EnCirca

GENERAL CONTROLS SUPPORTING THE DOMAIN NAME REGISTRATION SERVICES

SOC 3 Audit Report

Independent Service Auditor's Report on Controls Placed in Operation Relevant to Security, Availability, and Confidentiality Principles Comprising Trust Services Principles Section 100

For the Period March 1, 2019 to February 29, 2020

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

INDEPENDENT SERVICE AUDITOR'S REPORT

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR’S REPORT

The Moore Group, CPA
SOC Audit Specialists

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of EnCirca, Inc.,

We have examined the accompanying management's assertion that during the period March 1, 2019 to February 29, 2020, EnCirca, Inc. (EnCirca) maintained effective controls to provide reasonable assurance that the domain name registration services and systems (the "System")

- was protected against unauthorized access, use, or modification;
- was available for operation and use, as committed or agreed;
- protected information designated as confidential as committed or agreed by the organization

based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. EnCirca's management is responsible for this assertion. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of EnCirca's relevant controls over the security, availability, and confidentiality of the System; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

In our opinion, EnCirca's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability and confidentiality.

The Moore Group CPA, LLC

Nashua, NH
April 10, 2020

SECTION 2

ASSERTIONS BY THE SERVICE ORGANIZATION'S MANAGEMENT

EnCirca

MANAGEMENT'S ASSERTION REGARDING THE EFFECTIVENESS OF CONTROLS BASED ON THE TRUST SERVICES PRINCIPLES AND CRITERIA FOR SECURITY, AVAILABILITY, AND CONFIDENTIALITY

April 10, 2020

EnCirca, Inc. (EnCirca) maintained effective controls over the security, availability, and confidentiality of its domain name registration services and systems (the "System") to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification
- the System was available for operation and use, as committed or agreed
- the System protected information designated as confidential as committed or agreed by the organization

during the period March 1, 2019 to February 29, 2020, based on the criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Our attached System Description of the domain name registration services and systems identified the aspects of the EnCirca System covered by our assertion.

EnCirca, Inc.

SECTION 3

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

DESCRIPTION OF CONTROLS PLACED IN OPERATION

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.

System Boundaries

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 five components described below: infrastructure, software, people, procedures and data.

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.

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

Infrastructure

Subservice Organization - EnCirca utilizes the services and controls of Amazon's Web Services (AWS) data centers, for hosting critical production web application servers, development servers and the necessary networking equipment. The AWS data center had SOC 1 Type II, SOC 2 Type II and SOC 3 audits which covered the period April 1, 2019 to September 30, 2019. The scope of this audit does not include the controls of AWS.

AWS is considered world-class data centers 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 highlyscalable, 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

A combination of custom developed and commercial applications are utilized to support the services provided to user organizations. The applications run on Red Hat Linux and enterprise grade server platforms with commercial databases to support the applications.

The applications run on UBUNTU OS platforms with RDS databases to support the applications.

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 from 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 and documenting the system security and availability 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. The IPS subscription for the firewall system is kept current.
- Firewall systems are in place to handle data flow between external parties and the EnCirca network.
- 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

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.

For backups of critical company data, AWS snapshots are taken on a daily basis and retained for at least 7 days.

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:

- Employees 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.
- 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.

- Policies and procedures require that new employees sign an **employee agreement** indicating that they understand their responsibility for adhering to the codes of conduct contained within the agreement. The signed agreement is kept in the employee personnel file.
- Employees must sign a **confidentiality and non-disclosure agreement** to not disclose proprietary or confidential information, including client information, to unauthorized parties.
- Comprehensive **background checks** are performed in-house for certain positions as a component of the hiring process.
- Management personnel perform **reference checks** on all candidates being considered for certain positions within EnCirca.
- *Contract employees (1099)* must sign a **confidentiality and non-disclosure agreement** to not disclose proprietary or confidential information, including client information, to unauthorized parties.
- Comprehensive **background checks** are performed by an independent third party for *contract employees (1099)* as a component of the hiring process.

Commitment to Competence

EnCirca's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' 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 employee 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.
- Management has developed a **training and development program** for employees. This includes:
    - **Initial training** with peers and supervisors in the period immediately after hire.
    - **Ongoing training** to maintain and enhance the skill level of personnel on an as-needed basis.

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.

- 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 employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- Comprehensive **background checks** are performed in-house for certain positions as a component of the hiring process.
- Management personnel perform **reference checks** on all candidates being considered for certain positions within EnCirca.
- Comprehensive **background checks** are performed by an independent third party for *contract employees (1099)* as a component of the hiring process.
- Management has developed a **training and development program** for employees. This includes:
  - **Initial training** with peers and supervisors in the period immediately after hire.
  - **Ongoing training** to maintain and enhance the skill level of personnel on an as-needed basis.
- 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 employee file.

END OF REPORT