Insight Assurance

Trusted Risk Advisory Professionals

System and Organization Controls 3 (SOC 3) Report

Report on StackState BV's Description of SaaS Services System of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability and Confidentiality Throughout the Period September 27, 2021, to December 26, 2021

TABLE OF CONTENTS

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: StackState BV

Scope

We have examined StackState BV's (StackState) accompanying assertion titled "StackState BV's Management Assertion" (assertion) that the controls within StackState's SaaS Services System (system) were effective throughout the period September 27, 2021, to December 26, 2021, to provide reasonable assurance that StackState'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 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

StackState uses a subservice organization to provide hosting services. The assertion indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at StackState, to achieve StackState's service commitments and system requirements based on the applicable trust services criteria. Attachment A presents the types of complementary subservice organization controls assumed in the design of StackState's controls. Attachment A 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 assertion indicates that certain complementary user entities are necessary, along with controls at StackState, to achieve StackState's service commitments and system requirements based on the applicable trust services criteria. Attachment A presents the complementary user entity controls assumed in the design of StackState'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

StackState 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 StackState's service commitments and system requirements were achieved. StackState has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, StackState 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.

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 StackState's service commitments and system requirements based on the applicable trust service criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve StackState'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 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 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.

Basis for Qualified Opinion

StackState states in its description of its SaaS Services System that performance evaluations are completed annually for all employees. However, there was no documentation to support that annual performance evaluations were completed. As a result, the controls were not operating effectively during the period September 27, 2021, to December 26, 2021, to provide reasonable assurance that its service commitments and system requirements were achieved based on trust services criterion CC1.5, *The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.*

Insight Assurance LLC

Tampa, Florida
April 8, 2022

STACKSTATE BV'S MANAGEMENT ASSERTION

StackState

STACKSTATE BV'S MANAGEMENT ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within StackState BV's (StackState) SaaS Services System (system) throughout the period September 27, 2021, to December 26, 2021, to provide reasonable assurance that StackState's service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. Our description of the boundaries of the system is presented in Attachment A, titled, "StackState BV's Management Description of the Boundaries of its SaaS Services System ", and identifies the aspects of the system covered by our assertion.

StackState uses a subservice organization to provide cloud hosting services. Attachment A indicates that effective complementary subservice organization controls are necessary, along with controls at StackState, to achieve StackState's service commitments and system requirements based on the applicable trust services criteria. Attachment A presents the types of complementary subservice organization controls assumed in the design of StackState's controls. Attachment A does not disclose the actual controls at the subservice organization.

Attachment A indicates that complementary user entity controls are necessary, along with controls at StackState, to achieve StackState's service commitments and system requirements based on the applicable trust services criteria. Attachment A presents the complementary user entity controls assumed in the design of StackState's controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period September 27, 2021, to December 26, 2021, to provide reasonable assurance that StackState'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 (AICPA, Trust Services Criteria). StackState'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 Attachment B titled "StackState's Principal Service Commitments and System Requirements."

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.

Except for the matter describer belowm, we assert that the controls within the system were effective throughout the period September 27, 2021, to December 26, 2021, if complementary subservice organization controls and complementary user entity controls were effective, to provide reasonable assurance that StackState's service commitments and system requirements were achieved based on the applicable trust services criteria.

StackState states in its description of its SaaS Services System that performance evaluations are completed annually for all employees. However, there was no documentation to support that annual performance evaluations were completed. As a result, the controls were not operating effectively during the period September 27, 2021, to December 26, 2021, to provide reasonable assurance that its service commitments and system requirements were achieved based on trust services criterion

CC1.5, *The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.*

StackState BV

April 8, 2022

ATTACHMENT A

STACKSTATE'S DESCRIPTION OF ITS SAAS SERVICES SYSTEM

COMPANY BACKGROUND

Stackstate BV ("StackState") is a privately held company established in September 2015, Services. StackState is a BV headquartered in Hilversum, Netherlands.

SERVICES OVERVIEW

StackState provides a software platform that allows companies to monitor and report on their on-premise and cloud based infrastructure. StackState imports information from many systems in realtime, via the use of an agent. It then uses this information to find issues and show the root cause of those issues. These leads to higher uptime and reduced time to resolve an issues, when they occur.

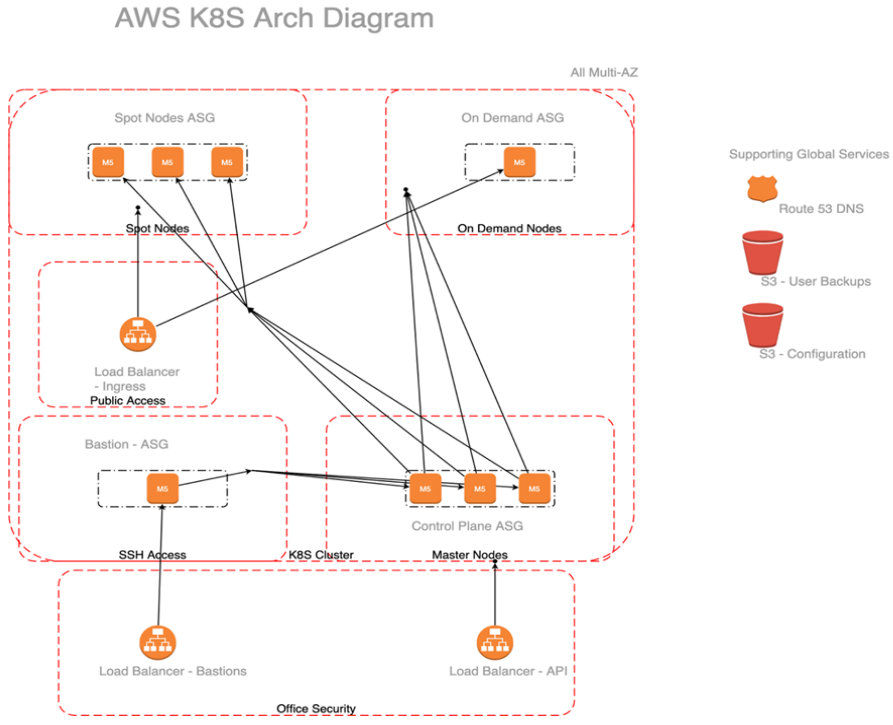
StackState provides both an on premise and SaaS offering of its software to enable customers to do Hybrid IT as well full public/private cloud.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The System description is comprised of the infrastructure, software, people, data and procedures at the service organization.

Infrastructure

StackState maintains a system inventory that includes virtual machines (EC2 instances), computers (desktops and laptops), and cloud based storage (S3). The inventory documents device name, device type, vendor function, OS, location, and notes. To outline the topology of its network, the organization maintains the following network diagram.



The StackState application infrastructure is located at AWS' data centers. AWS acts as a hosting subservice organization for the company. The subservice organization (SSO) provides the physical security and environmental protection controls, as well as, managed services for StackState's infrastructure.

The SSO's network security uses hardware and software-based intrusion prevention, advanced content filtering, anti-malware, and anti-spam modules.

In addition to the firewall, StackState uses anti-virus and anti-spyware applications to protect systems from viruses.

StackState's Information Security Policy and security procedures ensure that all computer devices (including servers, desktops, printers, etc.) connected to the StackState network have proper virus protection software, current virus definition libraries, and the most recent operating system and security patches installed. The IT department verifies that all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating. In the event of a virus threat, the anti-virus system will attempt to delete or quarantine the infected file. If the virus cannot be deleted or quarantined, the infected machine will be disconnected from the network and cleaned manually.

Multiple controls are installed to monitor traffic that could contain malicious programs or code. External perimeter scans are performed annually by a third-party vendor to expose potential vulnerabilities to the production environment and corporate data. Email is scanned at the gateway and in the hosted email environment. Server operating systems utilize anti-virus and anti-spyware programs. All employee workstation computers have a minimum standard hardware and software configuration. Employees are not allowed to install any software on StackState-owned computers. IT staff maintains several replacement computers that can replace workstations in need of repair or maintenance, thereby disrupting the employee's workday as little as possible.

Software

StackState maintains a list of critical software in use within its environment. The organization also retains appropriate software license documentation. Critical software in use includes the following:

- Gitlab
- GitHub
- Jira
- Slack
- AWS

People

The StackState staff provides support to the above services. StackState employs dedicated team members to handle all major product functions, including operations, and support. The IT Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the StackState and its data secure. The following are key roles that support the system and operations of the company.

Chief Executive Officer (CEO) – Handles the strategic direction of the organization. The CEO assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments.

Chief Fiancial Officer (CFO) – Handles the overarching financials of the company and leads investment and M&A discussions as well as input into the day to day running of company

VP Product – Responsible for the overarching direction of the product. Taking input from customers as well as internal resources directs development and product focus to meet the needs of stakeholders

Chief Technology Officer – Responsible for the technological direction and advancements of the organization. Directs the operations, engineering, and support teams to efficiently create/present new services, maintain existing ones, and help support the StackState customer based using the service.

VP SaaS – Responsible for the overarching direction of the SaaS Offering. Taking input from customers as well as internal resources directs development and product focus to meet the needs of stakeholders for the monthly subscription based version of the product

Head of Communication – Primary responsible for creating customer communications channels as well as creating the tone and personalities for marketing materials

Head of lead generation – Primary responsible to create new lead generation strategies for the organisation

Consultants/support – The professional services organisation liaises with customers to provide installation and support services.

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements. Customer data is captured which is utilized by StackState in delivering its SaaS Services.

Information takes many forms. It may be stored on computers, transmitted across networks, printed or written on paper, and spoken in conversations. All employees and contractors of StackState are obligated to respect and, in all cases, to protect confidential and private data. Customer information, employment-related records, and other intellectual property-related records are, subject to limited exceptions, confidential as a matter of law. Many other categories of records, including company and other personnel records, and records relating to StackState's business and finances are, as a matter of StackState policy, treated as confidential. Responsibility for guaranteeing appropriate security for data, systems, and networks is shared by the Client Services and IT Departments. IT is responsible for designing, implementing, and maintaining security protection and retains responsibility for ensuring compliance with the policy. In addition to management and the technology staff, individual users are responsible for the equipment and resources under his or her control.

StackState has policies and procedures in place to ensure prior retention and disposal of confidential and private data. The retention and data destruction policies define the retention periods and proper destruction procedures for the disposal of data. These policies are reviewed at least annually. The destruction of data is a multi-step process. Client data is deleted upon termination of the contract. A ticket is created and assigned to the product team and system engineering team to

coordinate the deletion of the data. First, all files received or generated from the client are identified and deleted by the system engineering team then the product team deletes all user-related data.

Electronic communications are treated with the same level of confidentiality and security as physical documents. Networks are protected by enterprise-class firewalls and appropriate enterprise-class virus protection is in place. Passwords protection with assigned user rights is required for access to the network, application, and databases. Access to the network, application, and databases is restricted to authorized internal and external users of the system to prohibit unauthorized access to confidential data. Additionally, access to data is restricted to authorized applications to prevent unauthorized access outside the boundaries of the system.

Procedures

Formal IT policies and procedures exist that describe logical access, computer operations, change management, incident management, and data communication standards in order to obtain the stated objectives for network and data security, data privacy, and integrity for both the company and its clients and define how services should be delivered. These are communicated to employees and located within the organization's intranet. Reviews and changes to these policies and procedures are performed annually and are approved by senior management.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

StackState uses a subservice organization to provide hosting services. Management of StackState receives and reviews the SOC 2 report of AWS on an annual basis. In addition, through its daily operational activities, the management of StackState monitors the services performed by AWS to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively to meet StackState's service commitments and system requirements based upon the security, availability and confidentiality trust services criteria.

The assertion indicates that certain applicable trust services criteria can be met only if the Subservice Organizations controls, assumed in the design of StackState's controls, are suitably designed and operating effectively along with related controls at the service organization.

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

StackState's controls related to the SaaS Services System only cover a portion of the overall internal controls for each user entity. It is not feasible for the applicable trust service criteria related to the system to be achieved solely by StackState control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of StackState.

User auditors should determine whether the following controls have been in place in operation at the user organization:

- Controls to provide reasonable assurance that user access including the provisioning and de-provisioning are designed appropriately and operating effectively.
- User entities are responsible for reporting issues with StackState systems and platforms.
- User entities are responsible for understanding and complying with their contractual obligations to StackState.
- User entities are responsible for notifying StackState of changes made to the administrative contact information.

ATTACHMENT B

STACKSTATE BV'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

StackState designs its processes and procedures related to StackState's SaaS Services System ("System") to meet its objectives. Those objectives are based on the service commitments that StackState makes to user entities, the laws and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that StackState has established for the services.

Security, availability, and confidentiality commitments to user entities are documented and communicated in service agreements, and other customer agreements, as well as in the description of the service offering provided on the organization's public website. Security, availability, and confidentiality commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of services 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.
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Uptime availability of production systems
- Ensuring correct access levels for staff and 3rd parties

StackState establishes operational requirements that support the achievement of security, availability and confidentiality, relevant laws and regulations, and other system requirements. Such requirements are communicated in system policies and procedures, system design documentation, and agreements 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 employees are hired and trained. In addition, how to carry out specific manual and automated processes required in the operation and development of the System.