



System and Organization Controls (SOC) 3 Report
Management's Report of Its Assertions on YuJa Inc.'s
Ed-Tech Product Portfolio System Based
On the Trust Services Criteria for Security

For the Period June 1, 2021 to May 31, 2022





TABLE OF CONTENTS

Section 1	Report of Independent Accountants	1
Section 2	Management’s Report of Its Assertions on the Effectiveness of Its Controls over YuJa Inc.’s Ed-Tech Product Portfolio System Based on the Trust Services Criteria for Security.....	4
	Attachment A: YuJa Inc.’s Description of its Ed-Tech Product Portfolio System	6
	Attachment B: Principal Service Commitments and System Requirements	11



SECTION ONE: REPORT OF INDEPENDENT ACCOUNTANTS

To: Management of YuJa Inc.

Scope

We have examined management’s assertion, contained within the accompanying “Management’s Report of Its Assertions on the Effectiveness of Its Controls over YuJa Inc.’s Ed-Tech Product Portfolio System Based on the Trust Services Criteria for Security” (Assertion) that YuJa Inc.’s controls over the Ed-Tech Product Portfolio System (System) were effective throughout the period June 1, 2021 to May 31, 2022, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the trust services criteria relevant to Security (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*).

The Assertion also indicates that YuJa Inc.’s (“Service Organization” or “YuJa”) controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of YuJa’s infrastructure’s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

YuJa uses a subservice organization to provide cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at YuJa to achieve YuJa’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system 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 suitable design or operating effectiveness of such complementary subservice organization controls.

Service Organization’s Responsibilities

YuJa management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Ed-Tech Product Portfolio System and describing the boundaries of the System;
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of the System; and
- Identifying, designing, implementing, operating, and monitoring effective controls over the Ed-Tech Product Portfolio System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes:

- Obtaining an understanding of YuJa's Ed-Tech Product Portfolio System relevant Security policies, procedures, and controls;
- Testing and evaluating the operating effectiveness of the controls; and
- Performing such other procedures as we considered necessary in the circumstances.

The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating YuJa's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent Limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design and operating effectiveness of the controls to achieve YuJa's Ed-Tech Product Portfolio System's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system of controls, may alter the validity of such evaluations.

Opinion

In our opinion, management's assertion that the controls within YuJa's Ed-Tech Product Portfolio System were effective throughout the period June 1, 2021 to May 31, 2022 to provide reasonable assurance that YuJa's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

CyberGuard Compliance, LLP

June 15, 2022
Las Vegas, Nevada



SECTION TWO: MANAGEMENT’S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER YUJA INC.’S ED-TECH PRODUCT PORTFOLIO SYSTEM BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY

June 15, 2022

Scope

We, as management of YuJa, are responsible for:

- Identifying the YuJa’s Ed-Tech Product Portfolio System (System) and describing the boundaries of the System, which are presented in the section below (Attachment A) titled YuJa Inc.’s Description of its Ed-Tech Product Portfolio System (Description);
- Identifying our principal service commitments and system requirements (Attachment B);
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in the section below (Attachment B)
- Identifying, designing, implementing, operating, and monitoring effective controls over YuJa’s Ed-Tech Product Portfolio System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements; and
- Selecting the trust services categories that are the basis of our assertion.

In designing the controls over the System, we determined that certain trust services criteria can be met only if complementary user entity controls are suitably designed and operating effectively for the period June 1, 2021 to May 31, 2022.

YuJa uses a subservice organization to provide cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at YuJa, to achieve YuJa’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization.

We assert that the controls within the system were effective throughout the period June 1, 2021 to May 31, 2022, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to Security set forth in the AICPA’s TSP section 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy, if subservice organization and user entities applied the

complementary controls assumed in the design of YuJa's Ed-Tech Product Portfolio System controls throughout the period June 1, 2021 to May 31, 2022.

YuJa Inc.

ATTACHMENT A: YUJA INC.'S DESCRIPTION OF ITS ED-TECH PRODUCT PORTFOLIO SYSTEM

System Overview

The System is comprised of the following components:

- **Infrastructure** - The physical and hardware components of a system (facilities, equipment, and networks)
- **Software** - The programs and operating software of a system (systems, applications, and utilities)
- **Data** - The information used and supported by a system (transaction streams, files, databases, and tables)
- **People** - The personnel involved in the operation and use of a system (developers, operators, users, and managers)
- **Procedures** - The automated and manual procedures involved in the operation of a system

Infrastructure

The AWS-hosted Infrastructure Layer is the data center building and the equipment and systems that keep it running. Components like back-up power equipment, the HVAC system, and fire suppression equipment are all part of the Infrastructure Layer. These devices and systems help protect servers and ultimately customer data. In addition to the Infrastructure Layer, the following additional layers comprise the full attested AWS infrastructure deployed by YuJa:

- **Perimeter Layer:** AWS data center physical security begins at the Perimeter Layer. This Layer includes a number of security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures.
- **Data Layer:** The Data Layer is the most critical point of protection because it is the only area that holds customer data. Protection begins by restricting access and maintaining a separation of privilege for each layer. In addition, AWS deploys threat detection devices, video surveillance and system protocols, further safeguarding this layer.
- **Environmental Layer:** The Environmental Layer is dedicated to environmental considerations from site selection and construction to operations and sustainability. AWS carefully chooses their data center locations to mitigate environmental risk, such as flooding, extreme weather, and seismic activity.

Event logging is performed by both the operating systems and the YuJa-designed applications running on AWS, the YuJa Hardware Hub units, and the desktop application software. This logging is primarily used for security and debugging purposes.

Logging is periodically and routinely monitored by YuJa technical staff. Further, in the event of an abnormal situation, the logs are referred to in order to provide additional information when addresses abnormal events and conditions.

Software

System Components

The products offered by YuJa leverage AWS for all its physical production infrastructure.

Software (Systems and Applications)

YuJa design, develops, deploys and maintains all application-level software. The applications run on a mixture of both Linux and Windows operating systems that, in turn, run on AWS-hosted physical instances. The SaaS-based applications are accessible across devices including web-based applications (browsers), tablets and mobile devices. Additionally, the video encoders, officially called YuJa Hardware Hub, are built on a Windows operating system with additional application-level software designed and developed by YuJa.

Data

YuJa stores production data from customers entirely within AWS using the following storage mechanisms:

- Amazon S3 or Amazon Simple Storage Services, a "simple storage service" offered by AWS that provides object storage through a web service interface.
- Amazon RDS or Amazon Relational Database Service, a distributed relational database service by AWS. It is a web service running "in the cloud" designed to simplify the setup, operation, and scaling of a relational database for use in applications.
- Some transient storage is maintained on the YuJa Hardware Hub video encoders while the content is being processed and uploaded to either Amazon S3 or Amazon AWS.

YuJa collects data on behalf of customers as they upload content, use YuJa's or other tools to create content and analyzes stores data for the purpose of analytics. All data is purged once the services contract is cancelled or terminated.

People

YuJa employs only full-time employees to design, development, and maintain their production systems. YuJa does not currently use contractors or temp agencies for any aspects of development and administration of the software.

In terms of data access, only the Chief Technology Officer, Chief Business Officer, and Director of Software Engineering have access to the security keys and system-wide access. Beyond that, specific Senior-level Software Engineers do have access to production systems for the purpose of debugging, maintenance, and performance analysis.

The overall organization supports the framework for an effective control environment. The organization is comprised of the following functional areas:

Executive Management provides strategic direction and leadership for YuJa and all of its domestic and international subsidiaries and affiliates. Executive Management oversees, and is ultimately responsible for, all aspects of service delivery (including business development, marketing, and quality assurance), and all corporate services functions including but not limited to finance, information technology, human resources, legal, real estate and facilities, and corporate development.

Human Resources is responsible for managing all functions related to recruiting and hiring, benefits, employee relations, performance management, training, resource management, and career assistance. The Human Resources team partners proactively with Executive Management and business units to ensure that all initiatives are appropriately aligned with YuJa's mission, vision, and values. Additionally, Human Resources ensures that meaningful, accurate metrics are kept and that YuJa maintains compliance with all federal and state rules and regulations.

Information Technology ("IT") management has overall responsibility and accountability for the enterprise computing environment, including computer hardware, operating systems, network systems, and application development. IT personnel work closely with the end users of other functional areas to develop and implement guidelines and procedures to ensure that the enterprise computing environment is functioning both efficiently and effectively with regard to the Company's business objectives and requirements. IT personnel also support the client service business processes, including the administration of systems supporting key business processes as well as maintaining application patch levels in accordance with vendor recommendations.

Marketing is responsible for the strategic deployment of the YuJa brand and for building awareness through multiple media channels including the internet, public relations, advertising, industry associations, and direct mail. Marketing also supports the business development group through action-oriented targeted marketing initiatives that qualify prospects and drive revenue generation.

Finance Management is primarily responsible for the accuracy of financial reporting and non-client related tax compliance. Finance personnel are responsible for corporate treasury matters, client invoicing and payment applications, payroll, and procurement processing. Finance provides support and assistance as needed to client services.

YuJa is committed to equal opportunity of employment and all employment decisions are based on merit, qualifications, and abilities. Employment-related decisions are not influenced or affected by an employee's race, color, nationality, religion, sex, marital status, family status, sexual orientation, disability, or age. YuJa endorses a work environment free from discrimination, harassment, and sexual harassment.

Procedures

User Reporting

The software provided reporting, both analyzed and raw, to the end-users via administrative, analytics and reporting capabilities.

Data Security Controls

The safe transmission of its customer’s data is of the utmost importance. As such, YuJa employs the following rigorous procedures to its data transmission workflows:

- Data Security — All sensitive user data is transmitted through an encrypted TLS 1.2 channel, which uses 256-bit encryption.
- Data Center Security — YuJa uses AWS as its key data center. To learn more about AWS’ physical and environmental procedures, please review this document on AWS Global Infrastructure (<https://aws.amazon.com/about-aws/global-infrastructure>).
- User Security — Access to YuJa systems that utilizes data stored in its data centers is restricted to authorized and full-time YuJa employees. YuJa does not use external contractors or temp agencies.

Incident Disclosure

No security incidents were detected or reported during the audit period that would affect YuJa’s service commitments or system requirements.

Complementary Subservice Organization Controls

Certain principal service commitments and system requirements can be met only if complementary subservice organization controls (CSOC) assumed in the design of YuJa’s controls are suitably designed and operating effectively at the subservice organizations, along with related controls at YuJa.

Description of Complementary User Entity Controls

YuJa controls were designed with the assumption that certain controls would be implemented by user entities (or “customers”). Certain requirements can be met only if complementary user entity controls assumed in the design of YuJa’s controls are suitably designed and operating effectively, along with related controls at YuJa.

Complementary User Entity Controls

Users are responsible for adhering to all regulatory compliance issues when they are associated with YuJa in a service agreement.

Users are responsible for ensuring user owned or managed applications, platforms, databases, and network devices that may process or store data derived from YuJa are logically secured.

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Company Overview

YuJa is in ed-tech solutions. YuJa's Ed-Tech product portfolio provides organizations of all sizes with the tools to help educate, engage, inspire and collaborate. YuJa serves learning enterprises within all sectors, including higher-ed, K12, government, healthcare, non-profit and corporate.

Locations

YuJa has legal headquarters in Delaware with primary U.S. offices in San Jose, California, and Canadian offices in Toronto, Ontario.

Description of Services Provided

YuJa serves organizations of all sizes, within all sectors, including higher-ed, K-12, government, healthcare, non-profit and corporate delivering products for lecture capture, live streaming, video management, video conferencing, video test proctoring, digital asset management, enterprise accessibility, digital archiving, and student response systems.

The YuJa Enterprise Video Platform is an all-in-one video experience to securely create, manage, discover, collaborate, and live video content across any device, at any time. YuJa Video Conferencing deploy engaging video conferencing solutions for virtual classrooms, webinars, office hours, and tutorials.

YuJa Himalayas for Enterprise Archiving provides tools for enterprises to manage large data workloads in a secure, compliant, and discoverable manner.

YuJa Panorama for Enterprise Accessibility integrates seamlessly into all major Learning Management System (LMS) products to improve the accessibility of digital media and course content.

YuJa Video Conferencing enables institutions too scale online training and education programs.

Lecture Capture portfolio includes desktop-based lecture capture software, hardware capture appliance, in-browser capture tools, and mobile capture applications.

Digital Asset Management Platform enables organizations to get more value from their digital assets such as documents, images, and videos by making them easy to organize, discover and distribute.

Verity for Test Proctoring provides secure video exam proctoring tools along with live and post-test human review.

YuJa Engage is a Student Response System that transforms any course into a more active learning experience for students and allows instructors to gain actionable metrics.

Data Center Operations

YuJa offers its products through an Amazon Web Services (AWS) hosted data center located in a growing set of regions including United States (Oregon and Virginia), Canada (Montreal), and the European Union (Dublin). By leveraging AWS as data center provider, YuJa can leverage AWS' industry-leading expertise in managing data centers and physical computing infrastructure. The AWS infrastructure is attested by the following certifications to be highly stable, fault-tolerant and secure:

- System and Organization Control 1 (SOC 1) reported and published under both the Statement on Standards for Attestation Engagements 18 and the International Standard on Assurance Engagements 3402 (ISAE 3402) standards.
- Certified ISO/IEC 27001:2005 Information Technology.
- Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS).
- Federal Information Security Management Act (FISMA) Moderate Authorization and Accreditation received from the U.S. General Services Administration.

AWS is continuously innovating the design and systems of its data centers to protect them from man-made and natural risks. As a result, the most highly regulated organizations in the world trust AWS every day. AWS System and Organization Control Reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. AWS is also ISO 27001 certified to provide security management that is specified to have comprehensive security controls.

Principal Service Commitments and System Requirements

YuJa's security commitments to customers are documented and communicated to customers in the Master Services Agreement and the description of service document published on the customer-facing website. The principal security commitments include, but are not limited to:

- Perform annual third-party security and compliance audits of the environment, including, but not limited to:
 - Reporting on Controls at a Service Organization Relevant to Security (SOC 2) examinations.
- Use formal HR processes, including background checks, code of conduct and company policy acknowledgements, security awareness training, disciplinary processes, and annual performance reviews.

- Follow formal access management procedures for the request, approval, provisioning, review, and revocation of YuJa personnel with access to any production systems.
- Prevent malware from being introduced to production systems.
- Continuously monitor the production environment for vulnerabilities and malicious traffic.
- Use industry-standard secure encryption methods to protect customer data at rest and in transit.
- Transmit unique login credentials and customer data via encrypted connections.
- Maintain a disaster recovery and business continuity plan to ensure availability of information following an interruption or failure of critical business processes.
- Maintain and adhere to a formal incident management process, including security incident escalation procedures.
- Maintain confidentiality of customer data and notify customers in the event of a data breach.
- Identify, classify, and properly dispose of confidential data when retention period is reached and/or upon notification of customer account cancellation.

YuJa establishes system and operational requirements that support the achievement of the principal service commitments, applicable laws and regulations, and other system requirements. These requirements are communicated in YuJa's policies and procedures, system design documentation, and/or in customer contracts. Information Security policies define how systems and data are protected. These policies are updated as appropriate based on evolving technologies, changes to the security threat landscape, and changes to industry standards, provided any updates do not materially reduce the service commitments or overall service provided to customers as described in the customer contracts.

YuJa regularly reviews the security and performance metrics to ensure these commitments are met. If material changes occur that reduce the level of security commitments within the agreement, YuJa will notify the customer via the YuJa website or directly via email.