A-LIGN

Synopsys, Inc.
Type 2 SOC 3
2022

SYNOPSYS®

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

February 1, 2021 to January 31, 2022

Table of Contents

SECTION 1

ASSERTION OF SYNOPSYS, INC. MANAGEMENT

ASSERTION OF SYNOPSYS, INC. MANAGEMENT

March 3, 2022

We are responsible for designing, implementing, operating, and maintaining effective controls within Synopsys, Inc.'s ('Synopsys' or 'the Company') Software Integrity Group Services System throughout the period February 1, 2021 to January 31, 2022, to provide reasonable assurance that Synopsys' service commitments and system requirements relevant to Security, Availability, and Confidentiality (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "Synopsys, Inc.'s Description of Its Software Integrity Group Services System throughout the period February 1, 2021 to January 31, 2022" 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 February 1, 2021 to January 31, 2022, to provide reasonable assurance that Synopsys' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy* (AICPA, *Trust Services Criteria*). Synopsys' objectives for the system in applying applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Synopsys, Inc.'s Description of Its Synopsys Software Integrity Group Services System throughout the period February 1, 2021 to January 31, 2022".

Synopsys uses Amazon Web Services ('AWS') and Google Cloud Platform ('GCP') to provide cloud hosting 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 Synopsys, to achieve Synopsys' service commitments and system requirements based on the applicable trust services criteria. The description presents Synopsys' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Synopsys' 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 Synopsys' 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 Synopsys' 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 February 1, 2021 to January 31, 2022 to provide reasonable assurance that Synopsys' service commitments and system requirements were achieved based on the applicable trust services criteria.

BRUCE C JENKINS
Info & Product Security
Synopsys, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Synopsys, Inc.:

Scope

We have examined Synopsys, Inc.'s ('Synopsys' or 'the Company') accompanying description of Synopsys Software Integrity Group Services System titled "Synopsys, Inc.'s Description of Its Synopsys Software Integrity Group Services System throughout the period February 1, 2021 to January 31, 2022" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period February 1, 2021 to January 31, 2022, to provide reasonable assurance that Synopsys' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Synopsys uses AWS and GCP to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Synopsys, to achieve Synopsys' service commitments and system requirements based on the applicable trust services criteria. The description presents Synopsys' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Synopsys' 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 Synopsys, to achieve Synopsys' service commitments and system requirements based on the applicable trust services criteria. The description presents Synopsys' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Synopsys' 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

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria, and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:
- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

Inherent Limitations

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

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Synopsys' Software Integrity Group Services System were suitably designed and operating effectively throughout the period February 1, 2021 to January 31, 2022, to provide reasonable assurance that Synopsys' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on Synopsys' 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 Synopsys, user entities of Synopsys' Software Integrity Group Services during some or all of the period February 1, 2021 to January 31, 2022, business partners of Synopsys subject to risks arising from interactions with the Synopsys Software Integrity Group Services, and those who have sufficient knowledge and understanding of the complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

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

A-lign Assurance
Tampa, Florida
March 3, 2022

SECTION 3

**SYNOPSYS, INC.'S DESCRIPTION OF ITS SYNOPSYS SOFTWARE INTEGRITY
GROUP SERVICES SYSTEM THROUGHOUT THE PERIOD
FEBRUARY 1, 2021 TO JANUARY 31, 2022**

OVERVIEW OF OPERATIONS

Company Background

Synopsys, Inc. ("Synopsys") is headquartered in Mountain View, CA. The Company provides electronic design automation tools and services and has a portfolio of silicon Internet Protocol (IP) solutions covering interface, analog, embedded memory, and physical IP.

Description of Services Provided

The Software Integrity Group (SIG) is a Synopsys business unit that provides software tools and services to improve the security and quality of its customers' software applications. SIG provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to find and fix vulnerabilities and defects in proprietary code, open-source components, and application behavior. With a combination of tools, services, and expertise, SIG helps organizations optimize security and quality in development, security, and operations and throughout the software development life cycle.

The SIG Software as a Service (SaaS) offerings include Black Duck, Polaris, and the Managed Services Portal. Black Duck is a software composition analysis tool that assesses an application's open-source constituents and analyzes them for security defects and license compliance. Polaris is a cloud platform designed to integrate a broad variety of application security tools and provide a single "pane of glass" across a variety of application-testing technologies. Static analysis is provided through Coverity. Software composition analysis is provided through Open-Source Security Tools and Risk Analysis (OSRA). The Managed Services Portal allows customers to schedule security assessments and retrieve the results of those assessments.

The system description in this section of the report details the SIG SaaS offerings. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organizations).

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the SIG SaaS offerings. Commitments are communicated in end-user license agreements, security commitments, data privacy and protection statement, and master service agreements, which can be found on the Company's security web page.

System requirements are specifications regarding how the SIG SaaS 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 the SIG SaaS offerings include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• The Company will maintain best-practice technical and organizational security measures to protect against such risks as accidental or unlawful destruction, loss, or alteration of data and unauthorized disclosure or access	• Change Management • Incident Management • Risk Management • Configuration Management • Log Management • Vendor Management • Annual Security Assessment • Vulnerability Management • Access Management
Availability	• The Company will back up customer data daily with a 7-day retention policy • The Company will maintain a recovery time objective (RTO) of one (1) business day and a recovery point objective (RPO) of 24 hours	• Daily Backup and Restore Procedures • Business Continuity and Disaster Recovery Plans
Confidentiality	• The Company will disclose confidential information only to those who need to know in order to provide the services • Upon termination, the Company will return or destroy customer's confidential information • The Company will keep customer data encrypted in transit and at rest	• Data Classification • Retention and Destruction Standards • Data Handling Standards • Data Encryption in Transit and at Rest

Components of the System

The boundaries of the SIG SaaS 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 the SIG SaaS offerings.

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

Infrastructure

The Company utilizes Amazon Web Services (AWS) and Google Cloud Platform (GCP) to provide the resources to host the SIG SaaS offerings. The Company leverages the experience and resources of AWS and GCP to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the SIG SaaS offerings' architecture within AWS and GCP to ensure some of the availability, security, and resiliency requirements are met.

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

Infrastructure			
Production Tool	**Business Function**	**Operating System**	**Hosted Location**
MySQL, PostgreSQL, MongoDB, Eventstore, Kafka, Hadoop	Databases	CentOS Linux, Debian Linux, Alpine Linux, Ubuntu Linux	AWS and GCP
Google Transmission Control Protocol (TCP) Load Balancing (LB), Google L7 LB, Elastic LB, Nginx	Load Balancer	Solutions specific	AWS and GCP

Software

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

Software	
Production Application	**Business Function**
Datadog	Application monitoring, infrastructure monitoring
Velero	Backup and replication
Logz.io, Stackdriver	Logging system
Okta	Single sign-on
CloudHealth	Information technology (IT) asset management
Prometheus, Zabbix	Infrastructure monitoring
Coverity	Static Analysis
Prisma Cloud Compute (Twistlock)	File integrity monitoring, anti-malware, intrusion detection
Jira, BMC Remedyforce	Help desk, ticketing system

People

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

People	
Group/Role Name	**Function**
Information Security Management System (ISMS) Management Committee Body	• Provides the ISMS Program with operational and tactical direction, strategic alignment, and guidance as the Company encounters both successes and issues
VP Strategy and Operations	• Drives strategic initiatives and operations across SIG go-to-market and business unit strategy • Participates in the ISMS Management Committee as a member
VP of Engineering	• SIG Cloud Operations reports to VP of Engineering
VP of Finance	• SIG IT reports to VP of Finance
SIG Business Operations	• Oversees Company business operations and legal or regulatory compliance abidance • Business Operations Director participates in the ISMS Management Committee as a member
SIG Cloud Operations	• Oversees and manages Company application programming interfaces (APIs), SaaS services, database storage, OSs and Virtual Machines (VMs), and internal and external firewalls protecting production systems and services • Coordinates with Company IT to manage vulnerabilities and conduct operational change management • Cloud Operations Manager participates in the ISMS Management Committee as a member
SIG IT	• Oversees and manages user access management, network services, and projects and provides core IT services to internal customers • Coordinates with Cloud Operations to manage vulnerabilities and conduct operational change management • IT Director participates in the ISMS Management Committee as a member
SIG Info & Product Security Group	• Secures the Company's software products and professional service offerings • Info & Product Security Leader participates in the ISMS Management Committee as a chair

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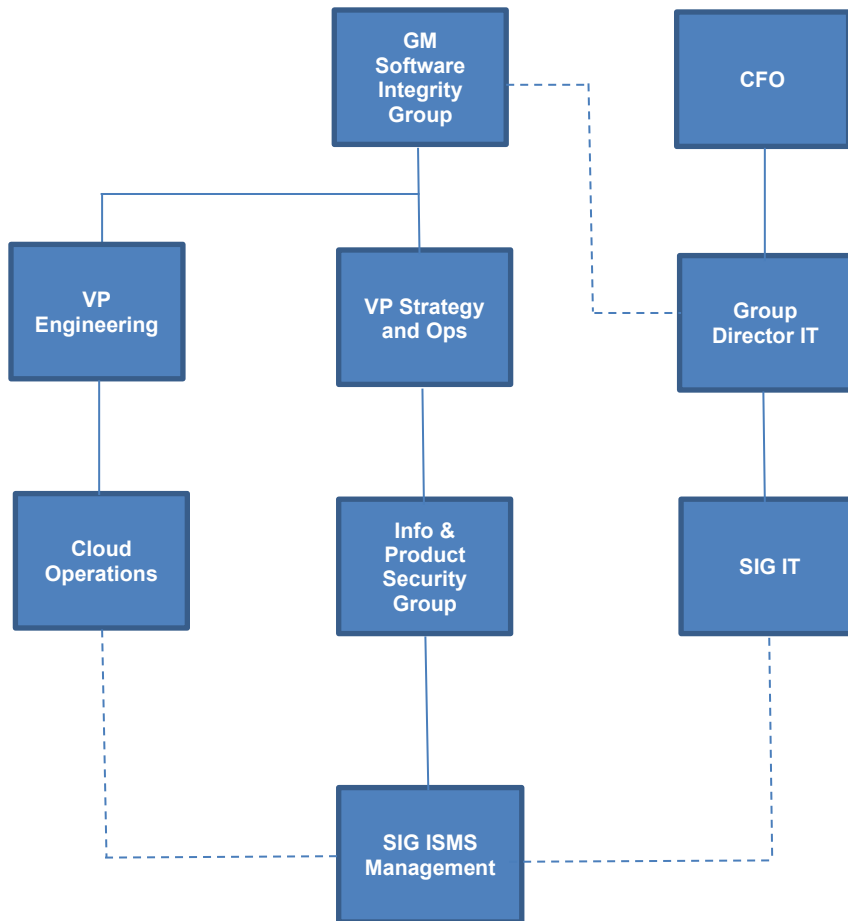

Figure 1: Synopsys Organization Chart

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the API, the customer or end user defines and controls the data they load into and store in the SIG SaaS offerings' 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 the transmission of confidential or sensitive information over public networks. Encryption is enabled for databases housing sensitive customer data.

The following table details the types of data contained in the production application for the SIG SaaS offerings:

Data		
Production Application	**Description**	**Data Store**
Polaris	- User credentials - Source code - Static analysis security assessment results	GCP, PostgreSQL, Eventstore
Black Duck	- User credentials - Source code snippets - Software composition security assessment results - Software license compliance results	GCP, PostgreSQL
Managed Services Portal	- User credentials - Source code, binary files, and documentation - Security assessment results	AWS, MongoDB, MySQL
Knowledge Base (KB)	Open-source software licensing and security defects	GCP, PostgreSQL, Hadoop

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

Physical Security

Wholly occupied company facilities are protected by walls and fencing around the entire perimeter. Each facility has a designated reception area which is attended by either a receptionist or a security guard 24 hours per day. Access to the reception area is unlocked from 8am to 5pm on business days and is locked at all other times. When locked, a visitor presses a buzzer to attract the attention of the guard at the visitor desk who can release the lock. The door may also be unlocked through the use of an access card/ID that has been assigned general access to the facility. Access beyond the reception area is controlled through the access card system.

Remaining exterior ingress doors are restricted to users possessing an access card/ID that has been assigned access to use the door. The access card/ID system uses zones to control access. Each exterior door and doors to restricted areas within the facilities are assigned to door zones. Access to zones is restricted through the use of access control lists. Employees and vendors granted access cards are assigned to roles based on their job responsibilities.

Visitors check in with the receptionist or security guard stationed in the reception area. Visitors must present a valid, government-issued photo ID. The visitor's name, employer, and purpose for visit are recorded in a visitor log and his or her visit must be approved by a Synopsys employee who is authorized to sign non-employees into the facility. The visitor is issued a temporary ID badge to be worn throughout his or her visit. This temporary badge does not permit users access through any secured doors within the facility.

Entrances to data centers are restricted by two doors; access through the first door is gained by using a key card to deactivate the locking mechanism, and access through the second door is granted by using a biometric hand reader and personal identification number (PIN).

Upon an employee's termination of employment, the HR system automatically generates an access deletion record in the event management system on the last day of employment. This record is routed to the access administrators for deletion. In addition, terminated employees turn over their access cards/IDs during their exit interview. These cards are then sent via interoffice mail to physical security for recording and destruction. On a monthly basis, the director of physical security runs a report detailing access cards with deleted access that have not been recorded as returned. The director investigates missing cards and documents the resolution in the event management system.

On a quarterly basis, zone owners review access to their zones. Access listings are generated by security and distributed to the zone owners via the event management system. Zone owners review the listings and indicate the required changes in the event management record. The record is routed back to the access administrators for processing. The director of physical security identifies any records not returned within two weeks and follows up with the zone owner.

On a semi-annual basis, the director of physical security sends a list of each vendor's employees who have been granted access to the vendor contact to review appropriateness of employee access. Vendors are required to return the confirmation of access within two weeks. The director follows up on any access lists not returned.

Logical Access

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

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

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

Employees accessing the system from outside the Synopsys network are required to use a token-based two-factor authentication system. Employees are issued tokens upon employment and must return the token during their exit interview. Vendor personnel are not permitted to access the system from outside the Synopsys network.

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

Customer employees may sign on to their systems using virtual server administration accounts. These administration accounts use a two-factor digital certificate-based authentication system.

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

On an annual basis, access rules for each role are reviewed by a working group composed of security help desk, data center, customer service, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the CISO. As part of this process, the CISO reviews access by privileged roles and requests modifications based on this review.

The HR system generates a list of terminated employees on a daily basis. This daily report is used by the security help desk to delete employee access. On an annual basis, HR runs a list of active employees. The security help desk uses this list to suspend user IDs and delete access roles from IDs belonging to terminated employees.

On a quarterly basis, managers review roles assigned to their direct reports. Role lists are generated by security and distributed to the managers via the event management system. Managers review the lists and indicate the required changes in the event management record. The record is routed back to the security help desk for processing. The security help desk manager identifies any records not returned within two weeks and follows up with the manager. As part of this process, the CISO reviews employees with access to privileged roles and requests modifications through the event management system.

Computer Operations - Backups

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

Backup infrastructure and on-site backup tape media are physically secured in locked cabinets and/or caged environments within the third-party data centers. The backup infrastructure resides on private networks logically secured from other networks.

Contracted customer off-site tape rotations are logged and maintained within an enterprise ticket management system. A third-party provider that specializes in off-site tape rotation has been contracted to perform off-site tape rotation services for clients that select this as part of the backup service. The ability to recall backup media from the third-party off-site storage facility is restricted to authorized operations personnel.

Computer Operations - Availability

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

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

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

Change Control

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

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

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

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

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.

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

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

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

Boundaries of the System

The scope of this report includes the Synopsys Software Integrity Group Services System performed in the Burlington, Massachusetts facility.

This report does not include the cloud hosting services provided by AWS and GCP at multiple facilities.

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 Synopsys' control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Synopsys' 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

Synopsys' 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 particular 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
- Training is provided to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style

Synopsys' 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 periodically briefed on regulatory and industry changes affecting the services provided
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole

Organizational Structure and Assignment of Authority and Responsibility

Synopsys' 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.

Synopsys' assignment of authority and responsibility activities include 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 Resources Policies and Practices

Synopsys' 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 ensures the service organization is operating at maximum efficiency. Synopsys' human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, 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
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

Risk Assessment Process

Synopsys' risk assessment process identifies and manages risks that could potentially affect Synopsys' 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. Synopsys identifies the underlying sources of risk, measures the impact to 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 Synopsys, 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

Synopsys has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Synopsys attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Synopsys' Software Integrity Group Services system; as well as the nature of the components of the system result in risks that the criteria will not be met. Synopsys 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 meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Synopsys' 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 Synopsys' 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, information technology. At Synopsys, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly 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, town hall meetings are held bi-annually in each geographic location to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the town hall meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Synopsys personnel via e-mail messages.

Specific information systems used to support Synopsys' Software Integrity Group Services System is 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. Synopsys' 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 is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Synopsys' management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Synopsys' 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 Synopsys' personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going 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 in the 12 months preceding the end of the review period.

Incidents Since the Last Review

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

Criteria Not Applicable to the System

All Common, Availability, and Confidentiality criterion were applicable to the Synopsys Software Integrity Group Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS and GCP at multiple facilities.

Subservice Description of Services

Synopsys uses AWS and GCP as subservice organizations for cloud hosting services. Synopsys' controls related to the SIG SaaS offerings cover only a portion of the overall internal control for each user entity of the SIG SaaS offerings. The description does not extend to the cloud hosting services provided by the subservice organizations.

AWS and GCP are responsible for physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS and GCP's physical security controls mitigate the risk of unauthorized access to the hosting facilities. AWS and GCP's environmental protection controls mitigate the risk of fires, power loss, climate, and temperature variabilities. GCP also provides security monitoring services as part of its Platform-as-a-Service offering. GCP security monitoring services mitigate the risk of unauthorized logical access.

Synopsys management receive and review the AWS and GCP SOC 2 reports annually. In addition, through its operational activities, Synopsys management monitor the services performed by AWS and GCP to determine whether operations and controls expected to be implemented are functioning effectively. Management also has communication with the subservice organizations to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS and GCP management.

Complementary Subservice Organization Controls

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

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

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.

Subservice Organization - AWS		
Category	Criteria	Control
		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.
		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.

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

Subservice Organization - GCP		
Category	Criteria	Control
Common Criteria / Security, Availability	CC6.4,	User access lists to data center server areas are reviewed on a quarterly basis and inappropriate access is removed in a timely manner.
		All visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components are maintained and operated.
		Visitors must be signed in by an employee before a single-day paper visitor badge that authorizes them can be issued.
		Annual data center security reviews are performed, and results are reviewed by executive management.

Subservice Organization - GCP		
Category	**Criteria**	**Control**
		Physical security measures in place include: - Existence of security guards, access badges, and video cameras to secure the data centers is reviewed during the annual data center security reviews - Data center entrances have a perimeter security system consisting of badge readers or biometric access system - Data centers utilize a badge reader or biometric access controls to restrict access to raised floor spaces and lock/keys to restrict access to facilities rooms within the building - All emergency exit points from the raised floor are alarmed - Badge reader and biometric access control systems are secured in a restricted space and no physical access to them from public spaces exists - Visitors to the datacenter facilities must gain appropriate approval, sign in at the front, and remain with an escort during the duration of their visit - Video cameras exist to monitor building entrances, exits, and the areas immediately surrounding the building - At least one security guard is on-site 24x7 - All staff members are required to either sign in or badge in to gain access to the facility and a no tailgating policy is in place - All Google cages, suites, and private rooms are secured using either lock/key, badge access control, or biometric access controls - A key sign out sheet and/or log of badge reader activity exists and covers access to Google spaces
	A1.2	Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).
		All data centers are equipped with fire detection alarms and protection equipment. Data center server floors and network rooms are connected to an UPS system and emergency generator power is available in the event of a loss of power. Google protects the information system from damage resulting from water leakage by providing shutoff valves that are accessible, working properly and known to key personnel.

Synopsys management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Synopsys performs monitoring of the subservice organization controls, including the following procedures:
- Reviewing attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

Synopsys' 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 Synopsys' services to be solely achieved by Synopsys control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Synopsys'.

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.

Criteria	Complementary User Entity Controls (CUECs)
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
CC6.4 CC6.5 CC7.2 A1.2	• 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
CC6.6	• Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company