caseware™

Caseware Cloud Management

SOC 3® REPORT

REPORTING ON AN EXAMINATION OF CONTROLS AT SERVICE ORGANIZATION RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

Throughout the period July 1, 2021, to June 30, 2022

KOMPLEYE

Office Address
12110 Sunset Hills Road, Suite 600
Reston VA 20190

Mailing Address
9893 Georgetown Pike #186
Great Falls, VA 22066

Telephone: (571)-830-5140

E-mail: info@kompleye.com
Website: www.kompleye.com

Independent Service Auditor's Report

To the Management of Caseware International Inc.

Scope

We have examined Caseware International Inc.'s (Caseware's) accompanying assertion titled "Assertion of Caseware International Inc." (assertion) that the controls within Caseware's Cloud Management system (system) were effective throughout the period July 1, 2021, to June 30, 2022, to provide reasonable assurance that Caseware'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).

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Caseware'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 Caseware's service commitments and system requirements based the applicable trust services criteria

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Caseware's Cloud Management system were effective throughout the period July 1, 2021, to June 30, 2022, to provide reasonable assurance that Caseware's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Kompleye

Patricio Garcia, CPA, CITP, CISA, CDPSE,
ISO 27001 LA, HITRUST CCSFP.
Partner
Kompleye ATT
Great Falls, VA
August 5, 2022

CASEWARE INTERNATIONAL INC'S ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within Caseware Inc.'s (Caseware's) Cloud Management System throughout the period July 1, 2021, to June 30, 2022, to provide reasonable assurance that Caseware's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in attachment A 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 July 1, 2021, to June 30, 2022, to provide reasonable assurance that Caseware'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). Caseware's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

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 July 1, 2021, to June 30, 2022, to provide reasonable assurance that Caseware's service commitments and system requirements were achieved based on the applicable trust services criteria.

DocuSigned by:
David Osborne
B3C94EABE00442C...

David Osborne, CEO
Caseware International Inc.

Attachment A

COMPANY OVERVIEW

Caseware International Inc. ("Caseware") is a software development company founded in 1988. We provide industry leading solutions for assurance and risk management that enable accountants and auditors to collaboratively work and manage their financial data, reports, and statements from a single platform.

Our solutions streamline processes through automation and enable customers to tailor the platform to meet their business and client needs, both large and small.

CASEWARE CLOUD

One of Caseware's solutions is Caseware Cloud ("**CWC**"). The CWC platform delivers next-level innovation by providing customers secure hosting services in addition to our core offerings for accountants and auditors. With CWC, customers can manage all their data online and leverage additional analytic and machine learning services to enhance business value.

INFRASTRUCTURE

CWC is a software as a service (SaaS) offering that is completely virtual and hosted on the Amazon Web Services ("**AWS**", or "**Amazon**") with locations in the United States, Australia, Canada, and the European Union ("**EU**").

The scope of locations includes:

- Amazon US (Datacenter)
- Amazon Ireland (Datacenter)
- Amazon Australia (Datacenter)
- Amazon Canada (Datacenter)

Customers access the software through the web portal. The Operations Team manages the infrastructure through AWS management tools (including but not limited to web console, API, CLI, cloudformation, terraform etc.), and a Privileged Access Management (PAM) system (which is implemented by StrongDM, VPN, AzureAD etc).

The CWC platform consists of the following:

- Caseware Cloud
- Caseware Hybrid Cloud
- Caseware Sherlock
- Caseware SE

SOFTWARE

Our software engineers innovate, enhance and maintain cloud based software that power Caseware Clouds platform and product base. We provide products and services to our customers, while

maintaining a strong network of distributors, resellers, trainers, and implementation specialists though long standing, and well established relationships.

Customers are provided with an administrative console to manage user credentials in CWC. An administrative account is created during client onboarding for the client to manage user accounts within their firm.

PEOPLE

Caseware is led by the Executive Leadership Team ("**ELT**") that assigns authority and responsibility to Senior Leadership ("**Management**") or, People Leaders ("**Managers**"), and teams with the skills and experience necessary to carry out their functions and assignments. Assignments are aligned with achieving information security objectives, corporate objectives, oversight of operations functions, and compliance with applicable regulatory requirements.

DATA

All traffic to CWC is encrypted, with advanced proxy services to provide high availability and high-speed operation, monitor for security threats, and protect against malicious traffic.

CWC also relies on the Amazon Web Services security policies and their accreditations, which are a key element to protecting sensitive information. Data that is transferred to and from CWC (data-in-transit) is encrypted via TLS with ephemeral key exchange and use industry-accepted strong cipher suites. Certificates use a minimum of 2048-bit key strength with SHA-2 or stronger signature algorithm.

Storage of data (data-at-rest) is encrypted at the server level using the industry-standard AES-256-GCM algorithm. Client data is held in one of Amazon's secure data centers for each region. Data is not permitted to leave the region without client consent.

Customers maintain ownership of their data. CWC may use Personal Information provided by its users in an anonymous, and/or aggregated fashion to improve or enhance its Cloud Services and other service offerings. Caseware does not otherwise access or use customer content for any purpose other than as legally required, for maintaining CWC services and providing service to our customers and their end-users. We never use customer content or derive information from it for marketing or advertising without explicit customer consent, other than for non-identifiable aggregated statistics.

Controls are in place to limit Caseware team members accessing user data, other than when requested by firms for customer support purposes including incident resolution. Caseware goes to great lengths to ensure users outside of the firm and its contacts do not have any access to the firm.

Amazon AWS Storage Technologies are used for both CWC's archive feature and regular backups. Backups, including all user data and system logs, are taken daily and are available for restores on firm requests for 90 days.

PROCESSES & PROCEDURES

Caseware has implemented an Information Security Program based on the ISO/IEC 27001 Information Security Management System. Policies and procedures are reviewed annually and approved by appropriate stakeholders including Management and the ELT. The policies and procedures cover the following key security areas:

- Access Control
- Availability Management
- Clean Desk
- Cryptography
- Software Development
- Release Management
- Password Management
- Logging and Monitoring
- Patch Management
- Network Security
- Mobile Device
- Technical Vulnerability Management
- Vendor Management
- Disaster Recovery and Business Continuity
- Remote Working

Attachment B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Caseware communicates its service commitments for CWC to customers in the form of a Service Level Agreement ("**SLA**"), customer agreements and/or through the description of the service offerings provided online through Caseware's external website.

Caseware has also implemented various methods of external communication to support its customer/subscriber base. Mechanisms are in place to allow Caseware's Customer Support Team to be notified and to notify customers of potential operational issues that could impact CWC services. A real-time operational status page is available and maintained by Caseware's Cloud Operations Team (the "**Operations Team**") to alert customers of issues that may be of broad impact. Current status information can be checked by the customer on this site. Details related to security and compliance of CWC can also be viewed in the frequently asked questions section of Caseware's external website.

Caseware Customer Support Services include:

- Technical support via telephone, email or web to answer queries concerning the use, operation or business functionality of CWC, including access to Local Distributors;
- Error analysis and correction;
- Access to in-line releases, including minor and major new versions of CWC when they become commercially available; and
- Online access to resources and information regarding CWC and its use.

Caseware's SLA sets out what levels of availability and support customers can expect, and aims to enable customers and CWC to work together effectively to resolve issues.