KOFAX

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

SOC 3®

January 1, 2022 to September 30, 2022

FORVIS

Kofax®

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

SOC 3®

January 1, 2022 to September 30, 2022

Contents

Section I
Independent Service Auditor's Report

FORVIS

111 Center Street, Suite 1600 / Little Rock, AR 72201
P 501.372.1040 / **F** 501.372.1250
forvis.com

Independent Service Auditor's Report

Audit Committee
Kofax®
Plano, TX

Scope

We have examined Kofax®'s (Kofax or the Company) accompanying assertion titled "Kofax Assertion" that the controls within Kofax Public Cloud Platform system, hereinafter "Kofax Public Cloud Platform," were effective throughout the period January 1, 2022 to September 30, 2022, to provide reasonable assurance, based on the TSP section 100, 2017 Trust Services Criteria for Security and Availability (AICPA, Trust Services Criteria), that:

- Kofax Public Cloud Platform system was protected against unauthorized access, use or modification to meet the entity's commitments and system requirements
- Kofax Public Cloud Platform system information and supporting systems were available for operation and use to meet the entity's commitments and system requirements

Kofax service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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

Kofax 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 Kofax Public Cloud Platform service commitments and system requirements are achieved. Kofax has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Kofax 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 Kofax 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 Kofax 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.

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 Kofax Public Cloud Platform system were effective throughout the period January 1, 2022 to September 30, 2022, to provide reasonable assurance that Kofax service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

FORVIS, LLP

FORVIS, LLP

Little Rock, AR

December 23, 2022

Section II
Assertion and Description Provided by Kofax®

Kofax®
Assertion

We, as management of Kofax® (Kofax or the Company), are responsible for designing, implementing, operating, and maintaining effective controls within Kofax Public Cloud Platform system hereinafter "Kofax Public Cloud Platform" throughout the period January 1, 2022 to September 30, 2022, to provide reasonable assurance that Kofax service commitments and system requirements relevant to security and availability were achieved. Our description of the aspects and boundaries of Kofax Public Cloud Platform covered by our assertion is presented in the section entitled, "*Kofax®' Description of the Kofax Public Cloud Platform system*.

We have performed an evaluation of the effectiveness of the controls within Kofax Public Cloud Platform throughout the period January 1, 2022 to September 30, 2022, to provide reasonable assurance that Kofax service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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*). Kofax®'s objectives for Kofax Public Cloud Platform 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 Appendix A.

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.

Kofax® asserts that the controls within the system were effective throughout the period January 1, 2022 to September 30, 2022, to provide reasonable assurance that:

- Kofax Public Cloud Platform system was protected against unauthorized access, use or modification to meet the entity's commitments and system requirements throughout the period January 1, 2022 to September 30, 2022, based on the Trust Services Security and Availability Criteria set forth in TSP Section 100 established by the American Institute of Certified Public Accountants (AICPA)

- Kofax Public Cloud Platform system information and systems were available for operation and use to meet the entity's commitments and system requirements throughout the period January 1, 2022 to September 30, 2022, based on the Trust Services Security and Availability Criteria set forth in TSP Section 100 established by the American Institute of Certified Public Accountants (AICPA)

The attached system description of Kofax Public Cloud Platform system identifies the aspects of the system covered by our assertion.

Kofax®'s Description of Its Public Cloud Platform for the Period January 1, 2022 to September 30, 2022

Organization of the Report

This report is intended to provide Kofax®'s (Kofax or the Company) customers and user entities with information about the controls related to the services provided by Kofax. This section provides an overview of Kofax's service offerings and specific control activities related to the administration of these services.

The system represented within this report encompasses the following services offerings hosted in the Kofax public cloud infrastructure; AP Essentials, SignDoc Cloud and TotalAgility Cloud.

Company Overview

Kofax as an enterprise provides organizations around the world with the technology needed to automatically transform their incoming business content into useful, digital data that is delivered directly into the applications that drive the business.

AP Essentials, SignDoc Cloud and TotalAgility are Cloud based deployments developed by R&D teams and supported by Cloud Services team in Helsingborg and Kista, Sweden, Derry, Northern Ireland, London, United Kingdom, Podgorica, Montenegro and Hyderabad, India. The SaaS systems are maintained and operated internally by the Cloud Services team. The Kofax Public Cloud is hosted in Microsoft Azure and is developed based on native Azure capabilities for cloud computing. The Azure platform enables hosting and scaling applications in Microsoft data centers providing an elevated level of security and compliance. The Technical Support team provide first line application support.

Service Offerings

Kofax's Cloud Services organization is responsible for the operation and delivery of all hosted applications, globally (AP Essentials, SignDoc Cloud, and TotalAgility Cloud). Centralizing the SaaS delivery responsibilities in this way allows Kofax to concentrate expertise and provide control continuity for all cloud-delivered applications and services.

AP Essentials

AP Essentials (APS) cloud solution provides automated invoice processing with workflow automation. APS accelerates invoice processing and ensures proper routing of invoices, enforced approval policies, higher levels of accuracy and decreased dependency on manual labor. APS provides data capture and extraction (optical character recognition (OCR)), line-item matching, approvals, general ledger coding and ERP-integration. APS integrates with enterprise resource planning (ERP).

SignDoc

SignDoc Cloud enables trustworthy, secure, and convenient paperless signing. Kofax SignDoc Cloud enables you to replace wet-ink signing with electronic signatures that simplify and expedite your business processes. SignDoc Cloud delivers substantial evidence of approval and adoption of a document's contents and its binding, conclusive, non-reputable character. It enables the

validation of authenticity and integrity of signed documents - by providing means to authenticate a signer's identity as well as verifying that the document has not been altered after signing.

TotalAgility Cloud

TotalAgility Cloud is an omnichannel solution that uses embedded AI to automate more unstructured content to capture, classify, extract, and understand print and language from any type of content (forms, claims, shipping documents, contracts, letters, etc.) coming from any channel (mobile, email, web, fax, folder, desktop scanner, MFP, etc.). This allows for a real-time link between customer-facing systems of engagement and internal systems of record.

Subservice Organizations Utilized

Cloud Services uses the following subservice organization to provide the services: **Microsoft Azure – Hosts cloud infrastructure.** Microsoft Azure is responsible for maintaining controls over logical and physical security to the cloud environment, identification and communication of potentially significant computer security events that may have an impact on the Cloud Service production environment, as well as change management of cloud servers and infrastructure equipment. Cloud Services does not maintain any hardware or networking equipment to support the services. There are no additional office spaces deemed as sensitive locations in the context of the services.

Our conclusion regarding effectiveness of controls within the system to Kofax's service commitments and system requirements based on the applicable trust services criteria assumes that the complementary subservice organization controls assumed in the design of the Kofax Public Cloud Platform operated effectively throughout the period January 1, 2022 to December 31, 2022.

Principle Service Commitments

Kofax designs its processes and procedures related to Cloud Services to meet its objectives for its Public Cloud offerings. These objectives are based on the service commitments that Kofax makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that Kofax has established for the services.

Security commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Average uptime
- Fundamental design of the system supports the protection of user data by ensuring that users access information based on their role in the system and restrict access to unauthorized users
- Use of encryption technologies to protect customer data both at rest and in transit

Kofax and Cloud Services have established operational requirements to achieve its objectives within 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, and Cloud Services security policies further define how its specific services protect data. These include policies around how the service is designed and developed, how the system is operated, and how the internal business systems and networks are managed and how employees are hired and train.

Components of the System

Infrastructure

The Kofax Public Cloud platform is hosted by infrastructure sub processors. Development occurs on systems in environments that are separate from the production environment. Customer data is processed by and stored in the hosted infrastructure. Azure regions used; North Europe, East US 2, East US, South Central US, West US, Central US, North Central US, Australia East, Australia Southeast, East US, North Europe, South Central US, Southeast Asia.

Access to the Azure production environment is by authorized Cloud Services (CS) personnel. CS personnel access the Azure production environment through a virtual private network (VPN) and multifactor authentication (MFA). Customers do not have direct access to Azure environment outside of the application via a web browser. Customer data and authentication is encrypted using TLS public key encryption.

Software

The applications are provided to customers as a fully managed software as a service (SaaS) application.

Supporting Applications

Kofax uses the following key applications to support the security of the system and the performance of the services listed in this report:

Tool Name	Purpose
Maintained by Cloud Services	
Issue and Project Tracking Software	Ticket and Project Management
Corporate Wiki	Document management (Policies and diagrams)
Version Control Software (Cloud)	Deployment Pipeline for applications
Server Monitoring Platform	Server monitoring for Azure Infrastructure
Password Manager Software	Password Management
Log Management Software	Log aggregation for production
Incident Response Platform	Various server and operational alerts
Security Information and Event Management System	Security Information and Event Management
Maintained by Kofax Enterprise	
Customer Service Platform	Customer Application Help Desk Management
Version Control Software (Co-location)	Development Project Management
Application Analysis Tool	Static Code Inspection
Code Review and Project Analytics Platform	Code Review in Development Process
Build Management Software	Build Management for Development
Help Desk and Ticketing System	IT and Security Ticket management

People

Kofax Cloud Services organization has defined role responsibilities and relationships between groups to ensure segregation of duties.

Cloud Services Roles

Management

Kofax's management believes that shareholders, employees, and clients are best served by a management team that is actively involved in the day-to-day operations of the company, while providing employees with the authority required to properly perform their job duties. As such, the Cloud Services Management Team takes a hands-on approach to service delivery and is ultimately responsible for the oversight and management of the groups listed below.

Cloud Services Delivery

The Services Delivery team is responsible for all tenant management, on- and off- boarding of customers, licensing. This group is also the elevation point offering back-office support for Technical Support, Professional Services and Sales/Sale Engineering during both the production phase as well as during implementation projects. During incidents, the Services Delivery team carries the responsibility of Customer Liaison.

Cloud Operations

The Cloud Operations team is responsible for the health and availability of the SaaS solutions hosted in the Kofax Public Cloud. Managing the infrastructure and third-party applications. Responsible for monitoring the telemetry systems and acting when anomalies occur. The Cloud Operations team operate a 24/7/365 On-Call rotation to maintain the ability to respond to incidents and remediate to meet defined SLAs.

Cloud DevOps and SecDevOps

This group is responsible for developing the; observability platform, deploy pipelines, backup, and disaster recovery. Responsible for new technology introduction. Defining hardening standards. design and implement secure network topologies. Take part in security incident response and remediations, security design reviews, implement to meet compliance requirements, raising security awareness.

Cloud Governance Risk and Compliance

This group are the custodians of the Cloud Services control environment. Developing and maintaining an effective policy and control framework. Manage and lead information security governance. Establish, monitor, and continuously improve risk management procedures. Facilitate external audits. Provide oversight and management of review and audit finding remediations.

Enterprise Roles

The Kofax enterprise supports the Cloud Services team with:

Security & Compliance

Security & Compliance is responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected within Kofax. The group must be up to date on changes to regulations and industry standards. The Senior Director of Security & Compliance reports to the CIO.

Human Resources

Human Resources is responsible to fulfill its security requirements for the employee onboarding, transfer, role change, and termination process. In addition, HR has the responsibility for employee education planning and the disciplinary process.

Enterprise IT

Enterprise IT is responsible for complying with security requirements in life cycle management for end user devices used by the Cloud Services Team. Enterprise IT maintains the email system and internal networks that support enterprise applications. It is important to stress that Enterprise IT is NOT responsible for maintaining the customer facing application's hosted in the Kofax Public Cloud as that is owned by Cloud Services. The Kofax Public Cloud environment does not have any dependencies or trusts with Enterprise IT's networks.

Research and Development (R&D)

The Development Team is responsible for code development for Kofax's suite of products. The team is focused on new product development and enhancements to existing products which are identified by the Product Management Team. The Development team is responsible for development and Quality Assurance in accordance with the SDLC. The Development team is staffed with personnel who have development skill sets and are responsible for bug fixes, minor features and break/fix that requires database or debug skill sets. The Quality Assurance Team is responsible for creating and executing test plans to ensure proper functionality and performance of code developed by Kofax. The team is responsible for logging defects into the bug tracking system and validating fixes by retesting.

Board of Directors

The Board of Directors is responsible for formulating strategy, corporate and capital structure, overseeing financial reporting and auditing, external communication, board appointments, compensation policy and maintenance of corporate governance standards. The Board of Directors is also responsible for ensuring that the necessary internal control mechanisms are in place to identify business, financial and operating risks and developing adequate structures and policies to mitigate those risks. The Board of Directors has a separately designated standing Audit Committee, Remuneration Committee and Nomination Committee. Each committee has a written charter that has been approved by the Board of Directors.

Procedures

Cloud Services has established policies and procedures. Policies are made available to team members via the Corporate Wiki. Cloud Services Controls, Practices, SOPs, and product specific documentation are only made available to contributors that are directly involved in delivering or developing the service. These documents are reviewed by Cloud Services leadership annually and are designed to address the security of the cloud environment. Policies include but are not limited to: Acceptable Use Policy, Access Control Policy, Availability Policy, Business Continuity Policy, Change Management Policy, Cryptography Policy, Data Communication Policy, Data Management Policy, Incident Management Policy, Information Security Policy, Malware Protection Policy, Risk Management Policy, Vendor Management Policy.

In addition, the Kofax enterprise maintains policies and procedures over its control environment and security. Policies and procedures guide various contributing departments such as Security & Compliance, Human Resources, and Enterprise IT. Similarly, R&D maintains policies and practices for software lifecycle management.

Data

The System stores and processes information provided by user entities; all such information is maintained as confidential. This confidential information is available only to members of the user entity. Each user entity has designated administrators who authorizes member access to information stored. As described in the Data Management Policy access to customer data by Company personnel are restricted to authorized personnel only. All other access to customer data

by Company personnel requires management authorization or explicit approval from the user entity.

Description of the Control Environment, Risk Assessment, Monitoring and Information and Communication Systems

Control Environment

The control environment reflects the overall attitude and awareness of management and personnel concerning the importance of controls and the emphasis given to controls in Kofax's policies, procedures, and actions. The company structure, separation of job responsibilities by department and business function, and documentation of policies and procedures are the methods used to define and implement operational controls.

Kofax's organizational structure provides the framework for planning and directing service operations. Kofax's Cloud Services Leadership Team oversees the activities related to delivering Kofax's Customer facing SaaS offerings. This team is responsible for establishing the overall policy and control environment and meets regularly to monitor the operations. Kofax has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and requirements as they relate to security. Lines of authority and responsibility are clearly established and communicated in the Kofax Roles and Responsibilities Policy.

Kofax has established and implemented policies and procedures to address critical operational processes including the Human Resources Department, information systems, security, and operations. The policies and procedures are maintained on an internal website for access by all Kofax employees that take part in either developing or delivering the service. Policies are reviewed annually, updated, and approved by Senior Management to remain current. Employees are required to complete security awareness training when hired and on an annual basis to understand their obligations and responsibilities to comply with security policies.

Kofax's commitment to competence includes management's determination of the levels of competence and expertise required for each position in the Company, ensuring employees meet or exceed the requirements of their position. All new hires undergo a third-party background check, criminal history check and drug testing before their first day of employment (subject to local regulations). New hires are given company policies to read and then sign acknowledgement forms.

Organizational values and ethical behavior standards have been established by the Senior Management Team in conjunction with the Human Resources Department. Employees are required to sign and acknowledge that they have read, understood and agreed to comply with Kofax's Employee Handbook.

The Human Resources Department, along with the employee's immediate supervisor, are responsible for ensuring that terminated employees leave the company in accordance with the exit process.

Communication and Information

Kofax has developed formal design and operation documentation that describes the system and has communicated that documentation to relevant parties. For internal users, system design documentation is available to authorized users on an internal website. For external system users, relevant system description and documentation has been provided within the applications in the

form of user help and administration guides. Kofax maintains formal agreements with customers that define service scope and standards related to security.

Cloud Services management review the necessary observable data requirements to support securing health and availability of its service annually. Performance metrics must be shared within Cloud Services on a weekly basis in order to perform trend analysis. The key data that is logged in accordance with the Observability, Logging, and Forecasting Policy is centralized and read-only in order to maintain its integrity.

The onboarding process for new employees includes training for internal system users on the appropriate process for reporting performance issues, system failures, security incidents or other concerns to the appropriate personnel. Additional training for reporting suspected security incidents is covered in the annual security awareness training program. User awareness is tested with a simulating phishing attack managed by Security & Compliance on an at least annual basis. Kofax has engaged a third party to maintain a whistleblower hotline to provide a separate communication line to enable anonymous or confidential communication if the need arises.

Management presents information regarding the functioning of internal control to the Board of Directors on a regular basis.

Risk Assessment

Kofax has established a risk assessment process to identify and manage risks that could affect the ability of Kofax to provide services to its customers. These processes require management to identify significant risks in their areas of responsibility and implement appropriate measures to address these risks. The Cloud Services Leadership Team meets on a regular basis to discuss any significant risk that may impact the business unit or the ability to deliver on customer obligations.

Oversight of the risk assessment process is conducted by Security & Compliance. Security & Compliance facilitates regular internal and third-party security vulnerability tests and security assessments against the Cloud Services group and its operations.

Security & Compliance maintain a vendor management program to assess its risk when using significant third parties. A vendor risk assessment must be completed prior to the relationship commencing. Vendors that pose significant risk undergo an annual review that includes a review of an internal control attestation report.

Monitoring

Kofax utilizes a variety of monitoring and management systems to ensure the security of the system.

Cloud Services utilizes various systems for continuous monitoring of security and operational controls, such as the Server Monitoring Platform, the Incident Response Platform, and the Security Incident and Event Management System (SIEM). These platforms are configured to send alerts to the Security & Compliance team or Cloud Services team. A third-party provides a managed Security Operations Center (SOC) which has oversight of the Security Incident and Event Management System. The Security & Compliance team is responsible meeting on a weekly basis to review any security events.

Kofax uses a combination of internal and third-party processes for vulnerability assessment. Internal vulnerability scans using are conducted monthly by Security & Compliance team. External vulnerability testing is performed by a cybersecurity solutions company. Kofax maintains an Incident Response policy that communicates the procedures for incident reporting, escalation, and communication. All security incidents are tracked in a ticketing system, triaged, and investigated by Security & Compliance.

Cloud Services is responsible for monitoring internal control, performance of its principal service commitments, and the services during regular leadership meetings. Regular operational meetings occur with the Technical Support, Development, Operations teams, as well as the product owners. Cloud Services and the Development Team collaboratively participate in daily stand-ups (agile) to monitor progress and issues in safeguarding site reliability and discuss any development or production issues that arise. Cloud Services employees have a monthly employee feedback meeting to monitor progress and goals. Management holds a quarterly All-Hands Cloud Meeting to discuss progress on goals and matters of internal control.

Logical Access Controls

Information Asset Management

The Data Management Policy outlines the requirements for security based on information classifications. All data used within the cloud environment is treated as confidential, and the individual Microsoft Azure Resources within each subscription is protected as such.

System Authentication

Access to the production environment is by authorized Cloud Services (CS) personnel only. CS personnel access the Azure production environment through a virtual private network (VPN) and multifactor authentication (MFA). Customers do not have direct access to the Azure environment outside of the application via a web browser. The memorized secret element of the MFA required to access the production environment is configured to conform to the minimum requirements outlined in the Password Policy.

When customers access via web browser, the Azure Application Gateway and Web Application Firewall protect customer data and authentication using TLS public key encryption. The application supports individual user authentication and can support SAML 2.0 and multifactor authentication (MFA). Customers are not required to utilize SAML 2.0 or MFA if their technology infrastructure or security posture does not allow or require it.

Data Protection

SQL data are encrypted at rest conforming to the Advanced Encryption Standard (AES). Encryption keys must be securely stored. Access to client data sets is logically segregated, meaning user organizations can only access their own data sets. TLS protects any transmissions when users access the system via a web browser. Cloud Services must have centralized malware protection installed on production assets and activated to detect and proactively prevent malware.

User Access Management

Production asset that supports applications that process customer data reside in an Azure subscription. The Cloud Services team is responsible for managing the access to the production assets.

There are four generic roles: Operations, Developers, Management, and Analysts.

Developers do not have access to promote items to production.

Requests for new system access are initiated in the Issue and Project Tracking Software. User access management changes follow the change management process and therefore must be approved prior to being granted. Cloud Services management must approve any request for new or changed access.

Upon employee termination, Cloud Services deactivates access to the production environment within 24 hours. An off-boarding checklist and inventory is completed to document the access removal of terminated employees, documented in the Issue and Project Tracking Software.

The Director of Cloud Services performs a user access review of Cloud Services accounts for the Application, network, and databases on a regular basis. If unauthorized or stale access is discovered, access is removed within one business day.

Boundary Protection

The applications operated in the Kofax Public Cloud are web application and is protected as such. A Web Application Firewall (WAF) sits on top of the Application Gateway. The WAF uses OWASP rule sets to protect the application from common web vulnerabilities and exploits. A combination of an Application Gateway and Network Security Groups (NSGs) are used to orchestrate and protect access to the production boundaries.

Mobile Device Management

Enterprise IT is responsible for maintaining controls over endpoints that Cloud Services personnel use to access production environments. Endpoints are centrally managed using a mobile device and operating system management system. Endpoints are disk encrypted using Microsoft's native BitLocker technology. The mobile device and operating system management system is also used to deploy antivirus to each endpoint. In the event of non-compliance with Acceptable Use Policies, IT has the ability to remotely erase data stored on mobile devices. When an employee terminates, mobile devices are collected, and data stored on the device is wiped in a secure manner.

Email Protection

Kofax Enterprise IT is responsible for maintaining controls to protect employees from email security events. The enterprise email service is equipped with the following capabilities: Incoming attachment scanning, URL verification and malicious URL blocking, anti-phishing protection.

The Enterprise Incident Response process is invoked in the event that a user is suspected of being affected by an email security event. Kofax Enterprise IT does not host or operate the email servers utilized by Kofax Public Cloud production environment, that is hosted and operated exclusively by the Cloud Services team.

System Operations

Baseline Configurations

A baseline configuration for Azure resources is established. This baseline is set up via security policy to automatically be applied when a new asset is built, even if the Administrator manually forgot to set up the item. As a failsafe, if this configuration was not automatically applying a desired security policy, the Incident Response Platform would trigger an alert to the On-Call Cloud Services contributor.

Event Detection

From a security incident standpoint, there are two main tools that the Cloud team uses: Security Incident and Event Management (SIEM), Incident Response Platform.

Optiv Security, Inc. provides and helps manage the SIEM for Cloud Services. The SIEM is the first line of defense in determining if events are a significant item. When a significant event is identified, Security & Compliance and Cloud Services are notified via email and the Incident Response Platform.

The SaaS based Incident Response platform aggregates information from numerous services and then will create alerts based on thresholds. The following items are examples of areas of interest for the Incident Response Platform: Application-level items such as slow processing time or CPU slowdowns, Errors in the underlying infrastructure, Maintenance jobs such as hosting validations and security groups, Failure of backup jobs.

In addition, events can be manually reported in the Issue and Project Management System or submitted by internal or external users via email.

Incident Triage

When Cloud Services is notified of a significant event, the triage process begins. The Incident Response Platform maintains a 24/7 alerting ‘On-Call’ schedule that notifies members of the Cloud Services team, that must acknowledge these alerts. This individual is now designated as the “Incident Lea." The Incident Lead is responsible for digesting the information associated with the event and determining if the event is a true security or operational incident. If so, the Incident Management Process begins.

Incident Management

Kofax Cloud Services defines two types of incidents: Information Security Incident and Operational Incident.

Incidents are tracked within the Incident Response Platform. The Incident Lead submits the urgency and impact which determine the severity level (SEV-1 through SEV-5). Communication of incidents to internal parties is defined by a formalized communication interval structure:

- SEV-1 and SEV-2 incidents must be addressed within one hour
- SEV-3, SEV-4, and SEV-5 incidents must be addressed within four business hours

The Incident Response Policy defines the incident response phases and the roles and responsibilities of stakeholders with responsibility for implementing incident response.

When an Information Security incident is identified either by Security & Compliance or by Cloud Services, it is up to Cloud Services to contain the incident as Security & Compliance does not have operational access to make changes to the cloud infrastructure to maintain appropriate segregation of duties. When a security incident has been contained, the infected host/asset cannot be brought back online to the network until the incident has been eradicated or solved. If applicable/feasible/necessary, a workaround or temporary solution or restoration can occur as part of the eradication process.

Restoration of an incident means that normal operations can be restored to how they were prior to the incident, meaning any implemented workarounds as part of the incident response can be put to rest. This may be simple in the event of an operational incident or can be complex in the case of a SEV-1 incident that requires the DR plan to be activated. The status of the incident must be monitored upon recovery to verify that return to normal operations was performed successfully and that the incident is resolved.

SEV-1 and SEV-2 incidents undergo a postmortem meeting to evaluate the effectiveness of incident response. The accuracy and completeness of documentation, effectiveness of communication, effectiveness of procedures, and lessons learned are all a part of this meeting.

During the postmortem evaluation of SEV-1 and SEV-2 incidents, one of the things that the Senior leadership of Cloud Services is evaluating is if new controls need to be implemented from preventing the issue from occurring again. If that is the case, expected delivery date of new controls or risk mitigating items are documented.

For major incidents that impact performance or availability of the application for users (SEV-1 or SEV-2), there is a status.kofaxcloud.com/history webpage where incidents and the resolution of such are reporting.

If a security incident has involved sensitive data, this would be escalated to the CIO, Legal, and HR. A determination on reporting the incident to the parties on the breach list, a document maintained by the Enterprise, is made in the event of a material data breach.

Incident Recovery Training

A monthly technical incident recovery exercise is held to train technical staff on recovering from failure events. These exercises could also include tabletop exercise to walk-through a hypothetical disaster recovery scenario.

Change Management

Application Change Management

Development

The Application typically follows a monthly release cycle. The development team runs a four-week sprint, with the last week being preparation for deployment.

Developers utilize a local Version Control Software system and test code locally. During the development process, a static-code scanning tool scans on a nightly basis to analyze source code for vulnerabilities are remediated by developers and are reported to management monthly. When initial testing and peer review is complete, updates are promoted to the Azure Development Environment to begin the Quality Assurance (QA) process.

Application Change Management

When a change is being submitted for deployment, justification and risk assessment is required to be documented in the Issue and Project Management System. Application changes require that a backout plan(s) is documented prior to being promoted to production. The Change Approver which is a member of Cloud Services Management designated according to the risk level assigned to the change, approves the change prior to being promoted to production when evidence of successful test plans was ran in a test environment. An appropriate member of Cloud Services promotes the change, as access to production must be appropriately segregated and restricted to authorized personnel. After implementation of an application change to production, the change implementer(s) will verify and validate the change.

Kofax publishes release notes that are available to user entities via help menus for every application release. Release information is presented to relevant departments internally for application releases within the Corporate Wiki.

Infrastructure Change Management

Infrastructure changes encompass a wide number of items. This includes, but is not limited to, WAF updates, server configuration, patch management, monitoring tool thresholds, database changes, and policy/procedure documentation updates. Cloud Services utilizes a two-week sprint

process to prioritize and manage changes to the cloud infrastructure. A Kanban board helps guide Cloud Services through its planned items.

The same change management process that applies to application updates is also applied to infrastructure changes. In the event a test environment is not feasible, justification must be provided.

A process for emergency changes is defined. When a Cloud Services contributor is submitting a change in the Issue and Project Management System, there is an option to select an emergency change. This allows changes to be implemented quickly with the requirement that they will be reviewed and approved by management at a later moment.

At the end of the month, Cloud team management and a Compliance Analyst review change, including high risk and emergency changes, for handling and impact on the environment.

Summary

The description presented above is designed to provide the reader a brief description of the activities performed by Kofax®. Kofax®'s management believes the activities are appropriate for the services provided.

Kofax®'s specific controls designed to meet the applicable trust services criteria are included in Section III of this report, "Information Provided by Service Auditor" and captioned as "Provided by Kofax®." Although the specific applicable trust services criteria and related controls are included in Section III, they are nonetheless an integral part of Kofax®'s description of its system and controls.

Complementary User Entity Control Considerations

Our description of the boundaries of the system and the principal service commitments and system requirements related to the applicable trust services criteria does not include complementary user entity controls.

Our conclusion regarding the effectiveness of controls within the system to achieve Kofax's service commitments and system requirements based on the applicable trust services criteria assumes that complementary user entity controls assumed in the design of the Kofax's controls operated effectively throughout the period January 1, 2022 to December 31, 2022.