A-LIGN

A-LIGN.com

# Type 2 SOC 3

Prepared for:
HCLSoftware

Year:
2025

HCLSoftware

# SOC 3 FOR SERVICE ORGANIZATIONS REPORT

## April 1, 2024 to March 31, 2025

# Table of Contents

## SECTION 1

## ASSERTION OF HCLSOFTWARE MANAGEMENT

## ASSERTION OF HCLSOFTWARE MANAGEMENT

January 5, 2026

We are responsible for designing, implementing, operating, and maintaining effective controls within HCLSoftware's ('the Company') HCL AppScan on Cloud (ASoC) System throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that HCLSoftware's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "HCLSoftware's Description of Its HCL AppScan on Cloud (ASoC) System throughout the period April 1, 2024 to March 31, 2025" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that HCLSoftware's service commitments and system requirements were achieved based on the trust services criteria. HCLSoftware's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "HCLSoftware's Description of Its HCL AppScan on Cloud (ASoC) System throughout the period April 1, 2024 to March 31, 2025".

HCLSoftware uses Microsoft Azure ('Azure' or 'subservice organization') 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 HCLSoftware, to achieve HCLSoftware's service commitments and system requirements based on the applicable trust services criteria. The description presents HCLSoftware's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of HCLSoftware's controls. The description does not disclose the actual controls at the subservice organization.

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

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2024 to March 31, 2025 to provide reasonable assurance that HCLSoftware's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of HCLSoftware's controls operated effectively throughout that period.

Stephen Padgett

Stephen Padgett, CIO
Authorized Signatory
HCLSoftware

## SECTION 2

## INDEPENDENT SERVICE AUDITOR'S REPORT

## INDEPENDENT SERVICE AUDITOR'S REPORT

To HCLSoftware:

*Scope*

We have examined HCLSoftware's (or 'the Company') accompanying assertion titled "Assertion of HCLSoftware Management" (assertion) that the controls within HCLSoftware's HCL AppScan on Cloud (ASoC) System were effective throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that HCLSoftware's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

HCLSoftware uses Azure 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 HCLSoftware, to achieve HCLSoftware's service commitments and system requirements based on the applicable trust services criteria. The description presents HCLSoftware's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of HCLSoftware's controls. The description does not disclose the actual controls at the subservice organization. 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 description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at HCLSoftware, to achieve HCLSoftware's service commitments and system requirements based on the applicable trust services criteria. The description presents HCLSoftware's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of HCLSoftware's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

*Service Organization's Responsibilities*

HCLSoftware 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 HCLSoftware's service commitments and system requirements were achieved. HCLSoftware was also provided the accompanying assertion (HCLSoftware assertion) about the effectiveness of controls within the system. When preparing its assertion, HCLSoftware is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

*Service Auditor's Responsibilities*

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

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

*Independence and Ethical Responsibilities*

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

*Inherent Limitations*

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

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

*Opinion*

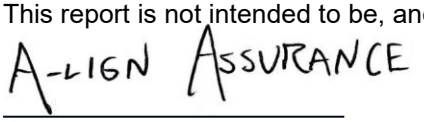
In our opinion, management's assertion that the controls within HCLSoftware's HCL AppScan on Cloud (ASoC) System were suitably designed and operating effectively throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that HCLSoftware's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of HCLSoftware's controls operated effectively throughout that period.

The SOC logo for Service Organizations on HCLSoftware's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

*Restricted Use*

This report, is intended solely for the information and use of HCLSoftware, user entities of HCLSoftware's HCL AppScan on Cloud (ASoC) during some or all of the period April 1, 2024 to March 31, 2025, business partners of HCLSoftware subject to risks arising from interactions with the HCL AppScan on Cloud (ASoC), and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

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




Tampa, Florida
January 5, 2026

## SECTION 3

## HCLSOFTWARE'S DESCRIPTION OF ITS HCL APPSCAN ON CLOUD (ASOC) SYSTEM THROUGHOUT THE PERIOD APRIL 1, 2024 TO MARCH 31, 2025

## OVERVIEW OF OPERATIONS

### Company Background

HCLSoftware is a subsidiary of HCL Technologies Limited that operates its primary software business. HCL develops, markets, sells, and supports over 20 product families in the areas of Customer Experience, Digital Solutions, Secure DevOps, and Security and Automation.

### Description of Services Provided

HCLSoftware provides customers with a number of software solutions for various uses. This report includes the HCL AppScan on Cloud (ASoC) which will be called in short hereafter ASoC. The HCL ASoC product is a comprehensive, cloud-based application security solution that delivers a suite of security testing tools to perform static (SAST), dynamic (DAST), interactive (IAST), and software composition analysis (SCA) testing on web, mobile, and open-source software:

- Leveraging Azure cloud provider for the infrastructure and container services needed to host the platform.
- Highly available, mission critical support. HCLSoftware offers an availability Service Level Agreements (SLAs) of 99.9% to customers, including Disaster Recovery capabilities to protect the service.
- Highly secure, with updated modern security toolsets designed to detect abnormal behavior, protect inbound traffic from malicious users, and scan both internally and externally to ensure no potential vulnerabilities exist. Traffic flows are secured with encryption, and data is encrypted as well either at the database or storage level to protect the confidentiality and integrity of the data.
- Rapid updates. The products leverage Kubernetes and other technologies that ensure that updates with new capabilities and patches can be deployed as quickly as possible.
- Robust set of scalability, monitoring, logging, and alerting capabilities designed to ensure the overall availability of the system.

HCLSoftware employs approximately 120 people that support HCL ASoC's customers that reside on the HCL ASoC. Application management services are provided under contractual arrangements incorporating a number of factors including the type of applications being licensed, the number of users covered and the frequency of access to the application.

### Principal Service Commitments and System Requirements

The standard Contract Agreement acts as the formal contract for users of the HCL ASoC. The Contract Agreement documents the contractual obligations of HCLSoftware and the terms of use for customers using the HCL ASoC. Contractual obligations include HCL ASoC's service commitments and system requirements as they relate to security, availability, and confidentiality. Additionally, the Contract Agreement serves to define and communicate the design and operation of the system and its boundaries. HCLSoftware representatives and its customers authorize the Contracts with formally documented signatures prior to provisioning of services.

Principal service commitments and relevant system requirements within the boundaries of the system are outlined further in the sections below.

HCLSoftware designs its processes and procedures related to the HCLSoftware cloud, data centers, and infrastructure services to meet its objectives. Those objectives are based on the service commitments that HCLSoftware makes to user entities and the financial, operational, and compliance requirements that HCLSoftware has established for the HCL ASoC.

Commitments to user entities are documented and communicated in SLAs and other agreements, as well as in the description of the services provided online. Commitments are standardized and include, but are not limited to, the following:

- Cloud Service availability is 24/7, subject to maintenance. The customer will be notified of scheduled maintenance and technical support
- Security principles within the fundamental designs of the HCLSoftware cloud, data centers, and infrastructure that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Facilities, personnel, equipment, software, and other resources necessary to provide the Cloud Services and available user guides and documentation to support the Customer's use of the Cloud Services
- Information and materials provided by HCLSoftware to the customer shall be kept confidential
- Use of encryption technologies to protect data both at rest and in transit
- Customer data retention as governed by the HCLSoftware backup retention policies
- HCLSoftware maintains a set of business conduct and related guidelines covering conflicts of interest, market abuse, anti-bribery and corruption, and fraud. HCLSoftware and its personnel comply with such policies and require contractors to have similar policies
- Formal SLAs to help ensure a timely response to security incidents based on defined priority levels

HCLSoftware establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in HCLSoftware system policies and procedures, system design documentation, and contracts.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented related to how specific manual and automated processes are executed to deliver the cloud, data centers and infrastructure.

**Components of the System**

*Infrastructure*

Primary infrastructure used to provide HCLSoftware's HCL ASoC System includes the following:

| **Primary Infrastructure** | | |
|---|---|---|
| **Hardware** | **Type** | **Purpose** |
| Azure | Databases, storage, virtual machines (VMs) containers infra, network, security services | Infrastructure computing resources and services |
| Elastic Cloud | Cloud service | Log monitoring |

*Software*

Primary software used to provide HCLSoftware's HCL ASoC System includes the following:

| **Primary Software** | | |
|---|---|---|
| **Software** | **Operating System** | **Purpose** |
| HCL ASoC services developed by HCLSoftware | Linux Ubuntu<br>Windows | Functionality of HCL ASoC services |

*People*

Organization and Reporting

Within the organization, key security roles and responsibilities are defined and communicated. Key security positions are documented in a formal organizational chart, which evidences key organizational structures and reporting lines. The organizational chart is reviewed and updated annually for accuracy.

Guidelines have been set for the use of third-party vendors, requiring that contractors be certified through the procurement portal and tracked. Third-party service providers are properly identified and procedures exist for controlling the activities of contract personnel to protect the organization's information assets.

Recruitment

The process for the recruitment of new employees is defined and documented. New employee requisitions are created based upon business need and approved by management prior to posting. Requisitions are posted to externally facing websites to identify potential candidates. Background checks are performed by a third-party for new HCLSoftware employees. New employees are required to adhere to various checks, such as education and criminal background checks, prior to the defined onboarding date. The checks are subject to local laws and vary in different countries. Each check are passed in order for new employees to be onboarded to HCLSoftware. HCLSoftware will notify recruiters of candidates' background status to proceed with the recruitment process. During onboarding, candidates sign employment contracts including a Non-Disclosure Agreement (NDA) and commitment to company policy.

Once employed, HCLSoftware employees are subject to HCLSoftware's procedures for accessing information technology (IT) assets and sanctions for violating HCLSoftware's information security policy. Each employee is required to complete annual trainings, including Code of Business Conduct and Ethics (COBEC), Data Privacy, Information security, and HCLSoftware's Information Security Management System (ISMS). HCLSoftware has a defined disciplinary policy for handling matters related to violations of Company policies, breach of discipline, and employee misconduct. Concerns regarding the code of conduct can be raised to the ombudsman through the whistleblower channels available within the organization. Employees are instructed to report potential security incidents to the HCLSoftware Help Desk or the Security and Compliance team. HCLSoftware's business associate agreement instructs user entities to notify their respective account representative if they become aware of a security breach.

Employee Performance Evaluation

Annual performance evaluations are performed to establish individual goals that are tied to the organization's objectives and provide timely feedback regarding the employee's progress in achieving those goals. Employees are required to submit a self-assessment evaluating individual fiscal year performance and submit for manager review. The reviewer provides feedback and assigns performance ratings defined by a rating scale. After the reviewer feedback is obtained, a calibration stage including peer level assessment is performed followed by the setting of goals for the next period.

HR Policies

Policies and accompanying standards are developed and maintained by HCL Corporate to help guide the HCLSoftware organization to meet its objectives. HCL Corporate operates a formal Corporate Policies Hub which is built upon the policies listed below and is delivered in a controlled wiki environment for use by HCLSoftware. HCLSoftware staff have access to reference the Corporate Policy hub at any time. The following HCL Corporate policies are classified for internal use and include the following:

- Disciplinary Policy - defined policy for handling matters related to a violation of company policies, breach of discipline, and employee misconduct through appropriate disciplinary action. Any person found guilty of violation of the Company's Code will be subject to disciplinary action up to and including termination of employment or removal from a position associated with the Company.
- Whistleblower Policy - defined policy for handling and reporting whistleblower complaints from employees. The appointed, external ombudsman receives whistleblower complaints through a dedicated e-mail or mail. Complaints can be categorized into two broad categories (complaints against C-suite and complaints against others).
- Human Resource - A policy describing HCLSoftware's approach to human resources (HR). The policy includes controls around culture, required annual trainings (CoC, InfoSec, Cybersecurity), communication, the performance evaluation process, and the termination process. HR also offers a whistleblower forum to employees.

*Data*

Based on the product delivered through the HCL ASoC System, customer data is transferred to the HCL ASoC, including sensitive data such as source code, and information about the customer's users and applications. Customers may scan their environments for vulnerabilities using the HCL ASoC, for their use and this data is secured and controlled via the controls included in this report.

The integrity and conformity with regulatory requirements of data sent to the HCL ASoC are solely the responsibility of HCL ASoC customers and not of HCLSoftware. HCLSoftware is, at no time, fulfilling the responsibilities of the Data Controller. HCLSoftware customers remain the Data Controllers. HCLSoftware's responsibility is limited to the Data Processor (i.e., management of the secure storage and processing of data following the Data Controller's instructions).

The integrity and conformity of regulatory requirements of customer data is not the responsibility of HCLSoftware and is not within the boundaries of this report.

*Processes, Policies and Procedures*

Policies and accompanying standards are developed and maintained by HCLSoftware to help guide the organization to meet its objectives. HCLSoftware operates a formal ISMS, which is built upon the policies listed below and is delivered as a controlled wiki environment within HCLSoftware. HCLSoftware staff have access to reference the ISMS at any time. The ISMS is certified to the ISO 27001 Security standard. The ISMS is structured around the following key policies which are reviewed annually at a minimum. The following HCLSoftware policies are classified as internal use and include the following:

- Information Security Policy - An overall statement of intent with respect to HCLSoftware's commitments to security.
- Risk Management - A policy describing HCLSoftware's approach to risk management. This is built on a Risk Register developed in Jira and a structured lifecycle for risks.
- Asset Management - A policy describing HCLSoftware's approach to asset management. Each asset has a structured set of attributes as its definition. The policy also has commitments to secure disposal of information and physical devices and the use of removable media.
- Access Controls - A policy describing HCLSoftware's approach to user access management and access controls. This includes the definition of user ID's and formal password controls.
- Cryptography - A policy describing HCLSoftware's approach to cryptography/data encryption and the encryption standards applied.

- Information Security Incident Management - A policy describing HCLSoftware's approach to the management of any security incidents. Security incidents are captured in Jira and managed in a structured lifecycle. Incident details can be entered by any HCLSoftware employee via the internal Jira tool. High impacting/severity incidents are escalated to the Director of Security.
- Physical Access Standard - A policy describing the access authorization to the HCLSoftware Data Centers.
- Access Control - A policy describing HCLSoftware's approach to a minimum-security standard for devices when being provisioned to or deprovisioned from the infrastructure.
- Vulnerability Scanning and Penetration Testing - A policy describing HCLSoftware's approach to vulnerability scanning of the infrastructure and penetration testing of products and environments. Penetration testing is conducted at a minimum of once per year.
- Information Handling and Disposal Standard - A policy describing HCLSoftware's approach to the usage and disposal of confidential information.
- Record Retention Standard - A policy describing the defined retention periods for categories of data.

These policies are supported by many Standard Operating Procedures (SOP) which describe how the HCL ASoC Development, IT and Operations teams operate to meet the policies and standards of HCLSoftware. The Standard Operating Procedures (SOP's) include system and service descriptions provided by the HCL ASoC Development and Operation teams. The SOP documents are reviewed and approved at least annually. The system description is communicated to users via the HCL ASoC Development wiki.

Physical Security

The in-scope system and supporting infrastructure is hosted by Azure. The HCL ASoC uses Azure Infrastructure as a Service (IaaS) for computer hosting facilities, including physical security access management and secured space for the physical infrastructure and environmental protection controls. The subservice organization, Azure, is responsible for operating and managing the computer hosting facilities. HCLSoftware management maintains responsibility for operations, support, and maintenance, operating and maintaining system software and services software.

Among other ongoing monitoring activities of the subservice organization, HCLSoftware management obtains and reviews a SOC 2 report from the subservice organization to determine whether controls at the subservice organization are suitably designed and operating effectively during the period.

The following is a description of services provided by the subservice organization relevant to this report:

| Subservice Organization | Locations | Services Provided |
|---|---|---|
| Azure Data Centers | Locations of data centers span multiple continents and are located in:<br>• East US<br>• East US 2<br>• Germany West Central<br>• West Europe | Computer hosting facilities, including:<br>• Physical security user access management<br>• Power supply<br>• Data connectivity<br>• Environmental controls<br>• Secured space |

*Asset and Configuration Management*

HCLSoftware generates a dynamic inventory of information assets, including classification, tags, location, and ownership, for the HCL ASoC. The asset owner and business owner share the responsibility to review the listing as-needed.

For any new information assets added to the environment, the assets are hardened in accordance with the baseline hardening procedures, using the Center for Internet Security (CIS) Azure Foundations Benchmark and going through the relevant quality checks and approval prior to being moved to production.

Assets are identified for disposal in accordance with Azure's policies. HCLSoftware uses Azure for secure disposal of information residing on information assets. Since the HCL ASoC utilizes Azure IaaS as a subservice organization to manage physical devices, it is Azure's responsibility to ensure the secure disposal of information residing on information assets upon notification from HCLSoftware or at the end of a hardware device's useful life. Additionally, Azure retains data disposal and destruction certificates. This process is not included within the scope of this report as Azure is carved-out of the boundaries of this report.

Logical Access

The Information Security Policy defines controls and actions taken by HCLSoftware for appropriate protection of customers' assets and to reduce the risk of intentional or accidental disclosure, modification, destruction, disruption, or misuse of data and information within the HCL ASoC managed by HCLSoftware. The security policy is consistent with contractual agreements between HCLSoftware and its customers.

HCLSoftware has implemented role-based security to limit and control access within its infrastructure. Administrative access to Active Directory (AD) and data center servers and databases is restricted to authorized employees. The ability to create or modify user access accounts and user access privileges is limited to authorized personnel.

*Remote Access*

Remote access to the HCLSoftware network is controlled via an encrypted Virtual Private Network (VPN) utilizing token-based, multifactor authentication (MFA). Users accessing the HCLSoftware network are required to input a username and a software token-based application, MFA combination to authenticate to the network.

*User ID and Password Settings*

Once authenticated to the HCLSoftware network through VPN, a combination of unique username (administered by HCLSoftware) and password is used to validate user identity to access the HCL ASoC application. Password requirements to access HCLSoftware's ASoC application are defined in accordance with the ISMS Password Management Policy. HCLSoftware's ASoC Services System has configured minimum requirements for privileged users including minimum character length, complexity, password history, and password expiration. Upon successfully entering the password and username, a user also input the MFA code sent to the user's registered device (e.g., phone call, text, or e-mail) and is able to connect to the ASoC environment.

*Logical Access Granting Process*

HCLSoftware personnel access the HCL ASoC production environment to investigate issues and provide technical support, via the Operations Console. The Information Security Policy establishes the access control requirements for requesting and provisioning user access for HCLSoftware employees and contractors. The policy requires that access be denied by default, follow the least privilege principle, and be granted only upon business need.

Access to the system is granted by the access provisioning team (Dev Manager, IT Manager and Operations Manager). Requests require justification for business need and documented approval by the appropriate personnel. Access provisioning requests are routed via e-mail to the access provisioning team. Access provisioning requires justification for business need and approval by appropriate personnel.

*Periodic Access Review Process*

User access is reviewed quarterly for system administered IDs to verify whether individuals' access is necessary for their job functions and to identify the existence of inappropriate accounts. The user access for the following is reviewed:

- Azure Virtual Machines of HCL ASoC (Remote Access)
- Azure Portal used to provision and manage HCL ASoC resources, view security recommendations and alerts from Azure
- HCLSoftware Launch and Jenkins used to deploy patches and changes to the production environments
- Operations Console used to access HCL ASoC data, support scans, and control system settings
- GitHub and Jira used for source code management and task management

Each review is documented in the HCL ASoC Operations wiki. Corrective actions identified are tracked to remediation, via e-mail, and changes are reflected within the HCL ASoC application production environments.

*Logical Access Termination Process*

The HR department identifies production user account IDs to be disabled on the day of separation from HCLSoftware. HR provides IT personnel with a daily employee termination report. The Global IT (GIT) team reconciles the termination report with current user access within the AD to determine that access is appropriately removed or disabled. Dormant network accounts are disabled after 90 days of inactivity and dormant accounts are disabled after 45 days of inactivity.

A PowerShell script is configured to identify terminated users by comparing the HCLSoftware AD to the manually maintained list of HCL ASoC users, daily. Upon completion of the run, an automated e-mail is sent to the HCL ASoC IT Manager and the system administrator to manually remove the terminated users' active access within the Operations Console. Additionally, access to the Operations Console is removed by the HCL ASoC Operations and IT team managers. The automated e-mails notifying appropriate personnel of terminated users are documented and maintained by the IT team.

Computer Operations - Backups

Backups are managed by the HCL ASoC DevOps team and are scheduled on a daily-basis. The DevOps team monitors backup processes for failures and resolves them in accordance with the procedures defined to meet the required backup frequency and retention requirements. Production data is encrypted on backup media.

Disaster Recovery and data restoration testing are performed by the DevOps team semi-annually and any findings are tracked to resolution through the ticketing system, Jira.

Computer Operations - Availability

HCLSoftware has established an organization-wide effective reliance methodology to proactively identify and address significant risks and threats or events that may potentially impact its ability to operate, be profitable or affect its reputation and value. Consistent implementation of its resilience methodology across the organization is important for HCLSoftware to achieve its objectives, while ensuring compliance to applicable contractual, legal and regulatory requirements.

HCLSoftware's resilience methodology objectives include:

- Establish frameworks for the development and implementation of appropriate business continuity, disaster recovery and crisis management processes that help the organization to manage, respond and recover from disruptive events, including large scale disruptions lasting for extended periods of time
- Establish a second line of defense to provide 'Advisory' and 'Assurance' to interested parties on building necessary response and resilience capabilities to safeguard mutual business interests
- Establish an appropriate risk management process aimed to mitigate resilience related risks
- Establish a mechanism to enable continuous improvement to enhance overall resilience posture

*System Processing Capacity and Usage Monitoring*

HCLSoftware continually monitors the HCL ASoC and its network processing capacity and usage to ensure availability and address capacity issues in a timely manner. System usage is scaled automatically as load increases and scales down as it decreases without need for manual intervention. The DevOps team configures capacity and usage rules within the Azure Portal and within HCL ASoC application. Incidents, as defined within the rules, are sent via e-mail notification to the DevOps team which performs a review in real time that includes:

- An analysis of the capacity based on various parameters (e.g., processing speed, disk utilization, memory, etc.)
- Corrective actions identified from the review, where IT components have exceeded the defined thresholds and a related incident ticket is assigned for appropriate resolution if required

Additionally, the DevOps team projects future capacity requirements based on internal operational reports, revenue forecasts and inputs from customers and internal component teams.

*Business Continuity Plan, Disaster Recovery Plan, and Backups and Restoration Process*

HCLSoftware's Business Continuity Management system is certified with ISO 22301. The certification covers HCLSoftware products, including HCL ASoC.

A formal, documented business continuity plan exists that includes a Disaster Recovery Plan. The business continuity plan is reviewed annually and changes to the procedures are approved. The business continuity plan includes the identification of the risks, corresponding risk mitigation strategies, and procedures to test the feasibility of the business continuity, disaster recovery, and restoration plans.

The business continuity plan is evaluated annually. Business continuity testing includes a tabletop exercise, and disaster recovery testing includes a simulation test. Modifications resulting from the tests are documented within the test reports.

In addition, processes have been implemented for the backup and recovery of critical components and data. Backups are managed by the DevOps team and scheduled on a daily-basis. The Operations team monitors backup processes for failures and resolves them in accordance with the procedures defined to meet the required backup frequency and retention requirements. Production data is encrypted on backup media.

Disaster Recovery and data restoration testing are performed by the Operations team semi-annually and any findings are tracked to resolution through the ticketing system, Jira.

*Data Redundancy and Replication*

HCLSoftware provides data redundancy to minimize disruptions to the availability of services/data within the system. Data redundancy is achieved through fragmentation of data into extents which are copied onto multiple nodes within different availability zones. This approach minimizes the impact of isolated node/availability zone failures and loss of data. Critical components that support the delivery of customer services are designed to maintain high availability through redundancy to another instance with minimal disruption to customer services. Agents on VM monitor the health of the VM. If the agent fails to respond, the VM is rebooted or the workload is transferred to alternative redundant VMs.

Change Control

HCLSoftware has defined and documented a change management process for the HCL ASoC that includes the IT components within the boundaries of this report.

HCLSoftware's change management process requires:

1. The identification and recording of changes.
2. The assessment of risk and potential effect of such changes.
3. The change requests originate from authorized personnel and the approval of proposed changes.
4. The testing of changes to verify operational functionality.
5. A post implementation review, for emergency changes only.

Proposed changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and user entity notifications, are performed. The relevant stakeholders meet to review the changes and the DevOps team implements the changes to the production environment.

If the need for a change to production is identified by the HCLSoftware teams through daily operations, the incident management process, or other means, the ASoC internal teams initiate a change ticket and ensure each requirement of the change management process is followed and documented.

Change requests can be raised by the ASoC internal teams. The Dev team perform development and user acceptance testing within their own development and pre-production environments. Depending on whether the change is infrastructure or customer related, the relevant stakeholders approve the change prior to the DevOps team's implementation of the change.

Changes to infrastructure and software are developed and tested in a separate development and test environment before implementation. The ability to migrate changes into production environments is restricted to DevOps, ensuring appropriate segregation of duties, through the various deployment tools: Argo CD, HCLSoftware Launch, and DART Jenkins.

The below table describes the various change types used by HCLSoftware management to manage changes to the HCL ASoC. These change types include Planned and Hot Fix Changes and follow the same approval and implementation process:

| Change Type | Description of Change | Relevant approvals required prior to implementation |
|---|---|---|
| Planned Change | A planned change involves changes in infrastructure, processes, and technologies. | Development and testing are performed by the Dev team. Approvals are obtained by the relevant stakeholders. The DevOps team implements the change. |
| Hot Fix (Emergency Change) | A hot fix is an emergency change that are deployed to restore services to normalcy. | |

Data Communications

The Procurement team contracts a third-party vendor to conduct external penetration tests at a minimum of once per year. The vendor produces a report identifying the scope of the environment reviewed, steps taken for penetration test, list of vulnerabilities identified, recommended remediation steps, and action plans. The reports are submitted to the Chief Information Security Officer (CISO) for review and acceptance of the suggested action plans. The Security and Compliance team tracks remediation activity to closure.

HCLSoftware's ASoC Services System is configured for security monitoring using CIS Azure Foundations Benchmark. The monitoring tool, Microsoft Defender for Cloud, detects potential unauthorized activity and security events such as the creation of unauthorized local users, local groups, drivers, and services. Azure resources and services of HCL ASoC, including storage, Structured Query Language (SQL) databases, virtual machines, containers, and network components, are scanned using Microsoft Defender for Cloud, at different intervals and to identify discrepancies in the system against the CIS Azure Foundations Benchmark. Upon Scan completion, an e-mail containing the scan results is sent to the DevOps manager for review. The DevOps manager will utilize a checklist to research the vulnerabilities present in the Microsoft Defender for Cloud dashboard to determine if there are false-positives and will dismiss false-positives within the Microsoft Defender for Cloud dashboard. Critical and high vulnerabilities are monitored to resolution using Jira tickets and resolved in accordance with the Application Vulnerability Management Standard.

**Boundaries of the System**

The scope of this report includes the HCL ASoC System that resides in the data centers of Azure in the US and in Germany.

Development and DevOps activities, including coding, code building, testing and transfer of the built code to Azure data centers are performed in HCLSoftware facilities in Israel, India and the US.

This report does not include the cloud hosting services provided by Azure at the various facilities.

**Changes to the System Since the Last Review**

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

**Incidents Since the Last Review**

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

**Criteria Not Applicable to the System**

All Common Criteria/Security, Availability, and Confidentiality criteria were applicable to the HCLSoftware's HCL ASoC System.

**Subservice Organizations**

This report does not include the cloud hosting services provided by Azure at the various facilities.

*Subservice Description of Services*

Azure provides cloud hosting services which include computer hosting facilities and physical and environmental security management to support the delivery of the HCL ASoC.

*Complementary Subservice Organization Controls*

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

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

| **Subservice Organization - Azure** | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| Common Criteria / Security | CC6.4 | Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors. |
| | | Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors. |
| | | Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team. |
| | | Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals. |
| | | The datacenter facility is monitored 24x7 by security personnel. |
| | CC6.4, CC7.2 | Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. |
| | CC6.7 | Datacenter team controls the delivery and removal of information system components through tickets on the Global Datacenter Operations (GDCO) ticketing system. Deliver and removal of information system components is authorized by system owners. System components/assets are tracked in the GDCO ticketing database. |
| | CC6.7, C1.2 | Guidelines for the disposal of storage media have been established. |
| | C1.2 | Customer data is retained and removed per the defined terms within the Product Terms, when a customer's subscription expires, or is terminated. |
| Availability | A1.2 | Datacenter Management team maintains datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures. |
| | | Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems. |

| Subservice Organization - Azure | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| | | Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses. |
| | | Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities. |
| | | Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services. |
| | | Customer data is automatically replicated within Azure to minimize isolated faults. |
| | | Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately. |
| | | Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities. |
| | | Offsite backups are tracked and managed to maintain accuracy of the inventory information. |
| | | Production data is encrypted on backup media. |
| | | Azure services are configured to automatically restore customer services upon detection of hardware and system failures. |

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

- Holding discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

**COMPLEMENTARY USER ENTITY CONTROLS**

HCLSoftware's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to HCLSoftware's services to be solely achieved by HCLSoftware control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of HCLSoftware's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are the 'data controller' and remain so at all times. HCLSoftware's responsibility is limited to the 'data processor' (processing and securing the data in HCL ASoC Services System).
2. User entities are responsible for the inputs and data that they upload to ASoC.
3. User entities are responsible for the data that they export, download, or retrieve from the ASoC.
4. User entities are responsible for their usage of the data.
5. User entities are responsible for protecting test user credentials of web applications that they scan using ASoC.
6. User entities are responsible for protecting test data in web applications that they scan using ASoC.
7. User entities are responsible for the integrity and conformity of regulatory requirements of their data.
8. User entities are responsible for establishing appropriate controls over the use of ASoC.
9. User entities are responsible for following appropriate security practices over the use of ASoC.
10. User entities are responsible for operating and protecting web applications that they scan using ASoC.
11. User entities are responsible for selection of the access mechanism to ASoC (HCLSoftware ID, Single Sign-On (SSO)).
12. User entities are responsible for adding and removing access to ASoC for their user accounts.
13. User entities are responsible for setting the privileges of their user accounts that have access to ASoC.
14. User entities are responsible for reviewing the privileges of their user accounts, consistent with customer organizational policies.
15. User entities are responsible for reviewing the access activities of their user accounts that have access to ASoC.
16. User entities are responsible for protecting the credentials of their user accounts that have access to ASoC.
17. User entities are responsible for their usage of ASoC, for everything they control in the ASoC portal.
18. User entities are responsible for their automation, for everything they automate using HCL ASoC Application Programming Interface (API).
19. User entities are responsible for understanding and verifying ASoC scan results and any other outcome of their usage of ASoC.
20. User entities are responsible for what they do with ASoC scan results and any other outcome of their usage of ASoC.
21. User entities are responsible for the consequences of their use of ASoC.
22. User entities are responsible for deployment, configuration and operation of ASoC utilities (clients) provided by HCLSoftware to be used on the user entity's network.
23. User entities are responsible for establishing appropriate controls and following appropriate security practices for ASoC utilities (clients) on the user entity's network.
24. User entities are responsible for training their users on the use of ASoC.
25. User entities are responsible for defining, documenting, and making available to their users, procedures for the operation of ASoC.
26. User entities are responsible for their network security requirements and connecting securely to ASoC.

27. User entities are responsible for establishing Internet connectivity to enable the use of ASoC securely.
28. User entities are responsible for managing compliance with applicable laws / regulations over the use of ASoC.
29. User entities are responsible for understanding and complying with their contractual obligations to HCLSoftware.
30. User entities are responsible for notifying HCLSoftware of any actual or suspected security incidents or breaches in ASoC.
31. User entities are responsible for notifying HCLSoftware about any unauthorized use of ASoC.
32. User entities are responsible for notifying HCLSoftware about operational problems in ASoC.