NOTICE: Report use and distribution limitations

Ernst & Young LLP ("EY") has prepared the attached report (the "Report") in accordance with the requirements of the applicable professional standards as described in the attached Report, for Apple Inc. (the "Company"). The Report is intended only to be used by management of the Company, members of the Apple Security Research Device Program, and Apple for Enterprise customers (collectively, the "Specified Parties"), as stated in the independent service auditor's report contained in the Report.

If you are a Specified Party, you may proceed to the Report.

In addition, entities other than the Specified Parties, including certain prospective user entities, identified by the Company (collectively, each an "Other Recipient"), may read the Report subject to the terms of this NOTICE. If you are an Other Recipient, you may only read the Report if you agree to the terms and conditions set forth below. Please review them carefully.

1. You acknowledge that the Report was prepared solely for the benefit and use of the Specified Parties and was not intended for any other purpose. Accordingly, EY has made no representation or warranty to the Other Recipient as to the sufficiency of the information contained in the Report. As such, any use of the Report by the Other Recipient is at the sole and exclusive risk of the Other Recipient.
2. Distribution or disclosure of any portion of the Report or any information or advice contained therein to persons other than the Company is prohibited.
3. The Other Recipient (a) does not acquire any rights against EY, any other member firm of the global Ernst & Young network, or any of their respective affiliates, partners, agents, representatives or employees (collectively, the "EY Parties"), and EY assumes no duty or liability to the Other Recipient, in connection with its reading of the Report; (b) may not rely on the Report; and (c) will not contend that any provisions of United States or state securities laws could invalidate or avoid any provision of this agreement.
4. Except where compelled by legal process (of which the Other Recipient shall promptly inform EY so that EY may seek appropriate protection), the Other Recipient will not disclose, orally or in writing, any Report or any portion thereof, or make any reference to EY in connection therewith, in any public document or to any third party.
5. The Other Recipient (for itself and its successors and assigns) hereby releases each of the EY Parties, from any and all claims or causes of action that the Other Recipient has, or hereafter may or shall have, against them in connection with the Report or the Other Recipient's reading of the Report. The Other Recipient shall indemnify, defend and hold harmless the EY Parties from and against all claims, liabilities, losses and expenses suffered or incurred by any of them arising out of or in connection with (a) any breach of the terms in this NOTICE by the Other Recipient or its representatives; and/or (b) any use or reliance on the Report by any party that obtains a copy of the Report, directly or indirectly, from or through the Other Recipient or at its request.

If you are an Other Recipient, by reading the Report, you signify that you, on behalf of your organization, agree to be bound by these terms and conditions. If you do not agree to these terms, please close this document and contact your representative at the Company.

Apple Inc.

SOC 3® – System and Organization Controls for Service Organizations: Trust Services Criteria

Management’s Report of Its Assertions on the Effectiveness of Its Controls over the Private Cloud Compute Provisioning System Based on the Trust Services Criteria for Security, Processing Integrity, and Confidentiality

For the Period February 1, 2025 to January 31, 2026

Ernst & Young LLP
303 Almaden
Boulevard
San Jose, CA 95110

Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Shape the future
with confidence

Independent Service Auditor's Assurance Report

Management of Apple Inc.

Scope

We have examined management's assertion, contained within the accompanying *Management's Report of Its Assertions on the Effectiveness of Its Controls over the Private Cloud Compute Provisioning System Based on the Trust Services Criteria for Security, Processing Integrity, and Confidentiality* (Assertion), that Apple Inc.'s (Apple) controls over the Private Cloud Compute Provisioning System (System) were effective throughout the period February 1, 2025 to January 31, 2026, to provide reasonable assurance that Apple's service commitments and system requirements were achieved based on the trust services criteria relevant to security, processing integrity, 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*.

Apple uses Digital Realty Trust, Inc. ("Digital Realty"), Equinix Inc. ("Equinix"), and NEXTDC Limited ("NEXTDC") (together, "subservice organizations") to provide physical security and environmental safeguard controls. The description of the boundaries of the system presented at Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with related controls at Apple, to provide reasonable assurance that Apple's service commitments and system requirements are achieved based on the applicable trust services criteria. The description of the boundaries of the system presents the types of controls that the service organization assumes have been implemented, suitably designed, and are operating effectively at Digital Realty, Equinix and NEXTDC. Our procedures did not extend to the services provided by Digital Realty, Equinix, or NEXTDC and we have not evaluated whether the controls management assumes have been implemented at Digital Realty, Equinix, and NEXTDC have been implemented or whether such controls were suitably designed and operating effectively throughout the period February 1, 2025 to January 31, 2026.

Management's responsibilities

Apple's management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that Apple's service commitments and system requirements were achieved. Apple management is also responsible for providing the accompanying assertion about the effectiveness of controls within the System, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the service commitments and system requirements that are the objectives of the System.

Shape the future
with confidence

Our responsibilities

Our responsibility is to express an opinion on the controls over the System, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether the controls over the System operated effectively, in all material respects. An examination involves performing procedures to obtain evidence about the controls over the System, which includes: (1) obtaining an understanding of Apple's relevant security, processing integrity, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we consider necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Apple's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Our examination was not conducted for the purpose of evaluating the performance or integrity of Apple's Artificial Intelligence (AI) services. Accordingly, we do not express an opinion or any other form of assurance on the performance or integrity of Apple's AI services.

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

We apply International Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services engagements*, which requires that we design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Inherent limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Apple's service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the System or controls, or the failure to make needed changes to the System or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Shape the future
with confidence

Opinion

In our opinion, Apple's controls over the System were effective throughout the period February 1, 2025 to January 31, 2026, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Restricted use

This report is intended solely for the information and use of Apple, members of the Apple Security Research Device Program, and Apple for Enterprise customers and is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst & Young LLP

May 21, 2026

Management's Report of Its Assertions on the Effectiveness of Its Controls over the Private Cloud Compute Provisioning System Based on the Trust Services Criteria for Security, Processing Integrity, and Confidentiality

May 21, 2026

We, as management of Apple, are responsible for:

- Identifying the Private Cloud Compute Provisioning System (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our service commitments and system requirements, which are presented in Attachment B
- Identifying the risks that would threaten the achievement of our service commitments and system requirements that are the objectives of our System
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the service commitments and system requirements
- Selecting the trust service categories and associated criteria that are the basis of our assertion

Apple uses Digital Realty, Equinix, and NEXTDC to provide physical security and environmental safeguard controls. The description of the boundaries of the system presented in Attachment A indicates that complementary controls at Digital Realty, Equinix, and NEXTDC that are suitably designed and operating effectively are necessary, along with controls at Apple, to achieve the service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Apple's controls. It does not disclose the actual controls at Digital Realty, Equinix, or NEXTDC.

We confirm to the best of our knowledge and belief that the controls over the System were effective throughout the period February 1, 2025 to January 31, 2026, to provide reasonable assurance that the service commitments and system requirements were achieved based on the applicable trust services criteria relevant to security, processing integrity, 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*.

Apple Inc.

Attachment A

Apple's Description of the Boundaries of the Private Cloud Compute Provisioning System

Company Overview

Apple Inc. ("Apple" or "the Company") is an SEC-registered company headquartered in Cupertino, California. Apple is one of the world's leading brands, offering a range of products designed for end-user computing and services to complement these products. The Private Cloud Compute (PCC) platform enables the use of Apple Intelligence, providing customers a product that complements Apple's line-up of hardware, software and services. The hardware provisioning process is predicated on the same manufacturing integrity, rigor, and oversight that Apple uses for customer devices.

Description of Services Provided

Apple's Private Cloud Compute is a platform that permits customers to use Apple Intelligence, leveraging the capabilities of high-performance cloud computing in a secured manner that maintains the confidentiality of customer data. Private Cloud Compute is available for customers with supported Apple devices (currently, iPhone 15 Pro or later, iPad and Mac with M1 and later Apple silicon chips, iPad mini with A17 Pro or later Apple silicon chips, Apple Vision Pro, Apple Watch Series 6 and later, all Apple Watch Ultra models, and Apple Watch SE 2 and later when paired with an Apple Intelligence-enabled iPhone nearby).

Private Cloud Compute was designed to enable Apple Intelligence to operate securely and privately with customer personal data. The services supported by Private Cloud Compute will enable additional functionality for customers to more efficiently and effectively use their Apple devices, allowing for new machine learning capabilities as a means of increasing productivity.

This system description pertains to Private Cloud Compute and covers the processes used for the provisioning, ongoing verification, and protection of information within compute nodes and the related policies, procedures and control activities. Public-facing documentation is published and provided that describes the purpose, design, and boundaries of the system.

The scope of this examination does not extend to Apple devices or to the accuracy of any requests processed using Apple Intelligence. Likewise, requests using on-device processing, or leveraging ChatGPT, are not covered by this system description as they are not processed by Private Cloud Compute. Refer to User Entity Responsibilities.

System Components

Infrastructure

Private Cloud Compute leverages Apple owned and operated Data Centers, some of which include Certificate Authority (CA) facilities, as well as carrier neutral co-location facilities around the world.

Software

Private Cloud Compute is supported by a variety of in-house and third-party software applications that are used to build, support, secure, maintain and monitor each respective system.

Code Management and Deployment Tools

Private Cloud Compute leverages a combination of Bitbucket, GitHub, Jenkins and in-house continuous build, integration and deployment tooling to build and deploy software to production compute nodes.

Operating System

Private Cloud Compute's software stack starts with a custom operating system based on a minimized and hardened subset of iOS. This brings Apple's existing security posture of iOS to Private Cloud Compute such that, as Apple adds new security features to the foundations of iOS, Private Cloud Compute nodes will naturally inherit those features.

This foundation supports a set of cloud extensions which enables Private Cloud Compute nodes to integrate with the data center infrastructure, including fleet management and diagnostic tooling.

Finally, Private Cloud Compute includes the software layer that enables inference on Large Language Models (LLMs) — which is the capability that powers Apple Intelligence. This includes the ability to distribute requests across multiple Private Cloud Compute nodes.

During the Private Cloud Compute hardware provisioning process, the ceremony toolkit requests the runtime measurements for each compute node and validates them against the approved values from the transparency log

Similarly, supported user devices can only send private requests to Private Cloud Compute nodes which have their software measurements present in the transparency log.

Hardware

The Private Cloud Compute system's trusted computing base is the node's Apple silicon system-on-a-chip (SoC) and the related software stack.

The security design of Private Cloud Compute relies on being able to encrypt a request end-to-end from a user device to a Private Cloud Compute node based on its strong cryptographic identity.

People

The teams supporting Private Cloud Compute are staffed by experienced professionals with a common set of goals and objectives. The teams are organized as follows:

Crypto Services

- Certificate Management for requesting and managing digital certificates.
- Cryptographic services that provide encryption and signing capabilities
- Key Management for managing encryption keys
- Secrets Management for managing sensitive information

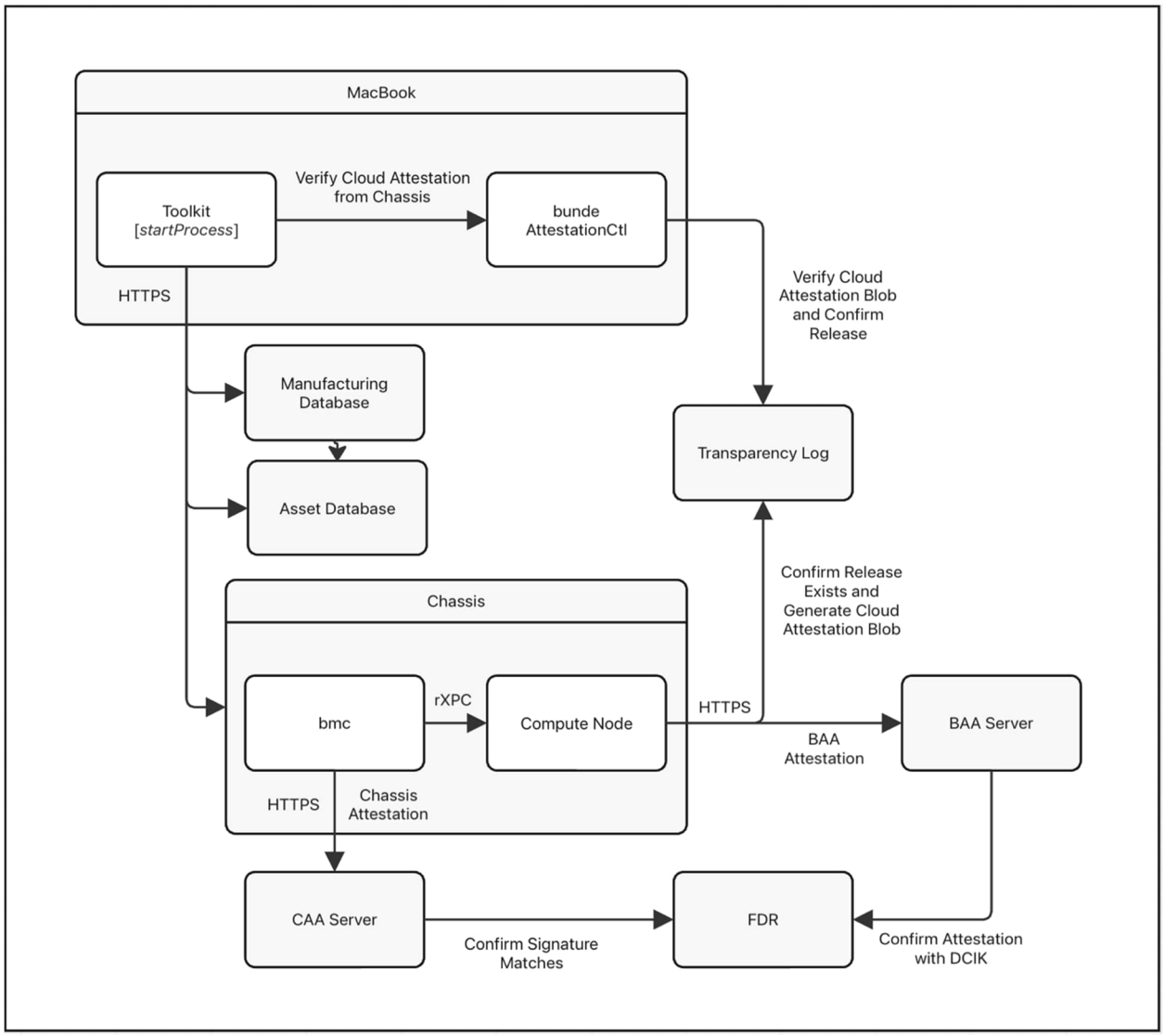
Private Cloud Compute Functions

- Apple Services Engineering: Developing the Private Cloud Compute service.
- Site Reliability Engineering: Ensuring availability and resiliency of Private Cloud Compute services.

Data

User data is the prompts and any context provided from the user device to a Private Cloud Compute node as part of a user's inference request. A prompt is the instructions or questions input by the user to an LLM. Context refers to any additional information or data provided by the user to enable an LLM to better understand the question and provide a more accurate answer.

Hardware Provisioning Control Activities

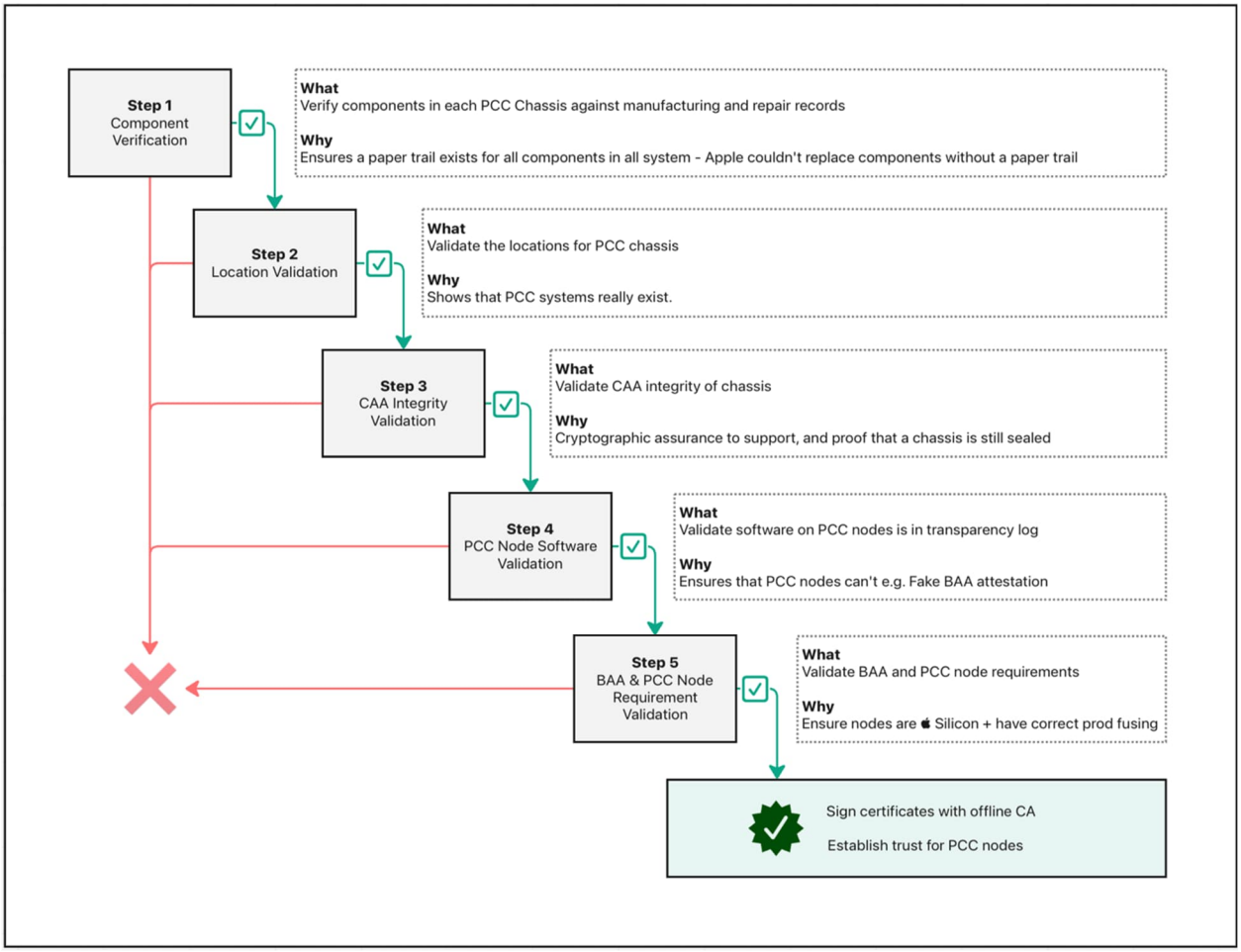


Node Provisioning

The security of Apple's CA is only as secure as the inputs into the certificate issuance process which are used to control issuance of certificates to appropriate Private Cloud Compute nodes. For this reason, Apple has built a comprehensive and robust provisioning flow that serves as the input to Apple's ceremony process.

The provisioning process implements multiple controls to validate the integrity of the hardware and software on the node and to confirm that the node was received in the exact same state it left the manufacturing facility. These controls require a multi-party quorum. Following the validation of each control for each node, signing requests are generated for the offline CA to sign.

Each certificate signing ceremony may need to operate on thousands of nodes while verifying a large range of controls, and the same steps must be executed consistently each time. To support this, Apple has created a toolkit which automates the steps to be taken for each ceremony and implements the necessary controls. At the start of each ceremony, there is an initial check to validate that an approved version of the toolkit is being used. Once confirmed, the ceremony can proceed. The toolkit's controls then validate:



To verify the toolkit's behavior, this requires observing, inspecting, and re-performing the provisioning ceremony controls. In addition to batch-mode processing, the toolkit is also able to:

- run all controls for a specified node or list of nodes,
- run a single specified control for a specified node (or list of nodes),
- output the Uniform Resource Locators being queried for a single control, so they can be manually re-performed outside of the toolkit, and
- output the full request/responses for a single control for a single node.

Each individual Private Cloud Compute node must pass all five validation checks before a certificate is issued.

User Entity Responsibilities

The system was designed with the assumption that controls included in this section would be implemented by user entities (e.g., users). The user entity responsibilities presented should not be regarded as a comprehensive list of all controls that should be employed by the user. The implementation of additional controls may be appropriate.

- Users are responsible for updating their Apple devices to the latest versions of Apple OSes (e.g., iOS or macOS). A minimum version of iOS 18.1, iPadOS 18.1, macOS Sequoia 15.1, visionOS 2.4, or watchOS 11 on a supported device is needed for a device to work with Private Cloud Compute.

Complementary Subservice Organization Controls

Apple uses Digital Realty, Equinix, and NEXTDC as subservice organizations for physical security and environmental safeguards. The description does not extend to the services provided by Digital Realty, Equinix, or NEXTDC, and as such, control activities performed by Digital Realty, Equinix, and NEXTDC have been excluded from this system description. However, Apple controls related to the Private Cloud Compute system cover only a portion of the internal control structure for user entities. In designing its system, Apple expects Digital Realty, Equinix, and NEXTDC to implement physical security controls to achieve its service commitments and system requirements based on the applicable trust services criteria.

To gain reasonable assurance over the Digital Realty, Equinix, and NEXTDC control environments related to physical security, AIS obtains and reviews the Digital Realty, Equinix, and NEXTDC SOC 1® and/or SOC 2® Type 2 reports on an annual basis.

The following list includes the expected subservice organization controls for Digital Realty, Equinix, and NEXTDC but should not be regarded as a comprehensive list of all controls that should be employed.

Criteria	Control Activity
CC2.3	The subservice organization provides publicly available mechanisms for customers to contact them to report security events and publishes information including a system description and security and compliance.

Criteria	Control Activity
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. 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.
CC7.3	Incidents are logged within a ticketing system, assigned severity rating, and tracked to resolution.

Attachment B

Principal Service Commitments and System Requirements

Service commitments are declarations made by Apple management to user entities (users) about the system used to provide the service. Service commitments are communicated in written individualized agreements, standardized contracts, service level agreements, or published statements.

Apple designs its processes and procedures to achieve the objectives for the Company's foundational beliefs and security goals. The objectives are rooted in Apple's belief that privacy is a fundamental human right, along with the laws and regulations that govern the provision of services, and the financial and operational requirements that Apple has established for the services. The primary objective of this report is to describe the Apple controls that are intended to help ensure that all hardware, operating system and firmware in systems provisioned for use with Private Cloud Compute would adhere to the security, processing integrity, and confidentiality policies Apple has published for Private Cloud Compute.

Apple designed Private Cloud Compute to achieve its service commitments and system requirements to customers. The security and compliance efforts of Apple evidence the organization's commitment to designing, implementing, and operating effective controls. Apple's commitments are as follows:

- Security: Systems used for Private Cloud Compute are protected against unauthorized access including, but not limited to, data encryption, monitoring and alerting, and multi-factor authentication. These systems must go through a secure provisioning process that validates – physically, logically and cryptographically – (1) the integrity of the hardware and (2) the specifications to support the Private Cloud Compute workloads.
- Processing Integrity: For every hardware provisioning ceremony, a quorum composed of team members from three separate Apple teams is required to issue certificates to Private Cloud Compute nodes. Each ceremony follows a detailed set of instructions and uses a toolkit that largely automates each step taken during the certificate issuance process and includes controls to confirm that the offline Hardware Security Modules have not issued any certificates outside of the provisioning ceremony. Each individual Private Cloud Compute node must pass all validation checks before a certificate is issued.
- Confidentiality: User data is encrypted directly to the Private Cloud Compute nodes that are processing a request, and the decrypted user data is retained for the time period needed to complete the request. Private Cloud Compute uses the data only to perform the operations requested by the user device.

  Before processing user data, Private Cloud Compute nodes enter a Restricted Execution Mode (REM) which systemically restricts the processes that are able to run to those for which an REM policy has been defined. This prevents debugging or administrative commands from being executed on the Private Cloud Compute nodes, thereby enforcing the confidentiality of data being processed.

  Private Cloud Compute's Ephemeral Data Mode means the data volume's encryption keys are rotated on every boot so that data written to the data volume does not persist to the next boot of the system. This functions to cryptographically erase the data volume every time a Private Cloud Compute node reboots.

Specifically for the Private Cloud Compute hardware provisioning process, the following requirements must be met:

- Maintain an appropriate chain of custody for the node's hardware over its entire lifecycle
- Validate that the node is authentic, untampered Apple silicon
- The node's specification and configuration meet the security and confidentiality policies Apple has published for Private Cloud Compute.