EnCirca

THE DOMAIN NAME REGISTRATION SERVICES

SOC 3 REPORT

*Independent Service Auditor's Report
On a Service Organization's Description of
Its System and the Suitability of the Design
and Operating Effectiveness of Its Controls
Relevant to Security, Availability, and
Confidentiality*

For the Period March 1, 2023 to February 29, 2024

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations
TM

INDEPENDENT SERVICE AUDITOR'S REPORT

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of EnCirca, Inc.,

Scope

We have examined EnCirca, Inc.'s (EnCirca) accompanying management's assertion found in Section 2 titled "Management Assertion of EnCirca" (assertion) that the description of its domain name registration services and systems (system) were effective throughout the period March 1, 2023 to February 29, 2024, to provide reasonable assurance that EnCirca's principal 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*).

EnCirca uses a third-party data center (subservice organization) to house its critical production computer servers, applications and networking equipment. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at EnCirca, to achieve EnCirca's service commitments and system requirements based on the applicable trust services criteria. The description presents EnCirca 's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of EnCirca's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on 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, in all material respects, management's assertion is fairly stated. 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 risk that controls were not effective to achieve EnCirca's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve EnCirca'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.

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

Inherent Limitations

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organizations' 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 EnCirca's domain name registration services were effective throughout the period March 1, 2023 to February 29, 2024 to provide reasonable assurance that EnCirca's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of EnCirca's controls were effective throughout that period.

The Moore Group CPA, LLC

Nashua, NH
March 29, 2024

SECTION 2

MANAGEMENT ASSERTION OF ENCIRCA

EnCirca

MANAGEMENT ASSERTION OF ENCIRCA

March 29, 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within EnCirca, Inc.'s (EnCirca) domain name registration services and systems (system) throughout the period March 1, 2023 to February 29, 2024 to provide reasonable assurance that EnCirca's service commitments and system requirements relevant to security, availability, and confidentiality (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented in Section 3 titled "Description of the Service Organization's System Provided by EnCirca Management" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period [date] to [date], to provide reasonable assurance that EnCirca'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). EnCirca's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements related to the applicable trust services criteria presented in Section 3.

EnCirca uses a third-party data center (subservice organization) to house its critical production computer servers, applications and networking equipment. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at EnCirca, to achieve EnCirca's service commitments and system requirements based on the applicable trust services criteria. The description presents EnCirca's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of EnCirca's controls. The description does not disclose the actual controls at the subservice organization.

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

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

We assert that the controls within the system were effective throughout the period March 1, 2023 to February 29, 2024 to provide reasonable assurance that EnCirca's service commitments and system requirements were achieved based on the applicable trust services criteria.

SECTION 3

DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM PROVIDED BY ENCIRCA MANAGEMENT

OVERVIEW OF OPERATIONS

Company Background

Founded in 2001 near Boston, Massachusetts by Thomas Barrett, EnCirca, Inc. (EnCirca) is an ICANN-Accredited domain name Registrar and a Trademark Agent for the Trademark Clearinghouse. EnCirca supports hundreds of generic top-level-domains and country-code top-level-domains with a specialty on securely managing domains and websites in restricted top-level-registries, such as: .BANK, .BOT, .COOP, .CPA, .INSURANCE, .PHARMACY, .REALTOR, and .JOBS. EnCirca also provides registrant validation services for domain name registries, including: .BANK, .CPA , .INSURANCE among others and partners with trade associations, such as serving as a Preferred Service Provider for the Independent Community Bankers of America.

EnCirca's customer-facing platform integrates domain name portfolios with add-on services such as: Secure DNS hosting, Secure website and email hosting, SSL digital certificates and DMARC authentication and reporting.

For scalability, security and reliability, EnCirca's technical infrastructure is based in Amazon's AWS Cloud and is integrated with the Packet Clearing House's Anycast network.

Scope of SOC Audit

The scope of this SOC audit includes an assessment of the general organizational and information technology controls supporting the domain name registration services and systems of EnCirca. The scope does not include an assessment of any banking, fraud protection, cash receipts/payments, accounting, or other internal or external financial responsibilities of EnCirca.

Description of Services Provided

EnCirca offers its customers value-add services which include:

- **SSL** – EnCirca clients can protect their domain names by purchasing and installing an SSL certificate. There are several different types of certificates available:
    - Standard SSL Certificates - require the certificate issuer to independently verify the information concerning the applicant's business.
    - Extended Validated (EV) Certificates - the applicant's business credentials are validated more extensively to help ensure that the applicant isn't a phisher, spoofer, or other type of online criminal.
    - Wildcard Certificates - protect multiple options of the same base domain (i.e. www.sample.bank and directory.sample.bank)
    - SAN Certificates - protect multiple, different domains (i.e. www.sample.bank and sample.com)
- **SecureDNS** – EnCirca's new DNS service is ISO 27001-certified and provides the "Carrier-Grade" technical stability, performance and high-availability demanded by banks today. A highly redundant and scalable Anycast network helps fight against Distributed Denial of Service (DDOS) attacks. The service also includes enhanced security tools to help banks fight phishing and other email-related fraud.

- **DMARC** – EnCirca was the first registrar to offer affordable email authentication services using DMARC. Domain-based Message Authentication, Reporting and Conformance (DMARC) is a requirement that involves the email addresses used by a business to send out email. DMARC is a way to determine whether or not a given message is legitimately from the sender, and what to do if it isn't. This makes it easier to identify spam and phishing messages, and keep them out of customers' inboxes.

- **Secure Website and Email Hosting** – Cybersecurity is an ever-growing concern for all businesses, but especially banks and credit unions. EnCirca offers website and email hosting with enhanced security features to protect against cyberattacks.

- **Search Engine Optimization (SEO)** – SEO is the process of positioning a website to rank highly on search results pages for the most relevant keyword searches. The entire process is tracked in EnCirca's SEO reporting tool, and reports can be automatically sent to clients.

- **Trademark Clearinghouse** – EnCirca is a Trademark Agent for the Trademark Clearinghouse (TMCH). The TMHC was created by ICANN as a repository for new Rights Protection Mechanisms covering new Top-Level-Domains (TLD's). All new TLD's will be required to use the TMCH for Trademark Claims and Sunrise Periods. The first phase of ICANN's new TLD program contains 1,300 unique strings. Eligibility in the TMCH is limited to active registered trademarks from a national or multi-national jurisdiction. Also covered are trademarks validated by a court order or treaty.

Principal Service Commitments and System Requirements

EnCirca makes service commitments to its customers and has established system requirements as part of the domain name registration services. Some of these commitments are principal to the performance of the service and relate to the applicable trust services criteria. EnCirca 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 EnCirca's service commitments and system requirements are achieved.

Service commitments to customers are documented and communicated in EnCirca's policies and procedures, system design documentation, customer agreements, or other written company materials provided to user entities as well as in the description of the service offering provided online. Service commitments include, but are not limited to, the following:

- Security: EnCirca has made commitments related to a secure information technology control environment and complying with relevant laws and regulations. These commitments are addressed through measures including data encryption, authentication mechanisms, physical security, and other relevant security controls.

- Availability: EnCirca has made commitments related to providing reliable and consistent uptime and connectivity for the IT systems used in the services offered by EnCirca. These commitments include, but are not limited to, design, development or acquisition, implementation, monitoring, and maintaining environmental protection of systems, software, data back-up processes, and recovery infrastructure to meet availability commitments.

- Confidentiality: EnCirca has made commitments related to maintaining the confidentiality of customers' data through data classification policies, data encryption and other relevant security controls.

EnCirca has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in its system policies and procedures, system design documentation, and customer agreements. 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 contractors are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of various EnCirca services.

Components of the System

<u>System Boundaries</u>
A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the description of services and the components of infrastructure, software, people, procedures, and data.

The components of the system used to provide the services are as follows:

Infrastructure

Subservice Organization - For colocation of critical production servers and systems, EnCirca utilizes a secure third-party data center, Amazon Web Services (AWS). AWS had a SOC 2 audit for the review period October 1, 2022 to September 30, 2023. The scope of this audit does not include the controls of AWS.

AWS is considered world-class data center with state-of-the-art systems for ensuring high availability, reliability, and protection against Distributed-Denial-Of-Service (DDOS) attacks and known vulnerabilities for unauthorized access.

The cloud environment infrastructure has redundancy at all levels. Redundant layers at the edge (routers and firewalls), redundant at the core (switching), redundancy within the hosts, and redundant backend storage. Redundant architecture exists such that data is replicated in real-time to at least two geographically dispersed data centers. The data centers are connected through multiple encrypted network links and interfaces.

Critical web servers are in Amazon's EC2 (Elastic Compute Cloud) environment and utilize its Elastic Load Balancer (ELB) offering. The system is highly scalable, and exists in multiple availability zones (AZs) for geographical redundancy. The server instances are in their own VPC (Virtual Private Cloud) such that they are logically isolated from other virtual networks in the AWS cloud.

The server and network hardware layer is managed by Amazon. The Virtual Private Cloud network (i.e.: logical administrative access to creating/moving production servers) is managed by EnCirca via IAM (Identity and Access Management). Internal EnCirca administrative access to servers is made via Linux shell/root authentication using SSH keys.

Software

Software consists of the programs and software that support the applications within the scope of the description. The list of software and ancillary software used to build, support, secure, maintain, and monitor the domain name registration services includes the following applications, as shown in the table below:

Component	Description
Hosting Systems	AWS Services, Digital Ocean, Gatsby, Netlify, Open-Xchange
Storage, Database, and Backups	AWS RDS (PostgreSQL, MySQL), AWS S3, AWS EFS, MongoDB, Digit al Ocean
Network and Firewall	Iptables, Fail2Ban, Amazon Virtual Private Cloud, Amazon Load Balancer
Build, Release, Continuous Integration Systems, and Change Management	Github, Jira, Gitlab, Jenkins, AWS CodePipeline, Docker Hub
Access Management	AWS IAM, Auth0, Authy, Google Authenticator
Monitoring, Alerting, Analytics, and Ticketing	Jira, Zendesk, Slack, Prometheus & Grafana, Cloudwatch
Vulnerability Scanning	AWS Inspector, Qualys, HostedScan Security
Human Resource	Intuit, Upwork, Wise, Payoneer, Remitly

People

EnCirca is led by its President, Thomas Barrett, and executives in the departmental areas of Professional Services, Development, and Sales and Marketing. EnCirca's organizational structure provides the overall framework for planning, directing, and controlling operations. Personnel and business functions are separated into departments according to job responsibilities. The structure provides defined responsibilities and lines of authority for reporting and communication. The assignment of roles and responsibilities within the various departments provides effective segregation of duties.

In the Control Environment section of this report beginning on Page 13, additional information is described related to organizational controls implemented at EnCirca. These organizational controls are intended to serve as the internal foundation for providing services to its customers.

Procedures

EnCirca has implemented processes and procedures to support the operations and controls over the services and systems provided to its customers. Specific examples of the relevant procedures include, but are not limited to, the following:

- Policies and procedures are in place to guide personnel regarding assessing risks on a periodic basis.
- Security policies are in place to guide personnel regarding physical and information security practices.
- Policies and procedures are in place for identifying the system security requirements of authorized users.
- Third-party enterprise monitoring applications are used to monitor and record performance criteria for critical EnCirca server and network equipment.
- System downtime and operations issues are monitored to help ensure that system downtime does not exceed predefined levels.
- An Incident Response plan is in place to ensure appropriate response to outages or security incidents in an organized and timely manner, and properly document them.
- Policies and procedures are in place to guide personnel regarding addressing how complaints and requests relating to security issues are resolved.
- Policies and procedures are in place to assign responsibility and accountability for system changes and maintenance.
- Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.
- Management utilizes intrusion prevention systems (IPS) to prevent unauthorized intrusion into the production environment.
- Firewall systems are in place to handle data flow between external parties and the EnCirca network. All external traffic intended for the EnCirca production environment must pass through a firewall system to communicate with the EnCirca servers.
- Policies and procedures are in place to add new users, modify the access levels of existing users, and remove users who no longer need access.
- Processes and procedures are in place to identify and authenticate users. Unique user security keys are used to authenticate users within the computing environment.
- Physical security policies and procedures are in place to guide personnel regarding restricting access to the facility.
- Management periodically performs internal security assessments, including reviews of server logs and other critical items.
- Policies and procedures are in place to ensure that design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.
- Policies and procedures are in place to ensure that change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by EnCirca and typically includes the following defined categories:

- PUBLIC – pertains to all data that does not require specific accountability and/or audit trails for use. The unauthorized disclosure of this data would not cause any adverse impact to EnCirca's reputation, financials, or client engagements. Such information includes non-strategic information, publicly available information, or non-specific application information.

- INTERNAL – pertains to all information created by an individual user of the internal system and not meant to be generally shared with others. The unauthorized disclosure of this information reasonably could be expected to cause low substantive damage to EnCirca's reputation, financials, or client relations. Such information and communication of it is intended by the creator for a specific audience only.

- INTERNAL SENSITIVE – pertains to all data having compromising or competitive elements or implications intended strictly for use within EnCirca. Such information includes but is not limited to basic financial, security, and audit information.

- CONFIDENTIAL – pertains to all data of the highest sensitivity due to its time and financial sensitivity or possible fraud potential. Such data includes all types of identifiable information, social security numbers, health records, account numbers, payroll, personal information, passwords, code, client relations/engagements, and contracts under negotiation.

Access to data is limited to authorized personnel in accordance with EnCirca's system security policies. EnCirca is also responsible for the overall availability of data, including system backups, monitoring of data processing, and file transmissions as well as identifying and resolving problems.

Encryption is utilized to protect data in transit, including SSL encryption over HTTPS connections utilized for secure communications between EnCirca and customer end users.

Controls in place specific to the data responsibilities of EnCirca include, but are not limited to, the following:

- *Contractors (1099)* must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.
- Firewall systems are in place to handle data flow between external parties and the EnCirca network. All external traffic intended for the EnCirca production environment must pass through a firewall system to communicate with the EnCirca servers.
- Policies and procedures are in place to guide personnel regarding sharing information with third parties.
- Communication sessions between EnCirca's servers/applications and external parties are secured using various encryption methods when applicable.
- External and internal servers and network devices that need access to internal resources are configured with industry standard SSL-encrypted tunnels to protect their connection.
- Transaction processing performed on web-based applications is secured through the use of the Secure Socket Layer (SSL) encryption protocol over HTTPS connections.

Disaster Recovery

EnCirca maintains a current Disaster Recovery Plan and Business Continuity plan. Disaster and business continuity emergency situations are ultimately managed through proper planning (crisis management, recovery and continuity) and response. Identified risks have been mitigated through prevention, minimization or rapid recovery resources and planning. EnCirca's disaster recovery and business continuity program helps to ensure that disruptive incidents are responded to quickly and effectively.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of EnCirca's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior is the product of EnCirca's ethical and behavioral standards, how they are communicated, and how they are reinforced in daily practice.

These standards include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, and by personal example.

Specific control activities that EnCirca has implemented in this area are described below.

- *Contractors (1099)* must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.

Commitment to Competence

EnCirca's management defines competence as the knowledge and skills necessary to accomplish tasks that define contractor's roles and responsibilities. EnCirca's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

Specific control activities that EnCirca has implemented in this area are described below.

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements that delineate contractor responsibilities and authority.

- Roles and responsibilities for company personnel to interact with and monitor the activities of external third-party information technology vendors are defined in written job descriptions and communicated to personnel.

- Each contractor's performance is reviewed annually before making the decision on whether or not to renew their contract. Contracts can also be terminated with a 30-day written notice if performance is not acceptable.

Board of Directors' Participation

EnCirca's control consciousness is influenced significantly by its Board of Directors participation. The Board of Directors oversees management activities and meets annually to discuss strategic, operational, and compliance issues.

Management's Philosophy and Operating Style

EnCirca's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring

business risks and management's attitudes toward the domain name registration services, information processing, accounting functions and personnel. Management is periodically briefed on regulatory and industry changes affecting services provided. Management meetings are held on a periodic basis to discuss and monitor operational issues.

Specific control activities that EnCirca has implemented in this area are described below.

- Each contractor undergoes Security Awareness training annually.

- Management regularly attends trade shows and belongs to industry associations and special interest groups to stay current on regulatory compliance or operational trends affecting the services provided.

- Operational meetings are held on a regular basis to discuss internal control responsibilities *(data and system security)* of individuals and performance measurement.

Organization Structure and Assignment of Authority and Responsibility

EnCirca's organization structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. EnCirca's management believes that establishing a relevant organization structure includes considering key areas of authority and responsibility and appropriate lines of reporting.   EnCirca has developed an organization structure suited to its needs. This organization structure is based, in part, on its size and the nature of its activities.

EnCirca's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring that all personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that EnCirca has implemented in this area are described below.

- EnCirca's organization structure is traditional, with clear lines of authority and responsibility. Autonomy within departments is allowed to a reasonable extent to provide for innovative approaches to managing the company, with close oversight maintained by the CEO.

Human Resource Policies and Practices

EnCirca's human resources policies and practices relate to contractor hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that EnCirca has implemented in this area are described below.

- Each contractor's performance is reviewed annually before making the decision on whether or not to renew their contract. Contracts can also be terminated with a 30-day written notice if performance is not acceptable.

- Management utilizes a termination checklist to ensure that specific elements of the termination process are consistently executed. A copy of the checklist is kept in the contractor file.

END OF REPORT