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 organization. CSOCs are expected to be in place at the organization identified, 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
- Security controls to provide the required information security assurances to the Company
- Compliance or governance controls to enforce the requisite security policies and procedures

The Company management receives and reviews the ISO/IEC 27001:2013 certification and SOC 2 report(s) annually where feasible. In addition, through its operational activities, Company management monitors the services performed by the subservice entity to determine whether operations and controls expected to be implemented are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned to services, and relay any issues or concerns to the respective management of each subservice organization.

It is not feasible for the service commitments, system requirements, and applicable criteria related to XaaS Enterprise Core to be achieved solely by the Company. The CSOCs that are expected to be implemented at AWS are described below.

Criteria	Complementary Subservice Organization Controls
CC6.1	• AWS is responsible for encrypting databases in its control.
CC6.4	• AWS is responsible for restricting data center access to authorized personnel. • AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.6 CC6.8	• AWS is responsible for deploying up-to-date security patches for the SaaS Experience infrastructure.
CC6.5 CC6.7	• AWS is responsible for securely decommissioning and physically destroying production assets in its control.
CC7.2 A1.2	• AWS is responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers. • AWS is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

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 XaaS Enterprise Core. Commitments are communicated through the Universal Cloud Agreement (UCA), Data Processing Terms (DPT), and the Privacy Notice.

System requirements are specifications regarding how XaaS Enterprise Core 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 XaaS Enterprise Core include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• The Company will implement appropriate technical safeguards to protect client data, conforming to an 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 de-provisioning of employee access • The Company will log and monitor all access and administrative activities within the system • The Company will implement anti-malware and vulnerability scanning on IT systems • The Company will logically segregate production and non-production environments • The Company will use 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

Trust Services Category	Service Commitments	System Requirements
Availability	• The Company will use commercially reasonable efforts to maintain a functional state 24 hours per day, 7 days per week, except for planned downtime (weekly 11:59pm EST Saturday – 11:59am EST Sunday) and any unavailability caused by circumstances beyond the Company's reasonable control • The Company will ensure the system is available for use 95% 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 a scheduled downtime for the system • In the event of a continuity event, the Company shall recover services within 24 hours (recovery time objective [RTO] of less than 24 hours) and ensure data restoration to be at a point within 24 hours (recovery point objective [RPO] of less than 24 hours)	• System logging and monitoring • Backup and recovery standards • Incident handling and response standards • Business continuity standards
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 transmitted over public networks • The Company will irretrievably erase data or destroy storage media before disposing or reusing IT systems	• Data Classification and handling standards • Encryption standards • Information sharing standards

Attachment C

Other Information Provided by Siemens Industry Software, Inc. That Is Not Covered by the Service Auditor's Report

Other Information Regarding ISO 27001, ISO 27017, ISO 27018

Siemens Industry Software, Inc. meets the requirements of ISO 27001, ISO 27017 and ISO 27018 over the following Scope: The Information Security Management Systems (ISMS) at SISW applies to the preservation of the confidentiality, integrity and availability (CIA) of SISW information assets that enable the management of SISW cloud environments and product offerings, registration No: 31602867 as of 2021-09-30 and valid until 2024-09-08. The scope of the ISO 27001, ISO 27017 and ISO 27018 audit includes Siemens' Xcelerator as a Service (XaaS) Enterprise Core. As a result of the ISO 27001, ISO 27017 and ISO 27018 surveillance audit January 2023, no major nor minor nonconformities were found; for the implemented supplier review process 2 opportunities for improvement were found. The Management has taken actions to improve the supplier review process, which will be implemented by November 2023.