Render

Render Services, Inc.

Report on Controls at a Service Organization Relevant to Security, Confidentiality, and Availability

SOC 3®

For the Period October 1, 2024 to September 30, 2025

SOC 3 is a registered service mark of the American Institute of Certified Public Accountants (AICPA)

BARR ADVISORY

Independent Service Auditor's Report

To the Management of Render Services, Inc. ("Render"):

Scope

We have examined Render's accompanying assertion titled "Assertion of Render Management" (assertion) that the controls within the Render Platform (the "system") were effective throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Render's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and availability (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).

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

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

Our examination included:

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

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within the Render Platform were effective throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Render's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

BARR Advisory, P.A.

Fairway, KS

November 7, 2025

Assertion of Render Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Render Platform (the "system") throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Render's service commitments and system requirements relevant to security, confidentiality, and availability were achieved. Our attached description of the boundaries of the system of the Render Platform identified 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 October 1, 2024 to September 30, 2025, to provide reasonable assurance that Render's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and availability (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) are presented in the attached description of the boundaries of the system.

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

We assert that the controls within the system were effective throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Render's service commitments and system requirements were achieved based on the applicable trust services criteria.

Render Services, Inc.

November 7, 2025

©2025 Render Services, Inc. | All rights reserved |

Render's Description of the Boundaries of Its Render Platform

Description of Services Provided

Render Services, Inc. ("Render" or the "company") is a unified cloud used to build and run apps and websites with Transport Layer Security (TLS) certificates, a global content delivery network (CDN), distributed denial-of-service (DDoS) protection, private networks, and auto deploy from Git for users around the world. Render launched in 2019 and is headquartered in San Francisco, California.

Render's core product, the Render Platform (the "platform"), is a Platform as a Service (PaaS) solution that includes the following services:

- Static sites, web services, background workers, and cron jobs
- Virtual hosting of anything with custom Dockerfiles or native environments
- The ability to run internal services on a private network with ease
- Fully managed PostgreSQL databases with automated backups
- Fully managed Redis service with persistence
- Fully managed in-memory storage using Redis with live metrics

Additionally, Render has developed a Software as a Service (SaaS) dashboard and public REST application programming interface (API) that is used to manage PaaS solutions, included in the Render Platform.

Components of the System Used to Provide the Services

The purpose of the description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below: infrastructure, software, people, data, and processes and procedures.

Infrastructure and Software

Render currently hosts the Render Platform in Amazon Web Services (AWS) and Google Cloud Platform (GCP). Aside from the Render Platform, there is a Render Administration App used by internal Render personnel that is hosted within GCP. The PaaS and administration portal are hosted in virtual private cloud (VPC) environments which protects the network from unauthorized external access. The network topology includes segmented VPCs, web application firewalls (WAFs), and access control lists (ACLs). User requests to Render's web-based systems are encrypted using TLS using certificates from an established third party certificate authority. Remote system administration access to Render web and application servers is available through a virtual private network (VPN) connection. The hardware components that make up the aforementioned system include servers hosted, managed, and protected by either AWS or GCP. Production servers at AWS and GCP maintain failover capabilities in the event of physical hardware or logical software failures. This infrastructure is hosted in high-availability data centers with multiple availability zones.

©2025 Render Services, Inc. | All rights reserved |

Render is responsible for managing the development and operation of the Render Platform, including the custom application codebase, and the selection of key vendor software systems. Infrastructure components such as servers, databases, and storage systems are developed and maintained by vendors, including AWS, GCP, as well as suppliers of source code repository software, single sign-on software, a web application firewall, and a password manager.

People

Render is organized in the following functional areas:

- **Corporate:** Responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
- **Engineering:** Responsible for the development, testing, deployment, and maintenance of the source code for the system. Also responsible for the product life cycle, including adding additional product functionality.
- **Security:** The security team is responsible for access controls, security of the production environment, all security and access controls for the company, risk assessment, privacy, vulnerability threats, and are members of the information security management system (ISMS) management committee.
- **ISMS Management Committee:** Responsible for coordinating with other members of the ISMS management committee and hosting ISMS management committee meetings at least annually. The members of the ISMS management committee are documented internally and include the corporate, ISMS manager, and other key ISMS stakeholders.
- **ISMS Manager:** Oversees the ISMS management committee and approves information security policies and procedures.
- **People:** Responsible for recruiting and onboarding new personnel, defining roles and positions for new hires, performing background checks, and facilitating the personnel termination process.
- **IT:** Responsible for managing laptops, software, and other technology involved in personnel productivity and business operations.
- **Customer Support:** Responsible for account management, customer success, and customer support activities.

Data

Data, as defined by Render, constitutes any information collected from personnel, candidates, users, customers, vendors, or other parties that provide information to Render.

Information assets are assigned a sensitivity level based on the audience for the information. The sensitivity level then guides the selection of protective measures to secure the information. All data is to be assigned one of the following sensitivity levels:

©2025 Render Services, Inc. | All rights reserved |

Sensitivity Level	Description	Examples of Data
Restricted	Restricted data includes any information that Render has a legal or regulatory obligation to safeguard in the most stringent manner. Data should be classified as restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to Render, its customers, or its partners. The highest level of security controls should be applied to restricted data.	• Render codebase • Intellectual property • Passwords, private keys, and other credentials • Bank information • Tax IDs • Information related to pending litigation or investigations • Data required to be protected by regulatory obligations • Additional employment information (e.g., background checks, health and medical information, social security numbers)
Confidential	Confidential data is information that, if made available to unauthorized parties, may adversely affect individuals or Render. This classification also includes data that Render may be required to keep confidential, either by law or under a confidentiality agreement or business associate agreement with a third party, such as a vendor.	• Individual employment information (e.g., salary, benefits, and performance evaluations for current, former, and prospective personnel) • Legal documents • Customer data • Contractual agreements • Compliance reports (i.e., SOC 2) • Data that is subject to an NDA or other confidentiality clause • Information shared by partners or investors
Internal	Internal data is information that is potentially sensitive and is not intended to be shared with the public. Internal data should be classified as such when the unauthorized disclosure, alteration, or destruction of that data would result in moderate risk to Render, its customers, or its partners.	• Unpublished Render memos • Unpublished marketing materials • Non-public Render customer and partner names and email • Procedural documentation that should remain private such as on-call runbooks and engineering guides

©2025 Render Services, Inc. | All rights reserved |

Sensitivity Level	Description	Examples of Data
Public	Public data is information that may be disclosed to any person regardless of their affiliation with Render. The public classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that does not require any level of protection from disclosure.	• Published press releases • Published documentation • Published press releases • Published documentation • Published blog posts anything on the Render public website • Anything on Render social media profiles

The Render Platform processes the information types as described in the table above. To assist with the data handling procedures, Render has policies in place that define system and operational requirements for data classification, retention, encryption, storage, and secure disposal. The policies are reviewed and updated accordingly on at least an annual basis by the security function.

©2025 Render Services, Inc. | All rights reserved |

Processes and Procedures

Render has developed and communicated policies and procedures to manage the information security of the system. Information security policies, including sanctions for policy violations, are approved by the security function at least annually and published on internal collaboration tools accessible to all personnel with access to Render systems. These policies and procedures cover the following key security life cycle areas:

- Acceptable Use
- Access Control and Termination
- Business Continuity and Disaster Recovery
- Change Management
- Code of Conduct
- Configuration and Asset Management
- Data Classification
- Data Retention and Disposal
- Encryption and Key Management
- ISMS Corrective Actions
- ISMS Monitoring and Measuring
- ISMS Roles and Responsibilities
- Enforcement
- Network Security
- Physical Security
- Risk Assessment and Treatment
- Secure Development
- Security Incident Response
- Vendor Management
- Vulnerability and Patch Management

©2025 Render Services, Inc. | All rights reserved |

Principal Service Commitments and System Requirements

Render designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Render makes to its customers, business partners, vendors, and subservice organizations and the operational and compliance requirements that Render has established for the services. Service commitments are declarations made by management to its customers regarding the performance of the Render system. Service commitments are set forth in standardized contracts, service-level agreements (SLAs), and in the description of the service offering provided online.

Commitments to user entities are documented and communicated in SLAs and other customer agreements, as well as in the description of the service offering provided online.

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role;
- Use of intrusion detection systems (IDS) to identify potential security attacks from users outside the boundaries of the system;
- Weekly vulnerability scans over the system and network, and annual penetration tests over the production environment; and,
- Operational procedures for managing security incidents and breaches, including notification procedures.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit;
- Confidentiality and non-disclosure agreements (NDAs) with employees, contractors, and third parties;
- Confidential information must be used only for the purposes explicitly stated in agreements between Render and user entities; and,
- Use of data retention and data disposal processes for system and customer information.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components;
- Responding to customer requests in a reasonably timely manner;
- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities; and,
- Operational procedures supporting the achievement of availability commitments to user entities.

©2025 Render Services, Inc. | All rights reserved

Render establishes system requirements that support the achievement of service commitments, relevant operational and compliance requirements, applicable laws and regulations, and other system requirements including the following:

- System functional requirements derived from service commitments, published documentation of system functionality, and other descriptions of the system;
- Monitoring of third-party providers to detect failures of those service providers to meet service agreements that could threaten the achievement of the service organization's service commitments and system requirements and respond to those failures; and,
- Business processing rules, standards, and regulations, including:
    - Digital Millennium Copyright Act of 1998 (DMCA);
    - ISO/IEC 27001: 2022
    - The NIST Cybersecurity Framework; and,
    - HIPAA

Render establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Render's system policies and procedures, system design documentation, and contracts with customers. 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 personnel are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system. Information security policies, including sanctions for policy violations, are approved by management at least annually and published on internal collaboration tools (i.e., Vanta) accessible to all personnel with access to the company systems.

©2025 Render Services, Inc. | All rights reserved |