



Caseware Cloud Platform

SOC 3® REPORT

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

*Throughout the period July 1, 2022, to August 31,
2023*





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 Platform system (system) were effective throughout the period July 1, 2022, to August 31, 2023, 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.

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 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 Platform system were effective throughout the period July 1, 2022, to August 31, 2023, 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, CMMC-CCP**

Partner

**Kompleye ATT
Great Falls, VA
October 31, 2023**



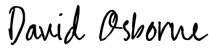
CASEWARE INTERNATIONAL INC'S ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within Caseware Inc.'s (Caseware's) Cloud Platform System throughout the period July 1, 2022, to August 31, 2023, 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, 2022, to August 31, 2023, 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, 2022, to August 31, 2023, to provide reasonable assurance that Caseware's service commitments and system requirements were achieved based on the applicable trust services criteria.

DocuSigned by:

B3C94EABE00442C...

David Osborne
CEO
Caseware International Inc.

Attachment A

COMPANY OVERVIEW

Caseware International Inc. (“Caseware Cloud Ltd.” or “Caseware”) is a leading supplier of software solutions to accountants and auditors worldwide. Founded in Toronto in 1988, Caseware provides mission-critical accounting and auditing software used by domestic and global accounting firms and is a leading provider of auditing software to governments, tax authorities and corporations.

Our customers use Caseware products to prepare, review and audit financial statements, manage client engagements, conduct detailed audit and fraud detection tests, track time, billing and support the overall lifecycle of practice management. 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

The Caseware Cloud (“CWC”) platform delivers next-level innovation by providing customers secure hosting services in addition to our core offerings for accountants and auditors. CWC offers numerous global and localized engagement applications, helping you manage practice and service functions with greater agility.

With CWC, customers can manage all their data online and leverage additional analytic and machine learning services to enhance business value. CWC boasts over 150 cloud applications and tools, along with seamless integration with other Caseware platforms like Caseware Working Papers and IDEA, as well as other external architectures. CWC platform features and integrations include:

- **Caseware Smart Engagement:** Caseware's Smart Engagement technology powers our Cloud Apps such as Agile Audit, SMSF Audit and Cloud Financials.
- **Caseware Sherlock:** Sherlock fully automates the process of extracting data from your engagements, loading it into a centralized database and transforming it into a format that allows you to easily analyze data from all engagements for business insights.
- **Caseware Hybrid Cloud:** Caseware Hybrid Cloud is what we call the integration of CWC products with Caseware Working Papers. In this 'hybrid' environment, your organization can benefit from the familiarity of Working Papers, while including the advancements and accessibility that Cloud brings.

INFRASTRUCTURE

CWC is a software as a service (SaaS) offering that is completely virtual and hosted on Amazon Web Services (“AWS”, or “Amazon”) with data center locations in the United States (“US”), Australia, Canada, and Ireland/European Union (“EU”). Upon subscribing to Caseware Cloud services, clients are informed of the jurisdiction in which the server that has been allocated to host your subscriber data and personal information is located. You may consent to such allocation, or refuse a server so allocated.

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

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 through long standing, and well-established relationships.

The following is utilized to support CWC’s service commitments to customers, and ensure secure cloud operations:



Application	Purpose
AWS Components including GuardDuty	AWS hosted databases, machine images, storage, and other AWS native tools used for development, testing, and system security.
GitHub	Software development and version control.
Bitbucket Cloud	A Git based code hosting and collaboration tool.
Jira	Managing development and deployment of changes to the CWC source code.
CrowdStrike	Endpoint Detection and Response (EDR)/antivirus and anti-malware protection for production environments.
New Relic	Monitoring performance and availability.
StrongDM	Auditing, access controls and securing communications to infrastructure.
PagerDuty	Incident management platform that provides reliable notifications, automatic escalations and on-call scheduling.
TTN	TTN monitors CWC production (no direct access/Admin) and provides 24x7 incident coordination support to ensure continued system availability to our clients.

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 (refer to Caseware’s Cloud Privacy Policy on MyCaseware, for EU customers the Data Processing Agreement is made available) or provided with the Master Services Agreement. 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 and monitor Caseware team members accessing user data (limited to Cloud Operations/AWS Admins). Backup restore may be required for incident resolution, or requested by firms for customer support purposes, for which a customer identity validation and sign-off process exists. 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 27001:2013 Information Security Management System. Policies and procedures are reviewed at least annually or after significant changes 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/Encryption
- Software Development
- Release Management
- Password Management
- Logging and Monitoring
- Patch Management
- Network Security
- Mobile Device
- 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 through the [Caseware Master Product & Services Agreement](#) (“MPSA”), which includes the Service-Level Commitments (“SLA”) and terms of use; and through the description of the online [CWC service offerings](#). Caseware’s MPSA sets out what levels of availability and support customers can expect and aims to enable customers and Caseware to work together effectively to resolve issues. Caseware will make the Services available 99.9% of the time, as calculated in a calendar month on a 24 hour/7-day basis (please refer to the SLA for exclusions).

Caseware has implemented various methods of external communication to support its customer/subscriber base, including:

- [Caseware Cloud Status](#) - A real-time operational CWC 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. The page includes scheduled maintenance notifications across different regions. Customers can subscribe to CWC system operation email notifications through this page to be notified when Caseware creates, updates, or resolves an incident.
- [Caseware’s Customer Support Team](#) - 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. 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 Security Certifications page](#) - Compliance page evidencing certifications, and frequently asked questions pertaining to CWC’s compliance, security, availability, confidentiality, and data/privacy.
- [MyCaseware](#), annual compliance reporting - Through MyCaseware, or as requested (through their account manager), customers who have signed Caseware’s Mutual Non-Disclosure Agreement (“MNDAs”), are provided Caseware’s compliance package as reports are made available. This includes an annual pen test report, SOC 2 Type 2 report, and ISO 27001 certification.

