



XEROX CORPORATION

App Gallery Platform

System and Organization Controls (SOC) for Service Organizations Report for the period of July 1, 2022 to June 30, 2023



Report of Independent Service Auditors issued by Aprio LLP

Table of Contents

- I. **Report of Independent Service Auditor 1**
- II. **Xerox Corporation’s Assertion 3**
- III. **Xerox Corporation’s Description of the Boundaries of its System 4**
 - A. Scope and Purpose of the Report..... 4
 - B. Company Overview and Background 4
 - C. System Overview 4
 - D. Principal Service Commitments and System Requirements 5
 - E. Non-Applicable Trust Services Criteria..... 6
 - F. Subservice Organizations 6
 - G. User Entity Controls 8

I. Report of Independent Service Auditor

We have examined Xerox Corporation's (the "Company" or "Xerox") accompanying assertion titled *Xerox Corporation's Assertion* (the "Assertion") indicating that the controls within the App Gallery Platform (the "System") were effective for the period of July 1, 2022 to June 30, 2023 (the "Specified Period"), to provide reasonable assurance that Xerox Corporation'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*).

The Company uses Microsoft Azure (Azure), a subservice organization, as a Platform-as-a-Service for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also uses the Azure SQL Database, as a Database-as-a-Service and Office 365 and Azure Active Directory as a Software-as-a-Service. In addition, the Company uses Deloitte MXDR (MXDR) as a Software-as-a-Service provider for monitoring of the production environments. Certain AICPA Applicable Trust Services Criteria specified in the section titled *Xerox Corporation's Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's Assertion includes only the controls of the Company and excludes the controls performed by the subservice organizations. The Assertion does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Assertion indicates that certain AICPA Applicable Trust Services Criteria specified in the section titled *Xerox Corporation's Description of the Boundaries of its System*, under the section *User Entity Controls*, can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. 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.

Service Organization's responsibilities

The Company 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 the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled *Xerox Corporation's Assertion* about the suitability of design and operating effectiveness of controls. When preparing its assertion, the Company is responsible for selecting, and identifying in its assertion, the Applicable Trust Services 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 the 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 the controls were not effective to achieve the Company's service commitments and system requirements based on the Applicable Trust Services criteria; and
- 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 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.

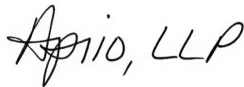
Other matters

We did not perform any procedures regarding the fairness of presentation as it relates to the description criteria of the description in Section III titled *Xerox Corporation's Description of the Boundaries of its System*, and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, Xerox Corporation's assertion that the controls within the Company's System were effective as throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria, in all material respects, is fairly stated.

Aprio, LLP



Atlanta, Georgia
October 11, 2023





II. Xerox Corporation's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls over Xerox Corporation's (the "Company" or "Xerox") App Gallery Platform (the "System") for the period of July 1, 2022 to June 30, 2023 (the "Specified Period"), to provide reasonable assurance that the Company's service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. We have performed an evaluation of the effectiveness of the controls within the System throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (the "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 Company'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 specified in the section titled *Xerox Corporation's Description of the Boundaries of its System*.

The Company uses Microsoft Azure (Azure), a subservice organization, as a Platform-as-a-Service for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also uses the Azure SQL Database, as a Database-as-a-Service and Office 365 and Azure Active Directory as a Software-as-a-Service. In addition, the Company uses Deloitte MXDR (MXDR) as a Software-as-a-Service provider for monitoring of the production environments. Certain AICPA Applicable Trust Services Criteria specified in the section titled *Xerox Corporation's Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's assertion includes only the controls of the Company and excludes the controls performed by the subservice organizations.

Certain AICPA Applicable Trust Services Criteria, specified in Section III, *Xerox Corporation's Description of the Boundaries of its System*, under the section *User Entity Controls* can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's assertion includes only the controls of the Company and excludes the controls performed by User Entities.

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 Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria.

III. Xerox Corporation’s Description of the Boundaries of its System

A. Scope and Purpose of the Report

This report describes the control structure of Xerox Corporation (the “Company” or “Xerox”) as it relates to its App Gallery Platform (the “System”) for the period of July 1, 2022 to June 30, 2023 (the “Specified Period”), for the trust services criteria relevant to Security, Availability, and Confidentiality (the “Applicable Trust Services Criteria”) as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. The internal control structures at the Company are not designed to compensate for any weaknesses that may exist if the internal control structure at a user organization is ineffective.

B. Company Overview and Background

Xerox provides technology that innovates the way the world communicates, connects, and works. Through a portfolio of technology and services, the Company provides back-office support that helps clients’ businesses.

The Xerox App Gallery Platform provides a collection of downloadable and installable applications designed to transform the handling of documents and data by simplifying processes. With these applications, Xerox ConnectKey technology-enabled printers or multifunction printers (MFP) become connected, simple-to-use, smart workplace assistants.

C. System Overview

Infrastructure

The Company utilizes Microsoft Azure to provide the resources to host the Xerox App Gallery Platform. The Company leverages the experience and resources of Microsoft Azure to securely scale as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the Xerox App Gallery Platform architecture within Microsoft Azure to help ensure the security, availability, confidentiality, and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Production Tool	Business Function	Operating System	Hosted Location
Databases	Customer data storage	Microsoft Structured Query Language (SQL) Server	Microsoft Azure
App Services	Processing	Microsoft Azure App Service	Microsoft Azure
Azure Functions	Deployment	Microsoft Azure Functions	Microsoft Azure

Software

Software consists of the programs and software that support the Xerox App Gallery Platform (operating systems [OSs], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor the Xerox App Gallery Platform include the following applications, as shown in the table below:

Production Application	Business Function
Microsoft Azure Monitor	Application monitoring
Microsoft SQL Server Always on Clustering, Geo-redundant Storage, Microsoft Azure Recovery Services vaults	Backup and replication
Microsoft Azure Service Health	Infrastructure monitoring
Windows Defender	Antivirus
Advanced Data Security and Vulnerability Assessment Reports	Intrusion detection
Xerox Service Manager (XSM), Microsoft Azure Help and Microsoft Azure Support, ServiceNow	Help desk, ticketing system

D. Principal Service Commitments and System Requirements

Xerox designs its processes and procedures to meet its objectives for its App Gallery Platform. Those objectives are based on the Global Operations Agreement and Privacy Statement that Xerox communicated to user entities, the laws and regulations that govern the provision of App Gallery Platform, and the operational and compliance requirements that Xerox has established for the services. Security, Availability, and Confidentiality commitments to user entities are documented and communicated in the Global Operations Agreement, Privacy Statement, as well as in the description of the service offering provided online. Security, Availability, and Confidentiality commitments are standardized and include, but are not limited to, the following:

- The use of security and confidentiality principles that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role;
- The use of encryption technologies to protect customer data in transit over untrusted networks;
- The use of reasonable precautions to protect the security and confidentiality of the information that is collected;
- The use of availability principles that are designed to help ensure availability of the systems supporting the system.
- Make commercially reasonable efforts that controls are in place to automatically filter certain personal information collected from the System such as password and account numbers; and
- Make commercially reasonable efforts that controls are in place to destroy or encrypt any information that is not filtered automatically.

Xerox establishes operational requirements that support the achievement of Security, Availability, and Confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Xerox’s system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected.

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	<ul style="list-style-type: none"> • Controls over the prevention, detection, and follow up upon the introduction of malicious software; • Controls over Azure Storage redundancy, including controls over data replication; • Controls over the monitoring of the Office 365 and Azure Active Directory components including backups, anti-virus, and incidents related to security and availability including responding to items identified; • Controls over the encryption of transmitted and stored data within the platform including Azure SQL Database; and • Controls over managing patching for the software and infrastructure supporting the platform, including Azure SQL Database. <p>In addition, the Company has identified the following control activity to help monitor the subservice organization:</p> <ul style="list-style-type: none"> • The Company maintains a vendor management program which includes maintaining a list of critical vendors and requirements for vendors to maintain their own security practices and procedures. The Company reviews attestation reports or performs a vendor risk assessment at least annually for all critical vendors/subservice organizations to evaluate the impact of noted exceptions on the service, and • Data backup restoration tests are performed at least annually to verify data reliability and information integrity. 	<p>A 1.2* A 1.3* C 1.1* C 1.2*</p>
<p>Deloitte MXDR (MXDR)</p>	<p>The Company uses Deloitte MXDR as a Software-as-a-Service provider for monitoring of the production environments. The following control activities are critical to achieving the Applicable Trust Services Criteria:</p> <ul style="list-style-type: none"> • Controls around the reporting and monitoring of the in-scope environments, and • Controls over the monitoring, investigation, notification to the Company, and remediation of security issues. <p>In addition, the Company has identified the following control activity to help monitor the subservice organization:</p> <ul style="list-style-type: none"> • The Company maintains a vendor management program which includes maintaining a list of critical vendors and requirements for vendors to maintain their own security practices and procedures. The Company reviews attestation reports or performs a vendor risk assessment at least annually for all critical vendors/subservice organizations to evaluate the impact of noted exceptions on the service. • Data backup restoration tests are performed at least annually to verify data reliability and information integrity. 	<p>CC 2.1* CC 4.1* CC 4.2* CC 5.1* CC 5.3* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5*</p>

** The achievement of design and operating effectiveness related to this criterion assumes that the complementary controls at this subservice organization that support the service organization's service commitments and system requirements are in place and are operating effectively.*

G. User Entity Controls

Xerox Corporation’s controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company. It is not feasible for the Company’s service commitments and system requirements to be achieved based on the applicable trust services criteria solely by the Company. Therefore, each user entity’s internal control must be evaluated in conjunction with the Company’s controls and taking into account the related complementary user entity controls identified within the table below, where applicable. As applicable, suggested control considerations and/or complementary user entity controls and their associated criteria have been included within the table below.

Management has highlighted criterion in which complementary user entity controls were assumed in the design of the Company’s system with an asterisk. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control environment to determine if the identified complementary user entity controls have been implemented and are operating effectively.

Furthermore, the table below includes suggested control considerations that the Company believes each user organization should consider in developing their internal controls or planning their audits that are relevant to the Company’s controls detailed in this report, however, such control considerations are not required to achieve design or operating effectiveness for the Company’s service commitments and system requirements based on the applicable trust services criteria. The following list of suggested control activities is intended to address only those policies and procedures surrounding the interface and communication between the Company and each user entity. Accordingly, this list does not allege to be, and is not, a complete listing of all the control activities which provide a basis for the assertions underlying the control environments for the Company’s user entities.

User Entity Control	Associated Criteria
User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames.	CC 2.2 CC 2.3
User entities have policies and procedures to inform their employees and users that their information or data is being used and stored by the Company and determine how to file inquiries, complaints, and disputes to be passed on to the Company.	CC 2.2 CC 2.3
User entities are responsible for granting and removing access to the App Gallery Platform’s system to authorized and trained personnel.	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.8*
User entities have policies and procedures over user IDs and passwords that are used to access services provided by the Company.	CC 6.1*
User entities are responsible to notify the Company of any changes to user entity vendor secure requirements or the authorized users list.	CC 6.1 CC 6.2 CC 6.3

Xerox Corporation

SOC 3[®] Report - SOC for Service Organizations: Trust Services Criteria for General Use

App Gallery Platform

User Entity Control	Associated Criteria
User entities are responsible for deploying physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.	CC 6.4 CC 6.5 C 1.1 C 1.2
User entities are responsible for informing the Company that its data should be deleted.	CC 6.5* C 1.1* C 1.2*

** The achievement of design and operating effectiveness related to this criterion assumes that the complementary user entity controls that support the service organization's service commitments and system requirements are in place and are operating effectively.*

Aprio[®] 