CASEWARE®

SYSTEM AND ORGANIZATION CONTROLS 3 (SOC 3) REPORT

CLOUD MANAGEMENT SYSTEM

FOR THE PERIOD JULY 1, 2019 TO JUNE 30, 2020.

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, 2019, to June 30, 2020, 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, 2019, to June 30, 2020, 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.

Patricio Garcia
Partner
Kompleye ATT
Great Falls, VA
July 23, 2020

1 Toronto St, Suite 1400
Toronto ON Canada, M5C 2V6
Tel: 416-867-9504
Fax: 416-867-1906
www.caseware.com

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, 2019, to June 30, 2020, 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, 2019, to June 30, 2020, 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, 2019, to June 30, 2020, to provide reasonable assurance that CaseWare's service commitments and system requirements were achieved based on the applicable trust services criteria.

CaseWare International, Inc.
Cal Bruner, CFO

Attachment A

COMPANY OVERVIEW

CaseWare International, Inc. 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 International Inc.'s solutions is CaseWare Cloud. The CaseWare Cloud platform is hosted, sold and delivered by CaseWare Cloud Ltd. and delivers next-level innovation by providing customers secure hosting services in addition to our core offerings for accountants and auditors. With CaseWare Cloud, customers can manage all their data online and leverage additional analytic and machine learning services to enhance business value.

INFRASTRUCTURE

CaseWare Cloud Ltd. provides a software as a service offering that is completely virtual and hosted on Amazon web service with locations in the United States, Australia, Canada and EU.

Customers access the software through the web portal. The operations team manages the infrastructure through the AWS console and VPN connection using multi factor authentication.

The following products and services work with CaseWare Cloud and require a separate subscription license:

- Working Papers Desktop
- Analytics

SOFTWARE

CaseWare Cloud is a web application that is developed and maintained by CaseWare International Ltd.'s in-house software engineering group. The software engineering group enhances and maintains the Cloud software to provide services to clients. In order to provide products and services to customers, distributors, resellers, trainers and implementation specialist are in place. CaseWare maintain a strong network and have a long relationship with the distributors, resellers, training and implementation specialists that are all well established.

Clients are provided administrative console to manage user credentials. An administrative account is created during client onboarding for the client to manage user accounts within their firm.

PEOPLE

CaseWare is led by the senior executive team that assigns authority and responsibility to management staff with the skills and experience necessary to carry out their functions and assignments. Assignments are

aligned with achieving corporate objectives, oversight of operations functions, and compliance with applicable regulatory requirements. There is a staff of approximately 400 employees organized in the following functional areas:

- Finance and Accounting
- Industry and Product Strategy
- Cloud Operations
- Product Line Management and Support

The Senior Managers are responsible for determining that their teams are properly staffed with sufficient personnel with the proper competence and capabilities to perform their functions. CaseWare has adopted the ISO 27001 standard as the approach to information security.

CaseWare continues to improve its development models through software and methodology changes.

DATA

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

CaseWare Cloud 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 CaseWare Cloud (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 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. CaseWare Cloud will use information resulting from data to enhance our services and to provide new or improved product offerings. CaseWare does not otherwise access or use customer content for any purpose other than as legally required, and for maintaining CaseWare Cloud 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 the CaseWare Cloud staff accessing user data, other than where requested by firms. CaseWare Cloud goes to great lengths to ensure users outside of the firm and its contacts, do not have any access to the firm. As well, it goes to great lengths to ensure that any data within a firm is visible and editable only by the specific set of users authorized by the firm.

Amazon AWS Storage Technologies are used for both CaseWare Cloud's archive feature and regular backups.

PROCESSES & PROCEDURES

Management has implemented an Information Security Management System based on the ISO 27001 standard to restrict logical access to CaseWare Cloud. Changes to these procedures are performed annually and authorized by senior management. The procedures cover the following key security life cycle areas:

- Software Development

- Release Management
- Access Control
- Password Management
- Logging and Monitoring
- Patch Management
- Network Security
- Cryptography
- Technical Vulnerability Management
- IS Supplier Management
- Disaster recovery and business continuity

Attachment B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

CaseWare Cloud communicates service commitments to user entities (CWC customers) in the form of Service Level Agreements (SLAs), customer agreements, contracts or through the description of the service offerings provided online through the CaseWare website.

At the subscriber level, CWC has also implemented various methods of external communication to support its customer base. Mechanisms are in place to allow the 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 the Cloud 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 CaseWare Cloud can also be viewed in the frequently asked questions section of the CaseWare website.

Support Services (available Monday to Friday, except January 1st and December 25th):

- Technical support via telephone, email or web
- Error analysis and correction
- Access to in-line releases (minor and major versions)
- Online access to resources regarding the CaseWare Cloud Services and its use

Requests for support are handled through the local Distributor channel.