Casper Validator Node

ROC (Report On Compliance)

Last Updated: July 26, 2021

Executive Summary

The consultants have performed a ROC (Report on Compliance) examination in 2021 on behalf of the ETA (Emerging Technology Association) for its 09/03/2021 Node Validators ("Entity") with it's Casper Node Staking Framework System (the 'Services') in accordance with the Trust Services Criteria (TSP) regarding Common Criteria; Security, Availability, Confidentiality and Privacy. The purpose of the report will be to assess the design of the internal controls supporting the Services. This readiness assessment is a proactive project designed to identify control weaknesses within the design of the entity's control environment. In preparation for adoption by other entities involving staking operations, this readiness assessment review was performed to review the controls in advance of the examination in order to achieve multiple objectives, including:

1. The entity management can address the findings identified during the ROC
2. The ROC testing procedures examination, the deliverable of a ROC readiness assessment report is a document intended for the use of internal management for the entities involved in the staking operations.
3. Control weaknesses identified during the ROC readiness assessment are not provided to customers or other third parties.
4. The deliverable of the ROC readiness assessment contains a report that mimics that of a Security and Compliance audit.
5. The existence of this report will allow the consultants to gain efficiencies during the ROC testing procedures for the entities involved in such operations.

Please note that as a part of this readiness assessment, inquiries and testing were performed, and controls were identified and assessed.

The high level potential control gaps noted during this review are mentioned below. Additionally, specific control gaps are noted in section 3 of this report. Management should consider implementing effective controls to mitigate these potential control gaps before undergoing any type of examination.

Guidance Regarding Information Provided by the Service Consultant

Rosadotech's examination of the controls of the Staking Node Framework was limited to the Trust Services Categories, related criteria and control activities specified by the management of the entity and did not encompass all aspects of the entity's operations or operations at user entities.

OVERVIEW OF OPERATIONS

Description of Services Provided

The Node validator provides Staking services in the Casper Network for individuals and or entities. A feature of Proof-of-Stake protocols is that token holders can actively participate in the protocol through a mechanism known as staking. Persons that hold their private keys can choose to stake their tokens with any validator in the Casper network. Alternatively, it is possible to stake tokens via an exchange or custody provider as well.

Boundaries of the System

The scope of this report includes the Staking Platform Services System performed in the United States and the European Union facilities. This report does not include the cloud hosting services provided by Amazon Web Services (AWS) or any other provider at multiple facilities.

Components of the System

Infrastructure

Primary infrastructure used to provide Staking Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Server	Containers/Servers	Hosts files and databases to support the Staking Node.
Firewalls	Firewall cloud or on-prem	Filters traffic into and out of the private network supporting the corporate services.
IDS/IPS	cloud or on-prem	Intrusion Prevention

Software

Primary software used to provide Staking Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Casper Staking	EKS (Elastic Kubernetes Service) - Ubuntu	Staking Node Service

Data

Data, as defined by the entity, constitutes the following:

- Customer Information (e.g. Personally Identifiable Information (PII))
- Customer Usage Data (e.g. clicks, interaction, time on the platform, any other metadata)
- Account information
- Documents, balances, transactions, statements
- Technical Logs
- Customer Communications

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the entity policies and procedures that define how services should be delivered. These are located on the Company's repository and can be accessed by any team member.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS or any other third party at multiple facilities. These third parties provide cloud hosting services, which includes implementing physical security controls for the housed in-scope systems.

Complementary Subservice Organization Controls

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

The following subservice organization controls have been implemented by the third party provider to provide additional assurance that the trust services criteria described within this report are met:

Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
Availability	A1.2	Third party owned data centers are protected by fire detection and suppression systems.
		Third party owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible power supply (UPS) units provide backup power in the event of an electrical failure in Third party owned data centers.
		Third party owned data centers have generators to provide backup power in case of electrical failure.

		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, UPS units, and redundant power supplies.
		The third party performs periodic reviews of colocation service providers to validate adherence with the security and operational standards.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
		Critical system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical system components are monitored for successful replication across multiple Availability Zones.

The entity’s management, along with the subservice organization, defines the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, the entity should perform monitoring of the subservice organization controls, including the following procedures:

- 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

TRUST SERVICES CRITERIA FOR THE

SECURITY CATEGORY

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Security

Security refers to the protection of:

i. information during its collection or creation, use, processing, transmission, and storage and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability

Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Core values are communicated from executive management to personnel through policies, directives, guidelines, the employee handbook and the code of conduct. An employee handbook and code of conduct is documented to communicate workforce conduct standards and enforcement procedures. Upon hire, personnel are required to acknowledge the employee handbook and code of conduct. Upon hire, personnel are required to complete a background check. Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis. Performance and conduct evaluations are performed for personnel on an annual basis. Sanction policies, which include probation, suspension and termination, are in place for employee misconduct. Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management roles and responsibilities are documented and reviewed annually. Executive management defines and documents the skills and expertise needed among its members. Executive management maintains independence from those that operate the key controls implemented within the environment. Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment. Executive management evaluates the skills and competencies of those that operate the internal controls implemented within the environment on a weekly basis. Operational management assigns responsibility for and monitors the effectiveness and performance of

CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	internal controls implemented within the environment. A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet. Executive management reviews job descriptions annually and makes updates, if necessary. Upon hire, personnel are required to acknowledge the employee handbook and code of conduct which requires adherence to the personnel's job role and responsibilities. Executive management has established proper segregations of duties for key job functions and roles within the organization. Roles and responsibilities defined in written job descriptions consider and address specific requirements relevant to the system. A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third parties. Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. Performance and conduct monitoring are communicated via weekly all-hands meetings. The entity evaluates the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities. The entity evaluates the competencies and experience of third parties prior to working with them. Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process. The entity's third-party agreement requires that third parties:

		● Consider the background, competencies and experience of its personnel ● Provide regular training to its personnel as it relates to their job role and responsibilities
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The entity has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives. Employees are required to attend continued training annually that relates to their job role and responsibilities. Executive management has created a training program for its employees. Upon hire, personnel are required to complete a background check. A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet. Upon hire, personnel are required to acknowledge the employee handbook and code of conduct which requires adherence to the personnel's job role and responsibilities. Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis. Performance and conduct evaluations are performed for personnel on an annual basis. Executive management reviews the job requirements and responsibilities documented within job descriptions annually and makes updates, if necessary. Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.
		Data flow diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system.
		Data that entered into the system, processed by the system and output from the system is protected from unauthorized access.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.
		Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet.
		Upon hire, employees are required complete cybersecurity awareness training.
		Current employees are required complete cybersecurity awareness training on an annual basis.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.
		Executive management meets weekly with operational management to discuss the entity's objectives as well as roles and responsibilities.
		Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.
		Documented escalation procedures for reporting failures, incidents, concerns and other complaints are in place and made available to personnel through the entity's intranet.

		The entity's objectives, including changes made to the objectives, are communicated to its personnel through weekly all-hands meetings.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The entity's third-party agreements delineate the boundaries of the system and describes relevant system components. The entity's third-party agreements communicate the system commitments and requirements of third parties. The entity's third-party agreements outline and communicate the terms, conditions and responsibilities of third parties. Customer commitments, requirements and responsibilities are outlined and communicated through service agreements. Changes to commitments, requirements and responsibilities are communicated to third parties, external users, and customers via mass notifications. Documented escalation procedures for reporting failures, incidents, concerns and other complaints are in place and shared with external parties.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics. Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART). Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved. Executive management reviews policies, procedures and other control documents for alignment to the entity's objectives on an annual basis. Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.

CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Executive management reviews operational and resourcing reports to evaluate performance and resourcing at least annually. Business plans and budgets align with the entity's strategies and objectives. Entity strategies, objectives and budgets are assessed on an annual basis. Documented policies and procedures are in place to guide personnel when performing a risk assessment. Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.
		The entity's risk assessment process includes: ● Identifying the relevant information assets that are critical to business operations ● Prioritizing the criticality of those relevant information assets ● Identifying and assessing the impact of the threats to those information assets ● Identifying and assessing the impact of the vulnerabilities associated with the identified threats ● Assessing the likelihood of identified threats and vulnerabilities ● Determining the risks associated with the information assets ● Addressing the associated risks ● Identified for each identified vulnerability Identified risks are rated using a risk evaluation process and ratings are approved by management. Risks identified as a part of the risk assessment process are addressed using one of the following strategies: ● Avoid the risk ● Mitigate the risk ● Transfer the risk ● Accept the risk Management develops risk mitigation strategies to address risks identified during the risk assessment process. For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to

		process owners based on roles and responsibilities. The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management. As part of the annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors and third parties.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud (e.g. fraudulent reporting, loss of assets, unauthorized system access, overriding controls) that could impact their business and operations. Identified fraud risks are reviewed and addressed using one of the following strategies: ● Avoid the risk ● Mitigate the risk ● Transfer the risk ● Accept the risk
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	As part of management's assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude. As part of management's assessment of fraud risks, management considers how personnel could engage in or justify fraudulent activities. As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT (e.g. unauthorized access, inadequate segregation of duties, default accounts, inadequate password management, unauthorized changes). Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment. Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment. Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment. Changes in vendor and third-party relationships are considered and evaluated as part of the annual comprehensive risk assessment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Monitoring Activities		
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis. On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses. Control self-assessments that include logical access reviews are performed on a quarterly basis. Vulnerability scans are performed monthly on the environment to identify control gaps and vulnerabilities. A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment. Performance and conduct evaluations are performed for personnel on an annual basis. Management obtains and reviews attestation reports of critical vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment. A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Senior management is made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance and risk assessments performed. Vulnerabilities, deviations and control gaps identified from the compliance and risk assessments are communicated to those parties responsible for taking corrective actions. Vulnerabilities, deviations and control gaps identified from the compliance and risk assessments are documented, investigated, and addressed. Management tracks whether vulnerabilities, deviations and control gaps identified as part of the

		evaluations performed are addressed in a timely manner.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations and control gaps. Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed. Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities. Prior to the development and implementation of internal controls into the environment, management considers the complexity, nature, and scope of its operations. Management has documented the relevant controls in place for each key business or operational process. Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls. Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process. Business continuity and disaster recovery plans are developed and updated on an annual basis. Business continuity and disaster recovery plans are tested on an annual basis. An analysis of incompatible operational duties is performed on at least an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Management has documented the relationship and linkage between business processes, the relevant technologies used to support the business

		processes, and the controls in place to help secure those business processes. Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet. Management has documented the controls implemented around the entity's technology infrastructure.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	As part of the risk assessment process, the use of technology in business processes is evaluated by management. The internal controls implemented around the entity's technology infrastructure include, but are not limited to: ● Restricting access rights to authorized users ● Limiting services to what is required for business operations ● Authentication of access ● Protecting the entity's assets from external threats Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet. Management has implemented controls that are built into the organizational and information security policies and procedures. Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet. Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities. Process owners and management investigate and troubleshoot control failures.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	An inventory of system assets and components is maintained to classify and manage the information assets. Privileged access to sensitive resources is restricted to authorized personnel. Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.
	Network (Google Workspace)	
		Google Workspace user access is restricted via role-based security privileges defined within the access control system. Google Workspace administrative access is restricted to user accounts accessible by the following personnel: • Chief Financial Officer (CFO) • Chief Technology Officer (CTO) Google Workspace is configured to enforce password requirements that include: • Password age (maximum) • Password length • Complexity Google Workspace users are authenticated via individually assigned user accounts and passwords. Google Workspace account recovery occurs through multi-factor authentication and security question verification. Google Workspace audit logging settings are in place that include: • Admin • Calendar • Drive • Login • Devices • Token • Groups • SAML • Google Chat • Currents • Voice • Google Meet • Users Accounts • LDAP

		• Data Studio • Groups Enterprise • Chrome
		Google Workspace audit logs are maintained and reviewed as needed.
	Production System (Application, Web, and Database Servers and Production Databases)	
		Production system user access is restricted via role-based security privileges defined within the access control system. Production system administrative access is restricted to user accounts accessible by the following personnel: • CTO • DevOps Specialist Production systems are configured to enforce password requirements that include: • Password history • Password age (maximum) • Password length • Complexity Production system users are authenticated via individually assigned user accounts and passwords. Production system audit logging settings are in place that include: • Account logon events • Account management • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Production system audit logs are maintained and reviewed as needed.
	Application	
		Application user access is restricted via role-based security privileges defined within the access control system. Application administrative access is restricted to user accounts accessible by the following personnel: • CEO • Compliance Counsel • Chief Operating Officer (COO) • Chief Compliance Officer (CCO) • Bank Secrecy Act / Anti-Money Laundering (BSA/AML) Officer • Global Compliance Officer

		The application is configured to enforce password requirements that include: ● Password length ● Complexity Application users are authenticated via individually assigned user accounts and passwords. Application account lockout settings are in place that include: ● Account lockout duration ● Account lockout threshold Application audit policy settings are in place that include: ● Account management ● Payment activity ● Information changes ● API history ● Process tracking ● System events Application audit logs are maintained and reviewed as needed.
	Remote Access	
		VPN user access is restricted via role-based security privileges defined within the access control system. The ability to administer VPN access is restricted to user accounts accessible by the following personnel: ● CTO VPN users are authenticated via unique certificates prior to being granted remote access to the system. The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel. Access into the environment by outside entities requires a valid user ID and password and invalid login attempts are configured to be logged. Data coming into the environment is secured and monitored through the use of firewalls and an IDS. A virtual private cloud (VPC) is in place to isolate outside access and data from the entity's environment. Server certificate-based authentication is used as part of the Transport Layer Security (TLS) encryption with a trusted certificate authority. Stored passwords are encrypted.

		Critical data is stored in encrypted format using software supporting the Advanced Encryption Standard (AES). Encryption keys are protected during generation, storage, use, and destruction. The entity restricts access to its environment using the following mechanisms: ● Classifying data (e.g. Public, private, restricted, etc.) ● Port restrictions (via firewall rule settings) ● Access protocol restrictions (via firewall rule settings) ● User identification Control self-assessments that include logical access reviews are performed on a quarterly basis. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked for an employee as a component of the termination process.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked for an employee as a component of the termination process. Control self-assessments that include logical access reviews are performed on a quarterly basis. Privileged access to sensitive resources is restricted to authorized personnel.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked for an employee as a component of the termination process. Privileged access to sensitive resources is restricted to authorized personnel.

		Control self-assessments that include logical access reviews are performed on a quarterly basis.
	Network (Google Workspace)	
		Google Workspace admin access reviews are completed by management on a quarterly basis. Google Workspace user access is restricted via role-based security privileges defined within the access control system.
	Production System (Application, Web, and Database Servers and Production Databases)	
		Production system admin access reviews are completed by management on a quarterly basis. Production system user access is restricted via role-based security privileges defined within the access control system.
	Application	
		Application admin access reviews are completed by management on a quarterly basis. Application user access is restricted via role-based security privileges defined within the access control system.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction. The entity purges backed up data per a defined schedule. Data that is no longer required for business purposes is rendered unreadable.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network address translation (NAT) functionality is utilized to manage internal IP addresses. VPN, SSL and other encryption technologies are used for defined points of connectivity. VPN users are authenticated via unique certificates prior to being granted remote access to the system. Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority. Transmission of digital output beyond the boundary of the system is encrypted.

CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.	VPN user access is restricted via role-based security privileges defined within the access control system. Logical access to stored data is restricted to authorized personnel. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches. The IDS is configured to notify personnel upon intrusion detection. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations on a weekly basis. Critical data is stored in encrypted format using AES. Logical access to stored data is restricted to authorized personnel. Backed up data is replicated across geographic regions on a daily basis. The entity secures its environment a using multi-layered defense approach that includes firewalls, an IDS and antivirus software. VPN, SSL and other encryption technologies are used for defined points of connectivity. Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority. VPN users are authenticated via unique certificates prior to being granted remote access to the system. A firewall is in place to filter unauthorized inbound network traffic from the internet.

		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Network address translation (NAT) functionality is utilized to manage internal IP addresses. An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches. The IDS is configured to notify personnel upon intrusion detection. Critical data is stored in encrypted format using AES. Backup media is stored in an encrypted format. Transmission of digital output beyond the boundary of the system is encrypted. The ability to migrate changes into the production environment is restricted to authorized and appropriate users. File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. Documented change control policies and procedures are in place to guide personnel in the change management process. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations on a weekly basis.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Management has defined configuration standards in the information security policies and procedures. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. The monitoring software is configured to alert IT personnel when thresholds have been exceeded. An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches. The IDS is configured to notify personnel upon intrusion detection. File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. Vulnerability scans are performed monthly on the environment to identify control gaps and vulnerabilities.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity’s ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.

		The monitoring software is configured to alert IT personnel when thresholds have been exceeded. An IDS is utilized to analyze network events and report possible or actual network security breaches.
		The IDS is configured to notify personnel upon intrusion detection. FIM software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations on a weekly basis.
	Network (Google Workspace)	
		Google Workspace account recovery occurs through multi-factor authentication and security question verification. Google Workspace audit logging settings are in place that include: ● Admin ● Calendar ● Drive ● Login ● Devices ● Token ● Groups ● SAML ● Google Chat ● Currents ● Voice ● Google Meet ● Users Accounts ● LDAP ● Data Studio

		• Groups Enterprise • Chrome Google Workspace audit logs are maintained and reviewed as needed.
	Production System (Application, Web, and Database Servers and Production Databases)	
		Production system audit logging settings are in place that include: • Account logon events • Account management • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Production system audit logs are maintained and reviewed as needed.
	Application	
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Application account lockout settings are in place that include: • Account lockout duration • Account lockout threshold Application audit policy settings are in place that include: • Account management • Payment activity • Information changes • API history • Process tracking • System events Application audit logs are maintained and reviewed as needed. Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. The incident response and escalation procedures are reviewed at least annually for effectiveness. The incident response policy define the classification of incidents based on its severity. Resolution of incidents are documented within the ticket and communicated to affected users. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.

		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. Identified incidents are reviewed, monitored and investigated by an incident response team.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users. Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach. Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented. Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. Resolution of incidents are documented within the ticket and communicated to affected users. Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents. Critical security incidents that result in a service/business operation disruption are communicated to those affected through mass notifications. Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach. A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. The incident response and escalation procedures are reviewed at least annually for effectiveness.

CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Change management requests are opened for incidents that require permanent fixes.
		The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: ● Rebuilding systems ● Updating software ● Installing patches ● Removing unauthorized access ● Changing configurations Data backup and restore procedures are in place to guide personnel in performing backup activities. Control self-assessments that include backup restoration tests are performed on at least an annual basis. A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. A business continuity and disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. The disaster recovery plan is tested on an annual basis. The business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Change Management		
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Documented change control policies and procedures are in place to guide personnel in the change management process. The change management process has defined the following roles and assignments: ● Authorization of change requests - IT Manager ● Development - product specialists ● Testing - product specialists ● Implementation - IT Manager System changes are communicated to both affected internal and external users. Access to implement changes in the production environment is restricted to authorized IT personnel. System changes are authorized and approved by management prior to implementation. Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed. Development and test environments are logically separated from the production environment. Developers do not have access to implement changes to the production environment. Changes implemented into the production environment trigger an alert to affected users. System change requests are documented and tracked in a ticketing system. FIM software is in place to ensure only authorized changes are deployed into the production environment. Back out procedures are documented within each change implementation to allow for rollback of changes when changes impair system operation. System changes are tested prior to implementation. Types of testing performed depend on the nature of the change. Change management requests are opened for incidents that require permanent fixes.

		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Mitigation		
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Documented policies and procedures are in place to guide personnel when performing a risk assessment. Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. Identified risks are rated using a risk evaluation process and ratings are approved by management. Risks identified as a part of the risk assessment process are addressed using one of the following strategies: ● Avoid the risk ● Mitigate the risk ● Transfer the risk ● Accept the risk Management develops risk mitigation strategies to address risks identified during the risk assessment process. The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances. Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process. Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.

		The entity's third-party agreement outlines and communicates: ● The scope of services ● Roles and responsibilities ● Terms of the business relationship ● Communication protocols ● Compliance requirements ● Service levels ● Just cause for terminating the relationship
		Management obtains and reviews attestation reports of critical vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment. A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements. Management has assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY		
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. The monitoring software is configured to alert IT personnel when thresholds have been exceeded. Processing capacity is monitored 24x7x365. Future processing demand is forecasted and compared to scheduled capacity on an annual basis.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Full backups of production data are performed on a daily basis. When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure. Logical access to stored data is restricted to authorized personnel. Backed up data is replicated across geographic regions on a daily basis. Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice

		Organizations section above for controls managed by the subservice organization.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A business continuity and disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. The business continuity plan is tested on an annual basis and includes: ● Various testing scenarios based on threat likelihood ● Identifying the critical systems required for business operations ● Assigning roles and responsibilities in the event of a disaster and ● Assessing and mitigating risks identified as a result of the test disaster Control self-assessments that include backup restoration tests are performed on at least an annual basis.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY		
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**
C1.1	The entity identifies and maintains confidential information to meet the entity’s objectives related to confidentiality.	Documented confidential policies and procedures are in place that include the following: ● Defining, identifying and designating information as confidential ● Storing confidential information ● Protecting confidential information from erasure or destruction ● Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed Confidential information is maintained in locations restricted to those authorized to access. Confidential information is protected from erasure or destruction during the specified retention period.
C1.2	The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.	Documented data destruction policies and procedures are in place that include the following: ● Identifying confidential information requiring destruction when the end of the retention period is reached ● Erasing or destroying confidential information that has been identified for destruction The entity purges backed up data per a defined schedule.

		The entity purges data stored on backup tapes and backup drives when requested by a user or data subject.

INDEPENDENT CONSULTANT’S REPORT

Scope

We have examined the staking node operations accompanying description of the Casper Staking System as of July 3, 2021 (description) based on the criteria for a description of a service organization’s system in DC section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design of controls stated in the description as of May 31, 2021, to provide reasonable assurance that the staking 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*).

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at the entity, to achieve the entity’s service commitments and system requirements based on the applicable trust services criteria. The description presents the entity’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the 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 consultant’s Responsibilities

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

Inherent Limitations

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

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

a. The description presents the Casper Staking Framework that was designed and implemented as of July 3, 2021, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of July 3, 2021, to provide reasonable assurance that entity service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of the controls as of that date.

Restricted Use

This report is intended solely for the information and use of the staking node operators, user entities as of July 26, 2021, business partners of the entity are subject to risks arising from interactions with the staking services, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

Puerto Rico
July 26, 2021