System and Organization Controls (SOC) 3 Report

DUX Experts, Inc.'s Description of Its DUX Platform

Relevant to Security

Throughout the Period May 1, 2024 to April 30, 2025

Table of Contents

Independent Service Auditor's Report

To: DUX Experts, Inc. (“DUX” or “the Company”)

Scope

We have examined DUX’s accompanying assertion titled “Assertion of DUX Experts, Inc. Management” (assertion) that the controls within the Company’s DUX Platform were effective throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that DUX’s 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)*.

Service Organization’s Responsibilities

DUX 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 DUX’s service commitments and system requirements were achieved. DUX has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, DUX 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 Company’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 the Company’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 the Company's service commitments and system requirements based on 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 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 DUX's controls over the DUX Platform were effective throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that DUX's service commitments and system requirements were achieved based on the applicable trust services criteria.

Laika Compliance LLC

Arlington, Virginia
May 14, 2025

Assertion of DUX Experts, Inc. Management

We, as management of DUX Experts, Inc., are responsible for:

- Identifying the DUX Platform and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and system requirements that are the objectives of our system, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion.

DUX uses a subservice organization for infrastructure and data hosting services. The boundaries of the System presented in Attachment A includes only the controls of DUX and excludes controls of the subservice organization. However, the description of the boundaries of the system does present the types of controls DUX assumes have been implemented, suitably designed, and operating effectively at the subservice organization. Certain trust services criteria can be met only if the subservice organization controls are suitably designed and operating effectively along with the related controls at DUX. However, we perform monitoring procedures for the subservice organization and based on procedures performed, nothing has been identified that prevents us from achieving our specified service commitments and system requirements.

We assert that the controls over the System were effective throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that DUX's service commitments and system requirements would be achieved based on the criteria relevant to Security set forth in the AICPA's TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Very truly yours,

DUX Experts, Inc.

Attachment A – DUX Platform Overview

SERVICES PROVIDED

DUX Experts, Inc. (“DUX” or “the Company”) is a leading technology company providing an AI-powered platform for virtual inspections across the insurance, construction, and restoration industries. The DUX Platform, a platform designed to streamline inspection workflows by enabling remote inspections, automating image and data analysis, and generating loss scopes, construction inspection reports and estimates. The system supports field and desk adjusters, inspectors, contractors, and restoration professionals in delivering faster and more consistent outcomes. Key components of the DUX Platform include:

- **Inspection App**: Enables users to schedule and manage inspections, track progress, and conduct both live virtual and offline inspections. The app includes high-definition photo and video capture, advanced call controls, and offline capabilities to ensure functionality regardless of connectivity.
- **DUX Erudite AI**: Leverages artificial intelligence to analyze photos, floorplans, and inspection data. The AI identifies defects, damages, material types, installation errors, and progress over time, and can automatically generate scopes of loss, estimates, and inspection reports.
- **Seamless Integration**: The platform supports rapid deployment into existing client systems via a one-line integration or through robust API options, enabling flexibility and scalability across different organizational environments.
- **Report Generation Tools**: Users can annotate images, compile inspection reports in real time during calls, or post-call using AI analysis and human input. Reports can be customized and completed in collaboration with inspectors, adjusters, or property owners.

INFRASTRUCTURE

The Company uses Microsoft Azure as a subservice organization for infrastructure and data hosting services. However, the Company is responsible for designing and configuring the architecture within Microsoft Azure to ensure security and resiliency requirements are met. Controls operated by Microsoft Azure are not included in the scope of this report.

The affected criteria are included below along with the minimum controls expected to be in place at the aforementioned service providers:

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC6.1	• Microsoft Azure is responsible for encrypting data at rest. • Microsoft Azure is responsible for server infrastructure access control.

CC6.4	• Microsoft Azure is responsible for restricting data center access to authorized personnel. • Microsoft Azure is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5	• Microsoft Azure is responsible for securely decommissioning and physically destroying production assets in its control.
CC6.6	• Microsoft Azure is responsible for patching the server infrastructure as part of routine maintenance.
CC7.2	• Microsoft Azure is responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers. • Microsoft Azure is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • Microsoft Azure is responsible for overseeing the regular maintenance of environmental protections at data centers.
CC8.1	• Microsoft Azure is responsible for performing server infrastructure changes.

SOFTWARE

Software consists of the programs and software that support the DUX Platform. Software and ancillary software is used to build, support, secure, maintain, and monitor the DUX Platform.

PEOPLE

The Company develops, manages, and secures the DUX Platform via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Customer Success	Responsible for managing customer relationships.
Engineering	Responsible for the development, testing, deployment, and maintenance of new code.
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Operations	Responsible for finance and accounting.

PROCEDURES

Procedures include the automated and manual procedures involved in the operation of the DUX Platform. Procedures are developed and documented by the respective teams for a variety of processes. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of DUX Platform:

Procedure	Description
Logical Access	How the Company restricts logical access, provides and removes that access, and prevents unauthorized access.

System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
Configuration and Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk and Compliance	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.
Business Continuity and Disaster Recovery (BC/DR)	How the Company identifies the steps to be taken in the event of a disaster to help resume business operations.
Data Classification and Handling	How the Company classifies data included in the service and the procedures for handling the data.
Incident Response Plan	How the Company identifies the steps to be taken in the event of a security incident.

DATA

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the DUX Platform production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

DUX's 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 DUX's controls are suitably designed and operating effectively, along with related controls at DUX. Identified complementary user entity controls were included in the service auditor's examination of SOC 2 controls.

Attachment B – Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of DUX Platform. The Master Service Agreement (MSA) includes the communication of the Company's commitments to its customers.

System requirements are specifications regarding how DUX should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the DUX Platform include the following:

Trust Services Category	Service Commitments	System Requirements
Security	DUX will implement and maintain reasonable administrative and technical safeguards and other security measures to protect customer data.	• Change Management • Encryption Standards • Identity and Access Management • Security Awareness Training • Security Incident Response • Security Monitoring and Reporting • Threat and Vulnerability Management • Vendor Risk Management