



**REPORT ON XEROX CORPORATION'S XEROX
HOSTED MANAGED PRINT SERVICES (MPS)
TOOL SUITE (COMMERCIAL) RELEVANT TO
SECURITY, AVAILABILITY, AND
CONFIDENTIALITY FOR THE PERIOD
JULY 1, 2020 TO JUNE 30, 2021**

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

TABLE OF CONTENTS

SECTION 1

Independent Service Auditor's Report..... 3

SECTION 2

Assertion of Xerox Corporation Management 6

ATTACHMENT A

Xerox Corporation's Description of the Boundaries of Its Xerox Hosted Managed
Print Services (MPS) Tool Suite (Commercial) 8

ATTACHMENT B

Principal Service Commitments and System Requirements..... 13

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Xerox Corporation ("Xerox")

Scope

We have examined Xerox's accompanying assertion titled "Assertion of Xerox Corporation Management" (assertion) that the controls within the Xerox Hosted Managed Print Services (MPS) Tool Suite (Commercial) (system) were effective throughout the period July 1, 2020 to June 30, 2021, to provide reasonable assurance that Xerox'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

Xerox 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 Xerox's service commitments and system requirements were achieved. Xerox has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Xerox 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 Xerox'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 Xerox'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.

Opinion

In our opinion, management's assertion that the controls within the Xerox Hosted Managed Print Services (MPS) Tool Suite (Commercial) were effective throughout the period July 1, 2020 to June 30, 2021, to provide reasonable assurance that Xerox's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Coalfire Controls LLC

Westminster, Colorado
August 20, 2021

SECTION 2

ASSERTION OF XEROX CORPORATION MANAGEMENT

Assertion of Xerox Corporation (“Xerox”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within the Xerox Hosted Managed Print Services (MPS) Tool Suite (Commercial) (system) throughout the period July 1, 2020 to June 30, 2021, to provide reasonable assurance that Xerox’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, 2020 to June 30, 2021, to provide reasonable assurance that Xerox’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*). Xerox’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, 2020 to June 30, 2021, to provide reasonable assurance that Xerox’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Gopi Tatachar
SR Director, Data Center Services
XDX Global Infrastructure & Production Support
Xerox Corporation

ATTACHMENT A

XEROX CORPORATION'S DESCRIPTION OF THE BOUNDARIES OF ITS XEROX HOSTED MANAGED PRINT SERVICES (MPS) TOOL SUITE (COMMERCIAL)

TYPE OF SERVICES PROVIDED

Xerox Corporation (“Xerox” or “the Company”) provides technology that innovates the way the world communicates, connects, and works. Through a broad portfolio of technology and services, the Company provides essential back-office support that helps clients’ businesses work better.

Xerox Managed Print Services (MPS) Tool Suite (Commercial) provides printing infrastructure and services involving all aspects related to printers; their output, supplies, and support; the way documents are used; and the people and processes that intersect each of these. MPS helps gain visibility and control of document processes and costs. This ultimately automates steps, boosts productivity, and improves document security and environmental sustainability.

MPS works by utilizing a three-step approach toward improving printing processes:

- Assess and Optimize
 - Provides assessment and analytics services, business intelligence, device optimization, device monitoring and proactive alerting, consolidated billing and reporting, and a print awareness tool.
- Secure and Integrate
 - Focuses on the following capabilities: print security audit, secure print management suite, print server management service, and help desk integration.
- Automate and Simplify
 - Focuses on helping the Company’s customers reduce the amount of paper in use by automating and simplifying content, collaboration, and process workflows.

THE COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The boundaries of the Xerox Hosted MPS Tool Suite (Commercial) are the specific aspects of the Company’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers performed in the Webster, New York, and Wilsonville, Oregon, facilities. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Xerox Hosted MPS Tool Suite (Commercial).

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

The primary infrastructure used to host the Xerox Hosted MPS Tool Suite (Commercial) consists of multiple supporting tools, as shown in the table below:

Infrastructure		
Hardware Type	Purpose	Hosted Location
Unified Computing System (UCS)	Compute resources	Webster, New York Wilsonville, Oregon

Infrastructure		
Hardware Type	Purpose	Hosted Location
Network (routing, switch, firewall, intrusion prevention system [IPS], or intrusion detection system [IDS])	Internal network	Webster, New York Wilsonville, Oregon
Storage area network	Storage	Webster, New York Wilsonville, Oregon
Load balancers	Load balancing	Webster, New York Wilsonville, Oregon
Backup technology	System backup	Webster, New York Wilsonville, Oregon

Software

Software consists of the programs and software that support the Xerox Hosted MPS Tool Suite (Commercial) (operating systems [OSs], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor the Xerox Hosted MPS Tool Suite (Commercial) includes applications to perform the following business functions:

- OS utilized by MPS infrastructure and applications
- Infrastructure operation system
- Relational database management system used by MPS
- Application monitoring
- Backup and replication
- Security information and event management (SIEM), logging system
- Infrastructure monitoring
- Patch management and file integrity monitoring
- Endpoint detection and response
- Help desk, ticketing system

People

The Company develops, manages, and secures the Xerox Hosted MPS Tool Suite (Commercial) via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	Function
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.

People	
Group/Role Name	Function
Engineering	Responsible for the development, testing, deployment, and maintenance of new code for the Xerox Hosted MPS Tool Suite (Commercial).
Global Security Services (GSS)	Responsible for oversight of cyber security.
Global Purchasing	Responsible for subcontract vendor management and governance, including security and risk management considerations.
Product Management	Responsible for overseeing the product life cycle, including adding new product functionality.
Engineering Services & Support	Responsible for managing access controls, security, and operations of the production environment.
Human Resources (HR)	Responsible for onboarding new personnel, defining the roles and positions of new hires, performing background checks, and facilitating the employee termination process.

Procedures

Procedures include the automated and manual procedures involved in the operation of the Xerox Hosted MPS Tool Suite (Commercial). Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (IT), and HR. 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 the Xerox Hosted MPS Tool Suite (Commercial):

Procedures	
Procedure	Description
Logical and Physical Access	How the Company restricts logical and physical 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.
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 Management	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. There are two types of data that the systems stores, transmits, and processes:

1. Customer data

Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the Xerox Hosted MPS Tool Suite (Commercial) production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet. Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

2. System data

System data is captured and utilized by the Company in hosting its services. Such data includes, but is not limited to:

- Alert notifications and monitoring reports generated from commercial monitoring applications
- Alert notifications received from automated backup systems
- Vulnerability or security alerts received from various sources, including security subscriptions, scanning tools, IDS alerts, or automated patching systems
- Incident reports documented via the ticketing systems

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Databases housing sensitive customer data are encrypted at rest.

The following table details the types of data contained in the production application for the Xerox Hosted MPS Tool Suite (Commercial):

Data	
Production Application	Description
XSM	The Company gathers information on printing hardware and its usage, including details from users within the customer's environment. The information gathered includes what kinds of documents are being printed, at what time of day, and the total size of the jobs. The Xerox Hosted MPS Tool Suite (Commercial) also gathers information on service tickets, device security, configurations, performance metrics, supply requests, and supply requirements.
Xerox Hosted MPS Tool Suite (Commercial) and system tools	The Company logs information about customers and their users, including Internet Protocol (IP) address. Log files are immutable records of computer events about an OS, application, or user activity, which form an audit trail. These records may be used to assist in detecting security violations, performance problems, and flaws in applications.

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

The Company designs its processes and procedures related to system hosting to meet its objectives for its Xerox Hosted MPS Tool Suite (Commercial) services. Those objectives are based on the service commitments that the Company makes to user entities, the laws and regulations that govern the provision of Xerox Hosted MPS Tool Suite (Commercial) services, and the financial, operational, and compliance requirements that the Company has established for the services.

Commitments are declarations made by management to customers regarding the performance of the Xerox Hosted MPS Tool Suite (Commercial). Commitments are communicated in the Global Operations Agreement and the Xerox Privacy Statement, as well as in the description of the service offering provided online.

System requirements are specifications regarding how the Xerox Hosted MPS Tool Suite (Commercial) 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 Xerox Hosted MPS Tool Suite (Commercial) include the following:

Trust Services Category	Service Commitments	System Requirements
Security	<ul style="list-style-type: none"> • The Company utilizes reasonable and appropriate physical, technical, and administrative procedures to protect customer data from unauthorized access, use, or disclosure. • The Company provides infrastructure and procedures associated with application-level security, including secure communications, data encryption, penetration testing, and monitoring of security events. 	<ul style="list-style-type: none"> • Logical access standards • Physical access standards • Employee provisioning and de-provisioning standards • Access review standards • Encryption standards • Intrusion detection and prevention standards • Risk and vulnerability management standards • Configuration management standards • Incident handling standards • Change management standards • Patch management standards
Availability	<ul style="list-style-type: none"> • The Company will ensure the hours of operation are targeted to authorized clients on a 24x7x365 basis outside of any scheduled maintenance windows. • The Company will ensure the service availability target for the collective MPS Suite of tools will be 99.95%. 	<ul style="list-style-type: none"> • System monitoring standards • Backup and recovery standards • Physical protections • Data redundancy

Trust Services Category	Service Commitments	System Requirements
	<ul style="list-style-type: none"> The Company maintains appropriate policies, technologies, and procedures for storing, restoring, and recovering data and systems in order to ensure business continuity. 	
Confidentiality	<ul style="list-style-type: none"> The Company will use a variety of security technologies and procedures to protect confidential data from unauthorized access, use and disclosure. 	<ul style="list-style-type: none"> Data classification standards Retention and destruction standards Data handling standards Internal confidentiality standards Information sharing standards