Warning

DOCUMENTS CONTAIN CONFIDENTIAL INFORMATION OF DOCUSIGN, INC.

UNAUTHORIZED DISCLOSURE IS STRICTLY PROHIBITED

DocuSign

DocuSign eSig Security and Trust Assurance Packet 2023

Trust Center Download

Table of Contents

Welcome

Thank you for your interest in DocuSign's security and compliance practices. We greatly value your trust in DocuSign and appreciate your business. With a foundation of deep and sustained investments in enterprise security and operations, we're proud to serve over a million customers and more than a billion users in over 180 countries, and we take active measures to ensure world-class security and operations to accelerate the process of doing business and simplify people's lives using the DocuSign Agreement Cloud.

This packet contains information and reports to share with you the measures we take to protect your data and maintain your trust. We've included third-party audit reports, certifications, attestations of compliance and high-level overviews of our security and privacy practices.

We hope you find this content helpful in answering the questions you may have about security, data privacy and compliance at DocuSign. If you need further information, please contact your sales representative with any additional requests.

Thank you,

DocuSign Trust Assurance Team

Stringent information security and controls

The privacy and security of our customers' information, documents, and data is a top priority for DocuSign. We adhere to some of the most stringent information security standards in the industry, qualify suppliers through an established third-party risk management program and audit our enterprise business and production operations to ensure our ongoing compliance. DocuSign eSignature provides a high degree of security that has been examined and validated through recognized global standards, including ISO 27001:2013 certification and SOC 1 Type 2 and SOC 2 Type 2 reports.

ISO/IEC 27001:2013 Certificate

Certificate of Registration, Information Security Management System ISO/IEC 27001: 2013, Certificate Number ISMS-DO-110222

ISO standards are published by an independent, worldwide federation of national standards bodies from more than 150 countries. ISO/IEC 27001:2013 is a formal set of requirements to ensure the comprehensive deployment, management, operation and continued improvement of information security with respect to the assets and information it's intended to safeguard. This is the highest level of global information security assurance available today and demonstrates to customers that DocuSign meets stringent international standards on security. We operate an Information Security Management System (ISMS) that complies with the requirements of ISO/IEC 27001:2013, ISO/IEC 27017:2015 and ISO/IEC 27018:2019.

DocuSign External Statement of Applicability

We supply customers with an External Statement of Applicability that details the breadth and applicability of control activities included in our global ISO/IEC 27001 certification. This document describes all control activities that DocuSign operates to ensure we maintain our annual certification with ISO/IEC 27001:2013, ISO/IEC 27017:2015 and ISO/IEC 27018:2019.

AICPA SOC report

The American Institute of Chartered Public Accountants (AICPA) developed a suite of internal System and Organization Control (SOC) reports for the services provided by a service organization. Two of these reports, SOC 1 and SOC 2, provide valuable information that customers need to build confidence in a service organization's systems.

- ***Report on Controls Placed in Operation, and Tests of Operating Effectiveness (SSAE 18, SOC1 Type 2):*** describes the internal controls in place over financial reporting at an organization and requires a third-party service auditor to review and examine the organization's operations over a set period of time. This report on DocuSign was issued by an independent auditor that examined DocuSign and determined that DocuSign is operating effectively and efficiently relative to its desired state. (Available upon request to current DocuSign customers.)
- ***Report on Controls Placed in Operation and Tests of Operating Effectiveness Relevant to the Security, Availability, and Confidentiality Principles (AT-C 205 SOC 2 Type 2)*** describes the controls in place at a service organization for security, availability and confidentiality. It's intended to provide additional assurance to users of the organization's services about the security and privacy of their data. This report on DocuSign was issued by an independent auditor that examined DocuSign and determined that DocuSign is operating effectively and efficiently relative to its desired state.

CSA Security Trust Assurance and Risk (STAR) program

DocuSign adheres to the requirements of the CSA STAR program, which comprises key principles of transparency, rigorous auditing, and harmonization of standards. Our Consensus Assessments Initiative Questionnaire (CAIQ) documents the rigor and strength of DocuSign's security posture and best practices and is publicly accessible for viewing and download from the CSA STAR registry.

Global reach and recognition

DocuSign processes also adhere to and are recognized by government regulations and frameworks for data privacy and security around the world.

Binding Corporate Rules

DocuSign BCR

DocuSign obtained approval of Binding Corporate Rules (BCRs) from the European Union Data Protection Authorities. The approved BCRs enable us to transfer personal data across borders in a compliant manner through the DocuSign platform when customers use DocuSign eSignature. Our BCRs reflect DocuSign's commitment to data protection in our business operations and engagements with customers, employees, suppliers, vendors, and business partners, as well as our compliance with data protection laws. Learn more about DocuSign's BCRs.

FedRAMP (U.S. Federal Risk and Authorization Management Program)

FedRAMP

FedRAMP is a standardized approach for assessing, monitoring, and authorizing cloud computing products and services. DocuSign was awarded the FedRAMP Agency authorization and is listed on the U.S. Federal Government's FedRAMP marketplace with a Government Community Cloud deployment model.

FISC (The Center for Financial Industry Information Systems)

The FISC develops security guidelines for information systems, which are followed by most financial institutions in Japan. These include guidelines for security measures to be put in place while creating system architectures, auditing of computer system controls, contingency planning, and developing security policies and procedures. Though compliance with the FISC Security Guidelines isn't required by regulation nor audited by the FISC, DocuSign elected to become a member of the FISC and implemented internal controls to be compliant with the FISC Security Guidelines. For a detailed description of how DocuSign demonstrates FISC compliance, please contact your account manager.

Compilation of (EU) Member States Notification on SSCDs and QSCDs

This publication lists the signature devices that shall be considered as Qualified Signature Creation Devices (QSCDs) under the eIDAS regulations. DocuSign owns and operates a remote signature device, which is listed in this publication, and is the leading global eSignature solution offering cloud-based eIDAS-compliant electronic signatures.

EU Trusted List

DocuSign France SAS, a DocuSign company, is a trust service provider (TSP) under EU Regulation 910/2014 for electronic identification and trust services (eIDAS). As a TSP, DocuSign France provides qualified electronic signatures (QES), qualified time stamps, advanced electronic signatures (AES), and advanced seals recognized by all EU member states. DocuSign France is listed as a qualified TSP in the Trusted List managed by the French IT Security Agency, ANSSI.

Validated payment security compliance with PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of information security requirements that any entity touching credit card data must comply with as mandated by the major credit card brands. As an organization that's both a service provider and a merchant, DocuSign undergoes annual audits by a Qualified Security Assessor that validates our compliance from both perspectives.

Attestation of Compliance (AOC) — Service Provider

A service provider as defined by PCI is "a business entity that is not a payments brand, directly involved in the processing, storage or transmission of card holder data on behalf of another entity." This document attests to DocuSign's compliance with the current version of the PCI DSS as a service provider.

Attestation of Compliance (AOC) — Merchant

A merchant as defined by PCI is "any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (i.e., American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services." This document attests to DocuSign's compliance with the current version of the PCI DSS as a merchant with an eCommerce payment channel.

ASV Scan Report Attestation of Scan Compliance (PCI Executive Report)

PCI DSS requires regular vulnerability scanning of all DocuSign systems. This document confirms that DocuSign underwent vulnerability scanning by an approved scanning vendor (ASV) with no vulnerabilities found. The latest reports are from December 2022 and September 2022.

DocuSign and Client PCI Responsibilities Matrix

This document is provided to help our customers meet the PCI DSS requirement: "Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity." It outlines which PCI requirements are the responsibility of DocuSign and which are the responsibility of DocuSign's customers.

PCI Penetration Test

PCI DSS requires penetration testing, which attempts to exploit vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing is conducted by an independent third-party and is designed to evaluate the overall security posture associated with DocuSign logical security controls, which are intended to prevent unauthorized access and abuse of DocuSign information and assets. The testing approach included both internal and external tests at both the network and application layers for all systems in DocuSign's cardholder data environment. Segmentation checks completed to confirm that there is a separation between the CDE and NCDE environment.

Findings are remediated by DocuSign's assessment per its exposure and context of the vulnerabilities in line with DocuSign policy.

Continuous business operations

DocuSign is committed to making service available so that customers can access the DocuSign Agreement Cloud whenever they need it. Continuous business operations with recovery plans wherever necessary mean that customers aren't impacted by events beyond their control.

DocuSign eSignature maintains a scalable, high-performance, high-availability platform that provides continuous availability across the globe. Customers can count on our service to conduct their business on practically any device, from almost anywhere, at any time.

DocuSign eSignature is architected for zero data loss during catastrophic events and includes built-in redundancy. We perform secure replication of customer data at the data center in use as well as, in near real time, to geo-diverse data centers. All historical and document data is synchronized using a proprietary document replication service, which takes the place of traditional backups. We also maintain a disaster recovery plan to be implemented in the event of a disaster (or prolonged interruption of service) and a business continuity plan.

To further ensure our service is highly available—even during peak traffic—and scalable for future growth, we undertake robust capacity planning. The DocuSign eSignature platform runs below capacity to accommodate spikes in demand on our service, and we process approximately 12 terabytes of telemetry data per day to monitor and assess the end-to-end customer experience as one of multiple inputs for scalability planning.

Certificate of liability insurance

This Certificate of Insurance (COI) from Aon Risk Insurance Services for Liability describes DocuSign's coverage.

Customer data flow diagram

The data flow diagram demonstrates the way that data is securely managed as it traverses DocuSign's systems, starting from the end user to storage in secure DocuSign data centers.

eSignature Legality Guide

The DocuSign eSignature Legality Guide is the result of legal research into the laws and practices regarding e-signatures on a country-by-country basis. Each country-level analysis was conducted by local law firms located in that country, in that country's local language. This legal analysis was then supplemented with complementary research on e-signature and digital signature technology standards conducted by independent technology experts. Together, this information is provided as a public resource to understand e-signature legality and clarify some of the common misconceptions about international legality.

The legality guide can be found at https://www.docusign.com/how-it-works/legality/global.

DocuSign®

Reports and Attestations:

ISO 27001:2013

A-LIGN

DocuSign,Inc.
Certificate Number: ISMS-DO-110222

CERTIFICATE OF REGISTRATION

Information Security Management System
ISO/IEC 27001:2013

DocuSign,Inc.

999 Third Avenue, Suite 1800,
Seattle, Washington 98104
United States

A-LIGN Compliance and Security, Inc. certifies that the organization operates an Information Security Management System that conforms to the requirements of ISO/IEC 27001:2013. The scope and boundaries of the ISMS is as follows:

The scope of the ISO/IEC 27001:2013 certification includes the information security management system (ISMS) supporting DocuSign's Product Development, Engineering, Quality Assurance, Operations, Information Security, Business Continuity, Legal, Human Resources, Information Technology, Customer Service, and Datacenter Operations, and is aligned to the control requirements within ISO/IEC 27017:2015 and ISO/IEC 27018:2019.

The statement of applicability includes control objectives from the ISO/IEC 27001:2013 framework.

The statement of applicability additionally includes control objectives from the ISO 27017:2015 & ISO 27018:2019 framework.

Certificate	ISMS-DO-110222	**Original Certification Date**	December 21, 2011
Version	1.0	**Recertification Date**	November 18, 2020
Statement of Applicability	Version 0.29 (April 15, 2022)	**Expiry Date**	December 21, 2023
		Issuance Date	November 2, 2022

Authorized by:

Petar Besalev
EVP of Cybersecurity and Compliance

400 N Ashley Drive
Suite 1325
Tampa, FL 32602
888.702.5446
info@a-lign.com

A-LIGN.COM

A-LIGN

DocuSign,Inc.

ADDITIONAL LOCATION(S)	REGISTERED ACTIVITY
221 Main Street 15th Floor San Francisco, California 94105 United States	Corporate Headquarters supporting the areas of Product Development, Engineering, Quality Assurance, Operations, Security, Business Continuity, Legal, Human Resources, Information Technology, Customer Service Operations
180 North Lasalle Avenue Suite 600 Chicago, Illinois 60601 United States	Corporate Office Facility supporting the areas of Product Development, Engineering, Quality Assurance, Operations, Security, Business Continuity, Legal, Human Resources, Information Technology, Customer Service Operations
5 Hanover Quay Ground Floor Dublin, 2 Ireland	Corporate Office Facility supporting the areas of Product Development, Engineering, Quality Assurance, Operations, Security, Business Continuity, Legal, Human Resources, Information Technology, Customer Service Operations
4320 Winfield Road Suite 210 Warrenville, Illinois 70555 United States	Corporate Office Facility supporting the areas of Sales and Facilities Operations
Shiroyama Trust Tower 35F 4-3-1 Toranomon, Minato-ku Tokyo, 105-6035 Japan	Corporate Office Facility supporting the areas of Sales and Facilities Operations
Level 8 126 Phillip Street Sydney, New South Wales 2000 Australia	Corporate Office Facility supporting the areas of Sales and Facilities Operations
1 Ha'arava St. Floor 4 Givat Shmuel Israel	Corporate Office Facility supporting the areas of Product Development, Engineering, Quality Assurance, Operations, Security, Business Continuity, Legal, Human Resources, Information Technology, Customer Service Operations
9-15 rue Maurice Mallet Issy-les-Moulineaux, 92130 France	Corporate Office Facility supporting the areas of Product Development, Engineering, Quality Assurance, Operations, Security, Business Continuity, Legal, Human Resources, Information Technology, Customer Service Operations
Tower Bridge Corporate, 02° Andar Conj. 21, Avenida Jornalista Roberto Marinho, 85, São Paulo, Brazil 04576-010	Corporate Office Facility supporting the areas of Product Development,Finance, Global Operations, Technology and Security, Global Sales, Legal, Human Resources, Marketing, Product Development
Microsoft Azure Canada East (Quebec City); Canada Central (Toronto); Australia East (Sydney); United States; European Union	Cloud services provider

400 N Ashley Drive
Suite 1325
Tampa, FL 32602
888.702.5446
info@a-lign.com

A-LIGN.COM

A-LIGN

DocuSign,Inc.

ADDITIONAL LOCATION(S)	REGISTERED ACTIVITY
Cyxtera, Inc. United States	Data center hosting provider
Equinix Germany; Netherlands; France; United States; United Kingdom	Data center hosting provider
Switch, LTD United States	Data center hosting provider
T-Systems France; Germany	Infrastructure services of DocuSign eSignature in France and Germany
Sungard Availability Services United States	Data center hosting provider
Amazon Web Services Global	Cloud services provider
Vodafone Libertel B.V. Netherlands	Infrastructure services of DocuSign eSignature in the Netherlands

400 N Ashley Drive
Suite 1325
Tampa, FL 32602
888.702.5446
info@a-lign.com

A-LIGN.COM

Note this is just a restructured view so that it can fit into a document for customer visibility (The ISO references and mappings are the same but are just displayed in a single column)

Statement of Applicability of ISO/IEC 27001:2013/27017/27018, including Annex A Controls		
Version 0.29	**Scope Statement**	**As of April 15th 2022**
The scope of the ISO/IEC 27001:2013 certification includes the information security management system (ISMS) supporting DocuSign's Product Development, Engineering, Quality Assurance, Operations, Information Security, Business Continuity, Legal, Human Resources, Information Technology, Customer Service, and Datacenter Operations, and is aligned to the control requirements within ISO/IEC 27017: 2015 and ISO/IEC 27018:2019		

DCF ID	Control Domain	Control Short Name	DocuSign Control Language	ISO References	Justification for Inclusion
AM-01-01	Asset Management	Asset Inventory	DocuSign maintains an inventory of assets, which is reconciled on a periodic basis.	[27001] - A.8.1.1 [27001] - A.8.1.2 [27001] - A.8.2.2 [27017] - 8.1.1	Security Requirement
AM-01-02	Asset Management	Hardware Labels	DocuSign labels hardware prior to deployment.	[27001] - A.8.2.2	Security Requirement
AM-02-01	Asset Management	Asset Transportation	DocuSign documents and authorizes the transfer of systems (e.g., servers, network devices) between data center or office locations. Systems are packaged securely and transported in a secure, traceable manner. Storage media (e.g., HDDs) are not transported between data center or office locations.	[27001] - A.8.3.3 [27001] - A.11.2.5 [27001] - A.11.2.6 [27001] - A.13.2.1 [27018] - 13.2.1 [27018] - A.11.4	Security and Privacy Requirement
AM-03-01	Asset Management	Portable Media	DocuSign restricts the use of portable media in data centers.	[27001] - A.8.3.1 [27018] - A.11.5	Security and Privacy Requirement
AM-04-01	Asset Management	Asset Maintenance & Forensics	System maintenance, sanitization, and forensic activities are performed onsite under DocuSign supervision.	[27001] - A.11.2.4	Security Requirement
AM-06-02	Asset Management	Secure Disposal of Media	DocuSign securely destroys media authorized to be decommissioned or purges stored data from media authorized to be repurposed.	[27001] - A.8.3.2 [27001] - A.11.2.7 [27018] - 11.2.7	Security and Privacy Requirement
BC-01-01	Business Continuity	Business Continuity Plan	DocuSign's business continuity plans are reviewed and approved by the plan owner and management on an annual basis or upon material change. Plans are made available to relevant team members.	[27001] - A.17.1.1 [27001] - A.17.1.2	Security Requirement
BC-01-02	Business Continuity	Continuity Exercise	DocuSign performs business continuity and disaster recovery exercises on an annual basis and ensures the following: • exercises are executed with relevant teams • exercise results are documented • corrective actions are taken for exceptions noted • plans are updated based on results	[27001] - A.17.1.2 [27001] - A.17.1.3	Security Requirement
BC-01-03	Business Continuity	Business Impact Analysis	DocuSign maintains and biennially updates an inventory of departmental functions and their associated tolerance for downtime resulting from workforce productivity outages. A recovery priority is established for each inventoried function.	[27001] - A.17.1.1 [27001] - A.17.1.2	Security Requirement
BM-01-01	Backup Management	Data Replication	DocuSign replicates data to redundant, geographically dispersed data centers.	[27001] - A.12.3.1 [27001] - A.17.2.1 [27001] - A.18.1.3 [27018] - 12.3.1	Security and Privacy Requirement
BM-01-02	Backup Management	Data Backup	DocuSign performs backups of data to resume system operations in the event of a system failure.	[27001] - A.12.3.1 [27001] - A.18.1.3	Security Requirement
BM-02-01	Backup Management	Data Replication Testing	DocuSign monitors data replication jobs for failures that indicate a data integrity compromise.	[27001] - A.12.3.1 [27018] - 12.3.1 [27018] - A.11.3	Security and Privacy Requirement
BM-02-02	Backup Management	Data Backup Testing	DocuSign conducts restoration testing to confirm the reliability and integrity of system backups.	[27001] - A.12.3.1	Security Requirement
CFM-01-01	Configuration Management	Configuration Standard	DocuSign documents and maintains security hardening and baseline configurations according to industry standards, which are reviewed and updated on an annual basis.	[27001] - A.12.5.1	Security Requirement
CFM-02-01	Configuration Management	Configuration Standard Implementation	DocuSign configures systems in accordance with defined configuration standards.	[27017] - CLD.9.5.2	Security Requirement
CFM-02-04	Configuration Management	Time Clock Synchronization & Configuration	Systems are configured to synchronize information system time clocks based on authorized time sources; access to modify time data is restricted to authorized personnel.	[27001] - A.12.4.4	Security Requirement

CG-01-04	Corporate Governance	Organizational Structure	The company has established appropriate lines of reporting, which are documented and maintained in organizational charts.	[27001] - 5.3	Security Requirement
CG-02-01	Corporate Governance	Policy Management	DocuSign's policies, which define roles and responsibilities that support company objectives, are periodically reviewed, approved by management, and communicated to DocuSign personnel.	[27001] - 5.1 [27001] - 5.2 [27001] - 5.3 [27001] - 6.2 [27001] - 7.3 [27001] - 7.5.2 [27001] - 7.5.3 [27001] - 8.1 [27001] - A.5.1.1 [27001] - A.5.1.2 [27001] - A.6.1.1 [27001] - A.6.2.2 [27001] - A.9.1.1 [27001] - A.10.1.1 [27001] - A.10.1.2 [27001] - A.11.2.9 [27001] - A.12.5.1 [27001] - A.13.2.1 [27001] - A.18.2.2 [27017] - CLD.6.3.1 [27017] - CLD.12.1.5 [27018] - 5.1.1 [27018] - A.10.2	Security and Privacy Requirement
CG-02-01 (01)	Corporate Governance	Acceptable Use Standard	DocuSign communicates acceptable uses of software and systems via an Acceptable Use Standard, which is made available to all employees.	[27001] - A.6.2.1 [27001] - A.8.1.3 [27001] - A.9.3.1 [27001] - A.11.2.6 [27001] - A.11.2.8 [27001] - A.11.2.9 [27001] - A.12.6.2 [27001] - A.18.1.2 [27018] - A.11.2 [27018] - A.11.7	Security and Privacy Requirement
CG-02-01 (03)	Corporate Governance	Information Security Policy	DocuSign maintains an Information Security Policy aligned to the purpose of the organization, and outlines the following: • information security objectives • commitment to information security requirements • evaluation of information security effectiveness and operation • continual improvement of the information security program	[27001] - 5.1 [27001] - 5.2 [27001] - 5.3 [27001] - 6.2 [27001] - 7.3 [27001] - 7.5.1 [27001] - 8.1 [27001] - 9.1 [27001] - 10.2 [27001] - A.7.2.1 [27017] - 5.1.1 [27017] - CLD.12.1.5	Security Requirement
CG-02-01 (04)	Corporate Governance	Document Retention Policy	Document retention periods are documented, periodically updated, and made available to DocuSign personnel.	[27001] - A.18.1.3 [27018] - A.10.2	Security and Privacy Requirement
CG-02-01 (07)	Corporate Governance	Data Classification Standard	DocuSign defines information classification and categorization levels to facilitate the appropriate protection of data.	[27001] - A.8.2.1 [27001] - A.8.2.2	Security Requirement
CG-02-01 (08)	Corporate Governance	Data Handling Standard	DocuSign determines the minimum security and privacy safeguards and requirements for data handling throughout the data lifecycle.	[27001] - A.8.2.3 [27001] - A.18.1.3 [27001] - A.18.1.4	Security Requirement

CG-02-01 (09)	Corporate Governance	Compliance Standard	DocuSign maintains an ISMS Policy to govern the DocuSign ISMS, which outlines the following: • scope, purpose, and intended outcome • internal and external issues relevant to the ISMS purpose • interested parties and their requirements • adherence to information security objectives • ISMS resources • internal and external communications • interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations • roles and authorities	[27001] - 4.1 [27001] - 4.2 [27001] - 4.3 [27001] - 4.4 [27001] - 5.1 [27001] - 5.3 [27001] - 7.4 [27001] - 7.5.1 [27001] - A.6.1.1	Security Requirement
CG-02-01 (10)	Corporate Governance	Incident Management Standard	DocuSign defines the procedures required to manage, track, and report incidents, including: • procedures for the identification and management of incidents • procedures for the resolution of confirmed incidents • key incident response systems • incident coordination and communication strategy • contact method for internal parties to report incidents • support team contact information • notification to relevant management in the event of a security breach • provisions for reviewing, approving, updating, and communicating the plan • provisions for training of support team • preservation of incident information • coordination with business continuity activities • metrics for measuring incident response capabilities	[27001] - A.16.1.1 [27001] - A.16.1.2 [27001] - A.16.1.7 [27018] - 16.1.1	Security and Privacy Requirement
CG-02-01 (11)	Corporate Governance	Secure Development Lifecycle Standard	Requirements for the secure development, modification, and maintenance of DocuSign software are governed via the DocuSign SDLC Policy, and include: • secure development guidelines • code repository and version control • security checkpoints within the project milestones • development and test environment separation • credit card and transactional data security • release timelines	[27001] - A.6.1.5 [27001] - A.14.2.1 [27001] - A.14.2.5	Security Requirement
CG-02-02	Corporate Governance	Work Instructions	DocuSign's supports critical business functions with procedural documentation, which is made available to authorized personnel.	[27001] - A.11.1.5 [27001] - A.12.1.1 [27001] - A.12.5.1 [27001] - A.17.1.2 [27017] - CLD.12.1.5	Security Requirement
CG-03-03	Corporate Governance	ISMS Review	The ISMS Owner conducts a formal management review of the DocuSign ISMS on an annual basis; key decisions relating to continual improvement and ISMS changes are documented and actioned. At a minimum, the review includes: • the status of actions from previous management reviews • changes in external and internal issues that are relevant to the information security management system • feedback on the information security performance, including trends in: - nonconformities and corrective actions - monitoring and measurement results - audit results • fulfillment of information security objectives • feedback from interested parties • results of risk assessment and status of risk treatment plan • opportunities for continual improvement	[27001] - 4.4 [27001] - 8.1 [27001] - 9.3 [27001] - 10.2	Security Requirement
CG-03-04	Corporate Governance	ISO Statement of Applicability	Management prepares a statement of applicability that includes control objectives, implemented controls, and business justification for excluded controls. Management aligns the statement of applicability with the results of the annual risk assessment.	[27001] - 6.1.3 [27001] - 7.5.1	Security Requirement
CG-03-05	Corporate Governance	Information Security & Privacy Resources	Resources required to support DocuSign's information security and privacy programs are reviewed with a financial business partner and consolidated for approval by the DocuSign FP&A team.	[27001] - 5.1 [27001] - 6.2 [27001] - 7.1	Security Requirement
CG-04-02	Corporate Governance	Privacy Impact Assessment	DocuSign performs privacy impact assessments of major product releases to: • identify high-risk processing activities that impact DocuSign personally identifiable information • determine lawful basis of processing • track non-compliance with DocuSign privacy practices through remediation	[27001] - A.18.1.4 [27018] - A.3.1 [27018] - A.3.2	Security and Privacy Requirement

CG-04-06	Corporate Governance	Internal & External Privacy Notice	DocuSign publishes privacy notices for consumption by internal and external parties. At a minimum, the notices include: • description and purpose of collected personal information (PI) • purpose(s) for sharing collected PI • activities that impact individual privacy such as collection, use, sharing, maintenance, sale, and return/transfer/disposal • authority to collect PI • available choices and subsequent consequences to individuals regarding how their PI is processed or shared • individual ability to access or correct PI • how PI is protected • DocuSign's management of PII disclosure requests • relevant contact information	[27018] - A.6.1 [27018] - A.8.1 [27018] - A.10.3 [27018] - A.11.11	Privacy Requirement
CG-04-06 (01)	Corporate Governance	Internal & External Privacy Notice: Subprocessor List	DocuSign publishes a listing of subprocessor names including their country of processing, provides a subscription mechanism to alert external parties of subprocessor changes, and makes available information regarding an individual's right to object to a subprocessor.	[27018] - A.8.1	Privacy Requirement
CG-04-07	Corporate Governance	Record of Disclosure	DocuSign maintains records of authorized and unauthorized data disclosures which capture the following: • date, nature, and disclosure purpose • name and address of the entity to which the disclosure was made • PII involved	[27018] - A.6.2	Privacy Requirement
CG-04-07 (03)	Corporate Governance	Record of Disclosure: Subpoena Notice	Unless otherwise prohibited, DocuSign provides notice to DocuSign customers regarding legally-binding requests from law enforcement agencies.	[27018] - A.6.1	Privacy Requirement
CG-05-01	Corporate Governance	Employee Agreements	DocuSign employees consent to a confidentiality agreement, mobile device policy, and code of conduct.	[27001] - A.7.1.2 [27001] - A.7.3.1 [27001] - A.13.2.4 [27018] - A.11.1	Security and Privacy Requirement
CG-05-02	Corporate Governance	Non-employee Agreements	DocuSign contingent workers, agency contractors, and independent contractors consent to a confidentiality or non-disclosure agreement, mobile device policy, and code of conduct.	[27001] - A.7.1.2 [27001] - A.7.3.1 [27001] - A.13.2.2 [27001] - A.13.2.4 [27018] - A.11.1	Security and Privacy Requirement
CG-05-03	Corporate Governance	Visitor Agreements	DocuSign visitors consent to a non-disclosure agreement.	[27001] - A.13.2.4	Security Requirement
CG-05-05	Corporate Governance	Employee Confidentiality Agreement Review	DocuSign's employee confidentiality contract provisions are reviewed on a as-needed basis.	[27001] - A.13.2.4	Security Requirement
CG-05-06	Corporate Governance	Non-employee Confidentiality Agreement Review	DocuSign’s non-disclosure agreement is reviewed on a periodic basis.	[27001] - A.13.2.4	Security Requirement
CG-07-01	Corporate Governance	Software Usage Restrictions	Software installed within the DocuSign network is procured lawfully via authorized channels. DocuSign monitors software usage against contractual commitments to maintain compliance.	[27001] - A.18.1.2	Security Requirement
CG-08-01	Corporate Governance	Legal Inquiries	DocuSign reviews legal-related inquiries, complaints, and disputes.	[27017] - 18.1.2	Security Requirement
CG-08-02	Corporate Governance	Privacy Inquiries	DocuSign reviews privacy-related inquiries, complaints, and disputes.	[27001] - A.18.1.4 [27018] - 6.1.1	Security and Privacy Requirement
CG-08-03	Corporate Governance	Public Incident Reporting Channel	DocuSign provides a contact method for external parties to report incidents.	[27017] - 16.1.2	Security Requirement
CHM-01-01	Change Management	Change Management Workflow	Change scope, change type, and roles and responsibilities are pre-established within DocuSign's change control workflow. The following documentation is required, where applicable, for a change to be approved and committed into the DocuSign live environment: • change description • impact of change • test results • back-out plan • independent code review • change implementor • validation steps & success criteria	[27001] - 8.1 [27001] - A.6.1.2 [27001] - A.12.1.2 [27001] - A.12.6.2 [27001] - A.14.2.2 [27001] - A.14.2.3 [27001] - A.14.2.4 [27001] - A.18.1.5	Security Requirement

CHM-01-02	Change Management	Pre-release Testing	DocuSign performs pre-release testing for code changes to validate that proposed changes meet business requirements.	[27001] - A.14.2.7 [27001] - A.14.2.8 [27001] - A.14.2.9	Security Requirement
CHM-01-04	Change Management	Server Acceptance Review	Prior to deployment, systems must pass a security acceptance review, which identifies unsafe or unauthorized configurations, including default vendor credentials.	[27001] - A.14.1.1 [27017] - CLD.13.1.4	Security Requirement
DM-02-01	Data Management	Personal Information Access & Update	DocuSign provides authorized data subjects the ability to access, correct, amend, restrict, or delete their stored personal information.	[27018] - A.2.1	Privacy Requirement
DM-03-01	Data Management	Non-production Data	PII and customer data including documents and envelopes are not used for testing purposes nor stored on non-production systems.	[27001] - A.14.3.1 [27018] - 12.1.4 [27018] - A.3.2	Security and Privacy Requirement
DM-04-01	Data Management	Encryption of Data in Transit	DocuSign's transmission of data over public networks is encrypted.	[27001] - A.13.2.1 [27001] - A.13.2.3 [27001] - A.14.1.2 [27001] - A.14.1.3 [27001] - A.18.1.4 [27018] - A.11.6 [27018] - A.12.2	Security and Privacy Requirement
DM-04-02	Data Management	Encryption of Data at Rest	DocuSign encrypts sensitive data including uploaded documents and their associated form data and signatures at rest.	[27001] - A.18.1.4 [27017] - CLD.9.5.1 [27018] - A.11.4	Security and Privacy Requirement
DM-06-01	Data Management	Data Storage Allocation	Allocated data storage space does not contain or make visible previously residing information.	[27018] - A.11.13	Privacy Requirement
DM-06-02	Data Management	Product Activity Logs	Logs of user activity and application events are made available to the user.	[27017] - 12.4.1 [27017] - CLD.12.4.5 [27018] - 12.4.1	Security and Privacy Requirement
DM-06-08	Data Management	Information and Asset Tagging	DocuSign provides users the ability to tag information and assets (e.g., envelopes, documents, and fields) with customer-defined values that are retained with the tagged information or asset.	[27017] - 8.2.2	Security Requirement
DM-07-03	Data Management	Envelope Purge	Account administrators are provided with functionality to automatically purge selected envelope documents, including their fields and contents. Account administrators have the option to redact sensitive information prior to the purge, and additionally configure recurring envelope purge activities against a defined schedule.	[27017] - CLD.8.1.5 [27018] - A.2.1	Security and Privacy Requirement
DM-07-06	Data Management	Expired Data	On a periodic basis, DocuSign identifies and securely deletes stored data that exceeds retention requirements.	[27017] - CLD.8.1.5	Security Requirement
DM-07-09	Data Management	Hardcopy Materials	DocuSign provides secured disposal bins within DocuSign offices to facilitate the secure destruction of hardcopy materials.	[27018] - A.11.7	Privacy Requirement
IAM-01-01	Identity & Access Management	Logical Access Provisioning	Logical access provisioning to information systems is based on the concept of least privilege and requires approval from authorized personnel prior to provisioning system access; permissions are granted based on the documented and approved access request.	[27001] - A.6.1.2 [27001] - A.9.1.2 [27001] - A.9.2.2 [27001] - A.9.2.3 [27001] - A.9.4.1 [27001] - A.9.4.4 [27001] - A.14.2.6 [27001] - A.18.1.3 [27017] - CLD.9.5.1 [27018] - A.11.9	Security and Privacy Requirement
IAM-01-02	Identity & Access Management	Logical Access De-provisioning	Logical access that is no longer required in the event of a termination is documented, communicated to management, and revoked.	[27001] - A.9.2.6	Security Requirement
IAM-01-03	Identity & Access Management	Logical Access Review	DocuSign performs account and access reviews on a periodic basis; corrective action is taken where applicable.	[27001] - A.9.2.5 [27018] - A.11.9	Security and Privacy Requirement
IAM-02-01	Identity & Access Management	Unique Identifiers	DocuSign requires unique identifiers for user accounts and prevents identifier reuse.	[27001] - A.9.2.1 [27001] - A.9.4.2 [27018] - A.11.8 [27018] - A.11.10	Security and Privacy Requirement
IAM-02-02	Identity & Access Management	Internal User Authentication	Access to the DocuSign live environment is restricted to identified and authenticated accounts. User and device authentication to DocuSign's internal information systems is protected by passwords that meet DocuSign's password complexity requirements.	[27001] - A.9.4.2 [27001] - A.9.4.3	Security Requirement

IAM-02-03	Identity & Access Management	Customer Authentication	DocuSign applications secure user data and maintain confidentiality by default or according to permissions set by the individual; DocuSign authenticates individuals with unique identifiers and passwords prior to enabling access to the application or their data.	[27017] - CLD.9.5.1 [27017] - CLD.12.4.5 [27018] - 9.4.2	Security and Privacy Requirement
IAM-02-03 (01)	Identity & Access Management	Customer Authentication: Account Management	DocuSign maintains a user registration and de-registration process and provides functionality for customer administrators to manage identity and access permissions including authentication configurations within their account.	[27017] - 9.2.1 [27017] - 9.2.2 [27017] - 9.2.3 [27017] - 9.4.1 [27018] - 9.2.1 [27018] - 9.2.2 [27018] - 9.2.3 [27018] - 9.2.6 [27018] - A.11.10	Security and Privacy Requirement
IAM-02-03 (02)	Identity & Access Management	Customer Authentication: Strong Authentication	Strong authentication mechanisms can be enabled by customers within their account.	[27017] - 9.2.3	Security Requirement
IAM-02-04	Identity & Access Management	Multifactor Authentication	Multi-factor authentication is required for: • remote VPN sessions • access to live environments	[27001] - A.9.4.2	Security Requirement
IAM-02-05	Identity & Access Management	Authentication Credential Maintenance	Authorized personnel verify the identity of users before initially provisioning, updating, or facilitating the modification of authentication credentials on their behalf.	[27001] - A.9.2.4	Security Requirement
IAM-02-06	Identity & Access Management	System Session Timeout	DocuSign configures systems to disconnect sessions and mask the user interface after 15 minutes of inactivity. Users must re-authenticate to the session prior to continued use, or may terminate the session by closing the session window or disconnecting from the DocuSign VPN.	[27001] - A.11.2.8	Security Requirement
IAM-03-01	Identity & Access Management	Source Code Security	Access to modify source code is restricted to authorized personnel.	[27001] - A.9.4.5	Security Requirement
IAM-03-03	Identity & Access Management	Shared Logical Account Restrictions	DocuSign prohibits the use of non-emergency default and shared accounts to administer systems or perform privileged functions.	[27001] - A.9.2.3	Security Requirement
IAM-04-01	Identity & Access Management	Virtual Private Network	Remote access to DocuSign networks is accessed via VPN through managed network access control points.	[27001] - A.6.2.2 [27001] - A.11.2.6	Security Requirement
IR-01-02	Incident Response	Incident Response	Confirmed incidents are assigned a priority level, investigated, and resolved.	[27001] - 8.1 [27001] - A.16.1.4 [27001] - A.16.1.5 [27001] - A.16.1.7	Security Requirement
IR-01-02 (02)	Incident Response	Incident Response: Recurrence Prevention	DocuSign performs a root cause analysis for high degradation incidents to detect and correct or prevent prior incidents from recurring.	[27001] - A.16.1.6	Security Requirement
IR-02-01	Incident Response	Incident Communication Requirements	DocuSign maintains external communication requirements for incidents, including: • external party notification requirements and contact information (e.g., law enforcement, regulatory bodies, customers, public/media) • criteria to notify • references to incident response procedures from the payment brands	[27001] - A.6.1.3 [27018] - A.10.1	Security and Privacy Requirement
IR-02-02	Incident Response	Incident Communication	In accordance with defined notification requirements, DocuSign communicates incident information to external stakeholders.	[27018] - A.10.1	Privacy Requirement
KM-01-01	Key Management	Key Repository Access	Access to the cryptographic keystores is limited to authorized personnel.	[27001] - A.10.1.2	Security Requirement
KM-02-01	Key Management	Data Encryption Key Lifecycle	DocuSign manages data encryption keys in accordance with the following: • generation of strong cryptographic keys • secure distribution and storage methods • conditions for retirement, replacement, and compromise • split knowledge and dual control for clear-text key management operations • control over unauthorized substitution	[27001] - A.10.1.2	Security Requirement
MDM-01-01	Mobile Device Management	Mobile Device Enrollment	Authorized DocuSign personnel must enroll mobile devices with the enterprise mobile device management program prior to obtaining access to DocuSign resources from mobile devices.	[27001] - A.6.2.1	Security Requirement
NO-01-01	Network Operations	Network Policy Enforcement Points	Network traffic to and from untrusted networks passes through a DMZ; firewall rules are established in accordance to identified security requirements and business justifications.	[27001] - A.13.1.1 [27001] - A.13.1.2 [27001] - A.13.1.3	Security Requirement

NO-02-01	Network Operations	Production Network Segmentation	Production environments are: • segregated from corporate environments • logically separated from the staging environment	[27001] - A.12.1.4 [27001] - A.13.1.3	Security Requirement
NO-02-04	Network Operations	Network Segregation	Networks are internally segregated by function.	[27017] - 13.1.3	Security Requirement
PR-01-01	People Resources	Background Checks	In accordance with applicable law, DocuSign employees and contingent workers are required to pass a background check as a condition of their employment.	[27001] - A.7.1.1	Security Requirement
PR-01-02	People Resources	Performance Management	DocuSign's employees and managers complete an annual assessment of employee performance. The assessment results are collaboratively reviewed between both parties to maintain alignment on role responsibilities and individual goals.	[27001] - 7.2	Security Requirement
PR-01-03	People Resources	Interviews	DocuSign employees are interviewed for relevant experience and competence as a condition of their employment.	[27001] - 7.2	Security Requirement
PR-02-01	People Resources	DocuSign Property Collection	Upon employee termination, management collects DocuSign property from the terminated employee.	[27001] - A.8.1.4	Security Requirement
PR-03-01	People Resources	Disciplinary Process	Employees that fail to comply with DocuSign policies are subject to a disciplinary process.	[27001] - A.7.2.3	Security Requirement
RM-01-01	Risk Management	Security Risk Assessment	DocuSign performs an annual security and privacy risk assessment.	[27001] - 6.1.1 [27001] - 6.1.2 [27001] - 6.1.3 [27001] - 8.2	Security Requirement
RM-01-03	Risk Management	Information Security Threat Model	DocuSign assesses the security posture of systems to determine information security risk and, if applicable, provides remediation recommendations. Findings for systems are tracked as risks within the information security risk register.	[27001] - A.6.1.5 [27001] - A.14.1.1 [27018] - A.5.1	Security and Privacy Requirement
RM-02-01	Risk Management	Remediation Plan	Management prepares a remediation plan to manage the resolution of nonconformities identified.	[27001] - 6.1.3 [27001] - 8.3 [27001] - 10.1	Security Requirement
RM-02-02	Risk Management	Information Security Risk Register	DocuSign maintains a risk register to track information security risk through its lifecycle. Documented remediation plans indicate whether the risk will be mitigated or accepted. Risk acceptance requires a documented business justification and communication to management.	[27001] - 6.1.2 [27001] - 6.1.3 [27001] - 8.3	Security Requirement
RM-03-01	Risk Management	Compliance Assessment	DocuSign establishes internal audit requirements based on the established control framework and executes audits on information systems and processes at planned intervals.	[27001] - 8.1 [27001] - 9.2 [27001] - A.12.7.1 [27001] - A.18.2.1	Security Requirement
RM-05-01	Risk Management	Control Framework	DocuSign maintains a control framework containing documented control responsibilities that mitigates risk and aligns business processes with compliance objectives.	[27001] - A.18.1.1	Security Requirement
RM-05-05	Risk Management	Legal Register	DocuSign maintains and periodically updates a list of applicable laws and regulations relating to the security of DocuSign's services.	[27001] - A.18.1.1 [27001] - A.18.1.5	Security Requirement
SDD-02-03	System Design Documentation	Product Implementation Documentation	DocuSign provides documentation to customers regarding: • envelope and document tagging • initial user registration and de-registration • ongoing identity and access management • strong authentication options • protection and distribution of authentication information • security practices and cryptographic mechanisms implemented by DocuSign or made available to customers which are used to protect customer data • NTP settings including how customers can sync with DocuSign-leveraged time sources • secure development practices • compliance with applicable legal jurisdictions • backup/replication and restoration capabilities implemented by DocuSign or made available to customers • certification of completion and envelope history logs	[27017] - 8.2.2 [27017] - 9.2.1 [27017] - 9.2.2 [27017] - 9.2.4 [27017] - 10.1.1 [27017] - 12.3.1 [27017] - 12.4.4 [27017] - 14.1.1 [27017] - 14.2.1 [27017] - 18.1.1 [27017] - 18.1.3 [27017] - 18.1.5 [27018] - 10.1.1 [27018] - 12.3.1 [27018] - 12.4.1	Security and Privacy Requirement
SDD-02-04	System Design Documentation	System Availability & Uptime	The geographical processing locations, availability, and uptime of DocuSign services are maintained and made publicly available.	[27017] - 6.1.3 [27017] - CLD.12.4.5 [27018] - A.12.1	Security and Privacy Requirement
SDD-02-05	System Design Documentation	Product Alerts	DocuSign makes available information regarding: • product and service updates • technical vulnerabilities	[27017] - 12.1.2 [27017] - 12.6.1 [27017] - 16.1.2	Security Requirement

SDD-02-06	System Design Documentation	Security Questionnaires & Independent Assurance Reports	Upon request, DocuSign completes security and privacy questionnaires and provides independent assurance reports to customers to demonstrate the operating effectiveness of information security controls.	[27017] - 18.2.1 [27018] - A.12.1 [27018] - 18.2.1	Security and Privacy Requirement
SDLC-01-02	Service Lifecycle	Development Environment	The development and modification of software is performed in development environments.	[27001] - A.14.2.6	Security Requirement
SDLC-02-01	Service Lifecycle	Source Code Management	Source code is managed with approved version control mechanisms.	[27001] - A.14.2.7	Security Requirement
SM-01-01	Systems Monitoring	Audit Log Access	DocuSign stores system logs in a secure repository, disables privileges to delete or modify audit logs, and restricts access to audit logs to authorized personnel.	[27001] - A.12.4.1 [27001] - A.12.4.3 [27018] - 12.4.2	Security and Privacy Requirement
SM-01-02	Systems Monitoring	Audit Log Capacity & Retention	DocuSign retains audit log data for 1 year and ensures 90 days of data is immediately available for analysis; additional storage capacity is allocated as necessary.	[27018] - 12.4.2	Privacy Requirement
SM-02-01	Systems Monitoring	System Logging	DocuSign logs critical information system activity.	[27001] - A.9.4.4 [27001] - A.12.4.1 [27001] - A.12.4.3 [27017] - CLD.9.5.2	Security Requirement
SM-03-01	Systems Monitoring	Security Monitoring Alert Criteria	DocuSign defines security monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel to receive and respond to alerts.	[27001] - A.9.4.4 [27001] - A.12.4.1 [27001] - A.12.4.3	Security Requirement
SM-03-01 (02)	Systems Monitoring	Security Monitoring Alert Criteria: Tampering Detection	DocuSign defines security monitoring alert criteria to detect tampering of logging and monitoring tools.	[27001] - A.12.4.2	Security Requirement
SM-04-01	Systems Monitoring	Security Monitoring	Critical systems are monitored in accordance to predefined security criteria and alerts are sent to authorized personnel.	[27001] - A.9.4.4 [27001] - A.12.4.1 [27001] - A.12.4.3	Security Requirement
SM-06-01	Systems Monitoring	Capacity Planning	Capacity planning and analysis is periodically performed by DocuSign management to maintain the reliability, performance, and capacity of systems required for the operation of DocuSign's live environment.	[27001] - A.12.1.3	Security Requirement
SM-06-02	Systems Monitoring	Availability Monitoring Alert Criteria	DocuSign defines availability monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	[27001] - A.12.1.3	Security Requirement
SM-06-03	Systems Monitoring	Availability Monitoring	Critical systems are monitored in accordance to predefined availability criteria and alerts are sent to authorized personnel.	[27001] - A.12.1.3 [27001] - A.17.2.1	Security Requirement
SM-07-01	Systems Monitoring	Data Loss Prevention	DocuSign maintains a data loss prevention program to monitor outbound email and workstation-connected media for unauthorized transfers of information. Privileged user workstations are restricted from writing to workstation-connected media.	[27001] - A.6.2.2 [27001] - A.8.3.1 [27018] - A.11.5	Security and Privacy Requirement
SO-01-01	Site Operations	Secured Facility	Physical access to restricted areas of the facility is protected by walls with non-partitioned ceilings, secured entry points, and/or staffed reception desks.	[27001] - A.11.1.1 [27001] - A.11.1.3 [27001] - A.11.1.4 [27001] - A.11.1.5 [27001] - A.11.1.6 [27001] - A.11.2.1	Security Requirement
SO-02-01	Site Operations	Physical Access Provisioning	Physical access provisioning requires management approval and documented specification of: • access privileges granted • intended business purpose • access start date • access duration	[27001] - A.9.2.2 [27001] - A.11.1.2	Security Requirement
SO-02-01 (01)	Site Operations	Physical Access Provisioning: Visitor Access	Visitors, who are not data center personnel, are authorized and assigned an escort prior to entering the facility.	[27001] - A.11.1.2	Security Requirement
SO-02-02	Site Operations	Physical Access De-provisioning	Physical access that is no longer required in the event of a termination is revoked. If applicable, temporary badges are returned prior to exiting facility.	[27001] - A.9.2.6 [27001] - A.11.1.2	Security Requirement
SO-02-03	Site Operations	Physical Access Review	DocuSign performs physical account and access reviews on a quarterly basis; corrective action is taken where applicable.	[27001] - A.11.1.2	Security Requirement
SO-03-01	Site Operations	Temperature & Humidity Control	Temperature and humidity levels of data center environments are monitored and maintained at appropriate levels. The design and function of relevant equipment is certified at appropriate intervals.	[27001] - A.11.1.4 [27001] - A.11.2.1 [27001] - A.11.2.2	Security Requirement

SO-03-02	Site Operations	Fire Suppression Systems	Fire suppression systems are implemented to protect critical infrastructure in accordance with the following: • powered via resilient or independent energy source • emergency responders are automatically contacted when fire detection systems are activated • the design and function of fire detection and suppression systems are maintained at appropriate intervals	[27001] - A.11.1.4 [27001] - A.11.2.1	Security Requirement
SO-03-03	Site Operations	Power Failure Protection	DocuSign employs uninterruptible power supplies (UPS) and generators to support critical systems in the event of a power disruption or failure. The design and function of relevant equipment is certified at appropriate intervals.	[27001] - A.11.2.2	Security Requirement
SO-04-01	Site Operations	Physical Cable Protection	DocuSign power and telecommunication lines are protected from interference, interception, and damage.	[27001] - A.11.2.3	Security Requirement
TA-01-01	Training & Awareness	General Security Awareness Training	On an annual basis, DocuSign employees complete security and privacy awareness training. Records of training completion are managed within DocuSign's Learning Management System.	[27001] - 5.1 [27001] - 7.2 [27001] - 7.3 [27001] - A.7.2.1 [27001] - A.7.2.2 [27001] - A.16.1.2 [27001] - A.16.1.3 [27001] - A.18.2.2	Security Requirement
TA-01-03	Training & Awareness	Privacy Training	DocuSign requires individuals with the ability to access or transfer PII or PHI to complete privacy training. The training includes consequences for mishandling sensitive data.	[27018] - 7.2.2 [27018] - A.11.1	Privacy Requirement
TPM-01-02	Third Party Management	Supplier Risk Assessment	DocuSign performs a risk assessment and reviews the security and privacy practices of suppliers who access, collect, process, transfer, or store data on behalf of DocuSign; non-compliance is tracked through remediation.	[27001] - 8.1	Security Requirement
TPM-01-03	Third Party Management	Supplier Independent Assurance Review	On a periodic basis, DocuSign reviews controls within third party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address any impact the disclosed gaps have on the organization.	[27001] - A.13.1.2 [27001] - A.15.2.1	Security Requirement
TPM-02-01	Third Party Management	Third Party Contracts	DocuSign enters into Master Service Agreements with third parties, including Data Protection and Information Security Attachments, for the collection, processing, transfer, or storage of data by, or on behalf of, DocuSign. The agreement imposes third party roles and responsibilities which support DocuSign's information security and confidentiality objectives.	[27001] - A.13.1.2 [27001] - A.13.2.2 [27001] - A.13.2.4 [27001] - A.14.1.1 [27001] - A.14.2.7 [27001] - A.15.1.1 [27001] - A.15.1.2 [27001] - A.15.1.3 [27001] - A.15.2.2 [27017] - 6.1.1 [27017] - 15.1.3 [27018] - A.11.12	Security and Privacy Requirement
TPM-02-02	Third Party Management	Customer Contracts	DocuSign enters into Master Service Agreements with customers, including Data Protection and Information Security Attachments, for the collection, processing, transfer, or storage of data by, or on behalf of, DocuSign. The agreement imposes customer roles and responsibilities which support DocuSign's information security and confidentiality objectives.	[27017] - 6.1.1 [27017] - 15.1.2 [27017] - 16.1.1 [27017] - CLD.6.3.1 [27018] - A.3.1 [27018] - A.6.1 [27018] - A.10.1 [27018] - A.10.3 [27018] - A.11.1 [27018] - A.11.11	Security and Privacy Requirement
TPM-02-03	Third Party Management	Network Service Level Agreements (SLA)	Suppliers which provide networking services to DocuSign are contractually bound to provide secure and available services as documented in SLAs.	[27001] - A.13.1.2	Security Requirement
VM-02-01	Vulnerability Management	Penetration Test	DocuSign facilitates a penetration test, which validates network segmentation, on an annual basis.	[27001] - A.12.6.1 [27001] - A.18.2.3	Security Requirement
VM-03-01	Vulnerability Management	Infrastructure Patch Management	DocuSign performs monthly system security scans to identify vulnerable software or firmware.	[27001] - A.12.6.1 [27001] - A.18.2.3 [27017] - CLD.9.5.2 [27017] - CLD.13.1.4	Security Requirement

VM-04-01	Vulnerability Management	Enterprise Antivirus	DocuSign has managed enterprise antivirus deployments and ensures the following: • signature definitions are updated automatically • scans are scheduled to run on a periodic basis • audit logs are forwarded to a centralized repository • alerts are reviewed and resolved by authorized personnel • real-time scanning is performed on files received from external sources	[27001] - A.12.2.1 [27017] - CLD.9.5.2	Security Requirement
VM-05-01	Vulnerability Management	Static Code Analysis	DocuSign conducts source code vulnerability scans on a periodic basis.	[27001] - A.12.6.1 [27001] - A.14.2.9	Security Requirement
VM-05-02	Vulnerability Management	Dynamic Application Scans	On a recurring basis, DocuSign conducts dynamic vulnerability scans against web applications prior to deployment into live environments.	[27001] - A.12.6.1 [27001] - A.14.2.9 [27018] - A.11.13	Security and Privacy Requirement
VM-05-03	Vulnerability Management	Third Party Library Check	DocuSign scans its codebase for open source software vulnerabilities on a periodic basis.	[27001] - A.12.6.1	Security Requirement
VM-06-03	Vulnerability Management	Information Security Contacts	DocuSign maintains contact information with external parties associated with the interest of information security.	[27001] - A.6.1.4	Security Requirement
VM-07-01	Vulnerability Management	Workstation Monitoring	Workstations are monitored to identify security vulnerabilities.	[27001] - A.6.2.2	Security Requirement
VM-09-01	Vulnerability Management	Vulnerability Remediation	DocuSign assigns a risk rating to identified vulnerabilities and prioritizes remediation of legitimate vulnerabilities according to the assigned risk.	[27001] - A.12.6.1	Security Requirement

Reports and Attestations:

AICPA SOC 2 Type II Report

DocuSign®

Report on DocuSign, Inc.'s Description of Its eSignature System and on the Suitability of the Design and Operating Effectiveness of its Controls Relevant to Security, Availability, and Confidentiality throughout the period November 1, 2021 to October 31, 2022

Prepared in Accordance with AICPA AT-C 205, and criteria set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria) and DC 200, Description Criteria for a Description of a Service Organization's System in a SOC 2 Report.

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign®

Table of Contents

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign®

Section I – Report of Independent Service Auditors

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

Report of Independent Service Auditors

To the Management of DocuSign, Inc.

Scope

We have examined DocuSign, Inc.'s (the "Service Organization") accompanying description of its eSignature system (the "system") titled "DocuSign's Description of Its eSignature System" throughout the period November 1, 2021 to October 31, 2022 ("description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout that period, to provide reasonable assurance that the Service Organization'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 information included in Section V, "Other Information Provided by DocuSign, Inc. That is Not Covered by the Service Auditors' Report" is presented by management of the Service Organization to provide additional information and is not a part of the description. Information about the Service Organization's management response to exceptions has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve the Service Organization's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

The Service Organization uses subservice organizations to provide Information Technology General Controls (ITGCs) related to server hosting and cloud services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Service Organization, to achieve the Service Organization's service commitments and system requirements based on the applicable trust services criteria. The description presents the Service Organization's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Service Organization's controls. The description 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.

Service organization's responsibilities

The Service Organization 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 Service Organization's service commitments and system requirements were achieved. In Section II, the Service Organization has provided the accompanying assertion titled "Management of DocuSign, Inc.'s Assertion" ("assertion"), about the description and the suitability of the design and operating effectiveness of controls stated therein. The Service Organization is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service auditors' responsibilities

PricewaterhouseCoopers LLP, 405 Howard Street, Suite 600, San Francisco, CA 94105
T: (415) 498 5000, F: (415) 498 7100, www.pwc.com/us

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements related to the engagement.

Inherent limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section IV.

Opinion

In our opinion, in all material respects,

PricewaterhouseCoopers LLP, 405 Howard Street, Suite 600, San Francisco, CA 94105
T: (415) 498 5000, F: (415) 498 7100, www.pwc.com/us

a. the description presents the system that was designed and implemented throughout the period November 1, 2021 to October 31, 2022, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that the Service Organization's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of the Service Organization's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of the Service Organization's controls operated effectively throughout that period.

Restricted use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of DocuSign, Inc., user entities of the system during some or all of the period November 1, 2021 to October 31, 2022, business partners of DocuSign, Inc. subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following ("specified parties"), if applicable:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

PricewaterhouseCoopers LLP, 405 Howard Street, Suite 600, San Francisco, CA 94105
T: (415) 498 5000, F: (415) 498 7100, www.pwc.com/us

This report is not intended to be, and should not be, used by anyone other than these specified parties. If a report recipient is not a specified party as defined above and has obtained this report, or has access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against PricewaterhouseCoopers LLP as a result of such access. Further, PricewaterhouseCoopers LLP does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

PricewaterhouseCoopers LLP

San Francisco, California
December 16, 2022

PricewaterhouseCoopers LLP, 405 Howard Street, Suite 600, San Francisco, CA 94105
T: (415) 498 5000, F: (415) 498 7100, www.pwc.com/us

DocuSign®

Section II – Management of DocuSign, Inc.'s Assertion

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign®

Management of DocuSign, Inc.'s Assertion

We have prepared the accompanying description of DocuSign, Inc.'s eSignature system (the "system") titled "DocuSign's Description of Its eSignature System " throughout the period November 1, 2021 to October 31, 2022, ("description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"). The description is intended to provide user entities with information about the system that may be useful when assessing the risks arising from interactions with the system, particularly information about system controls that DocuSign, Inc. has designed, implemented, and operated to provide reasonable assurance that its 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*).

DocuSign, Inc. uses subservice organizations to provide Information Technology General Controls (ITGCs) related to server hosting and cloud services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DocuSign, Inc., to achieve DocuSign, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents DocuSign, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DocuSign, Inc.'s controls. The description does not disclose the actual controls at the subservice organizations.

We confirm, to the best of our knowledge and belief, that

a. the description presents the system that was designed and implemented throughout the period November 1, 2021 to October 31, 2022, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that DocuSign, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations applied the complementary controls assumed in the design of DocuSign, Inc.'s controls throughout that period.

c. the controls stated in the description operated effectively throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that DocuSign, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of DocuSign, Inc.'s controls operated effectively throughout that period.

DocuSign®

Section III – Description of DocuSign, Inc.'s eSignature System Throughout the Period November 1, 2021 to October 31, 2022

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign®

Scope of the Report

For the purpose of this report, DocuSign, Inc. (“DocuSign”) is considered the service organization. Users of the eSignature service (“the Service”) through the eSignature System (“the System”) from the DocuSign Agreement Cloud are considered the user entities (“user entities”). This report covers the period from November 1, 2021 to October 31, 2022.

This report is intended to provide user entities of DocuSign’s System during some or all of the period November 1, 2021 to October 31, 2022, business partners of DocuSign subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators with information about the System and relevant controls designed and implemented to meet the security, availability, and confidentiality criteria set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)* throughout the period November 1, 2021 to October 31, 2022. The description that follows outlines the processes and controls that are performed by DocuSign for its customers. This should be read in conjunction with the Trust Services Principles, Criteria, and management’s related control activities described in Section IV that are intended to be incorporated herein by reference.

As this description is intended to focus on the controls relevant for the achievement of the security, availability, and confidentiality categories set forth in TSP Section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*, it does not encompass all aspects of the services provided or procedures performed by DocuSign.

Company Overview

DocuSign is a Software as a Service (“SaaS”) company offering the DocuSign Agreement Cloud. It has more than a dozen services and more than 350 integrations covering the entire agreement process, from preparing to signing, acting on, and managing agreements.

Overview of Services Covered

The Service provides a cloud-based platform to help user entities electronically sign documents from any computer or mobile device. The Service automatically guides user entities through the document set-up process of entering signing related data (e.g. name, title, etc.) and then electronically signing the documents. Once completed, the Service allows users to download copies of the signed documents for their records.

Key Terms

DocuSign uses the following key terms in the System:

- **Envelopes:** An Envelope is a container for Documents that is sent to a Recipient to sign. It holds data on the Documents to be signed, the Signers and other Recipients, and the places where Signers will sign the Documents. Note: Envelopes have statuses (e.g. sent, delivered, completed, voided) and typically contain documents, recipients, and

DocuSign

fields. They also contain information about the sender and timestamps that indicate the progress of the delivery procedure. When an Envelope is completed, DocuSign automatically generates a Certificate of Completion which details the full audit history of the transaction.

- **eDocuments:** Files uploaded into the System by Sender roles and stored in Envelopes. Also referred to as Documents throughout this report.
- **Templates:** A template is a reusable Envelope with specific Documents, set Recipient roles, routing order, authentication, signing tabs and information fields. Note: Saved templates can be used to start a new Envelope. Elements configured in the saved template (e.g., fields, Documents, roles, recipients, etc.) are applied and added to the new Envelope. Templates can be used as is, or additional Documents can be added, signing fields can be modified, recipients can be added, and messages can be modified.
- **Recipient Routing:** Collection of Recipient roles which need to either sign Documents or receive a copy of signed Documents.
- **Fields (also known as Tabs or Tags):** Fields (e.g., text boxes, radio buttons, checkboxes) that indicate where a specific information must be placed on a Document. Note: Fields are used to show information such as dates, company names, titles to Recipients. Senders add fields which can be edited or populated by a Signer.
- **Accounts:** A set of attributes that define a user's access to a given DocuSign service, application, or product. Account access can be further restricted or shared by adding users to a pre-determined set of users, referred to as a Group. Note: An Organization is comprised of a set of DocuSign eSignature accounts. When an Organization is first created, the Account on which the Organization is based is the default Account and is used for provisioning new users.

System Roles

DocuSign has defined the following user roles in the System:

- **Senders:** User entities responsible for creating, sending, and managing Envelopes. In addition, Senders perform many actions to Envelopes such as uploading Documents, adding Recipients, defining routing orders, and placing fields on Documents for Recipients.
- **Signers:** Persons or third-party entities designated by Senders to access or take action upon the Documents sent to such person or third-party entity via DocuSign eSignature.
- **Recipients:** User entities that are added to Envelopes by Senders, responsible for reviewing the Documents, entering data, or signing the Documents. There must be at least one Recipient for an Envelope, and a Sender can determine a route if multiple Recipients are involved. Each Recipient may have one or more Tabs (also known as fields or tags) defined for them. Each recipient is assigned a specific type, which defines their role in the signing process. Any of these recipients can be a remote recipient (who receives the envelope via email), or an embedded recipient (who views, approves, or signs the envelope’s documents directly through an app or website).
- **Account Administrators:** Senders’ authorized individual users responsible for configuring and managing the Sender’s production accounts in the System. Account

DocuSign

Administrators set up policies (e.g. password, document retention, etc.) and manage the DocuSign Senders authorized to send for the user entity. This is a default permission profile that gives a user access to all eSignature features and allows them to manage all account settings and users for an account.

- **Production Administrators:** DocuSign personnel authorized to access and perform job related tasks in the user entity's production instance of eSignature.

System Workflow Lifecycle

Below are detailed descriptions of the major steps within the System lifecycle:

Creating an Envelope

Senders initiate an eSignature transaction lifecycle by creating an Envelope either through Public APIs or in Web Applications (refer to *Key IT Components* section for definitions of these terms). The System allows Senders to create a new Envelope by specifying a Document or Document template that they wish to send.

Preparing an Envelope

Senders can upload any of the supported file types, including documents, images, presentations, and spreadsheets. Then, Senders add Recipients and define the Recipient routing order which can be sequential, parallel, or mixed. Senders can optionally set up alerts on the Envelope to remind Recipients to sign Documents and define an expiration date for the Envelope to prevent Recipients from signing Documents after a certain date. Once the routing order has been defined, Senders place fields on Documents to capture signing related data (e.g. name, title, etc.) and specify where to apply signatures or initials for Recipients. Lastly, Senders send the Envelope.

Accessing an Envelope

Upon sending the Envelope, the System emails invitations to each Recipient in the defined routing order that contains a web link to access the Envelope. When a Recipient clicks on the web link, it launches the applicable Web Application on the Recipient's computer or mobile device.

Signing the Documents

The Service displays the Documents and guides the Recipient through actionable fields. While a Recipient may view data entered by previous Recipients in the routing order, the Service prevents the current Recipient from editing this data or viewing fields assigned to any future Recipients of the Envelope. Alternatively, input from previous Recipients may be hidden from subsequent Recipients by configuring the "Document Visibility" feature. After the Recipient completes their assigned fields, the System ends the Recipient's signing session which prevents this Recipient from further modifying the data entered in their fields. Finally, the System sends the Envelope to the next Recipient in the routing order.

DocuSign®

Managing an Envelope
The System provides updates in real-time to the Senders on current status of the Envelope within the Web Applications and to third-party applications via web hooks. Whether managing Envelopes through the Web Applications, web hooks, or Public APIs, Senders retain full control of the process from creation to completion.

Retaining an Envelope
Once all Recipients have finished signing Documents, the System generates a summary of the Envelope called a Certificate of Completion ("CoC") that indicates the number of Documents and fields within the Envelope; date and time stamps for Envelope and Recipient events; and key details about the Recipients' signing sessions. The System also allows Senders and Recipients to download a copy of signed Documents and CoCs to store in their environment outside of the System. Further, the Senders' Web Applications retain Envelopes and associated data based on the Senders' document retention configuration.

Service Commitments and System Requirements

Service commitments to user entities are documented and communicated in user entity agreements and notifications, as well as in the description of the service offering provided online. The System is designed to meet the following commitments:

Security
- Restrict access to data and systems by applying the least privileged principle through logical and physical access management processes.
- Monitor key system components for security incidents to identify and respond to security threats timely through logical and manual security logging and monitoring processes.
- Use of encryption technologies to protect user organization data both at rest and in transit.
- Implement authorized and tested changes to system components through secure development and change management processes.

Availability
- Maintain and monitor an infrastructure that ensures user organization data are replicated and backed up at multiple locations.
- Maintain and monitor an infrastructure that ensures user organization capacity demands are met.

Confidentiality
- Maintain data classification standards and processes to identify confidential user organization data.
- Use of encryption technologies to protect confidential user organization data both at rest and in transit.
- Restrict access to confidential data applying the least privileged principle through logical and manual physical access management processes.
- Retain user organization data in line with user agreements.

DocuSign

DocuSign established operational requirements that support the achievement of security, availability, and confidentiality commitments. Such requirements are documented and communicated in DocuSign policies and system documentation. In addition, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the System.

Components of the System Used to provide the eSignature Service

People

The following section details DocuSign's organizational structure focusing on departments and teams involved with the controls relevant to this SOC2 report:

Board of Directors
DocuSign's Board of Directors currently consists of independent directors (as defined under applicable law and exchange listing rules) and DocuSign's Chief Executive Officer. The Board oversees the overall governance of the Company, including setting the tone at the top and maintaining the Company's Code of Business Conduct and Ethics.

Trust & Security
DocuSign's Trust & Security, led by the Vice President, Chief Information Security Officer ("CISO"), is responsible for trust services such as third-party management, information and application security, incident response, and business continuity. The following teams within Information Security support the System's processes and controls:

- **Incident Response:** This team responds to suspected security incidents related to the System. When security incidents are flagged by monitoring tools, this team tracks cases and follows the Incident Response Playbook and Standard Operating Procedures ("SOPs") to resolve these security incidents.
- **Security Infrastructure:** This team is responsible for managing and maintaining security infrastructure.
- **Vulnerability Management:** The team performs authenticated and unauthenticated scans to identify and track remediation of vulnerabilities. Additionally, the team monitors network and host attack surface through OS, Network penetration tests, Segmentation testing and coordinated response of emergent zero-day vulnerabilities.
- **Third-Party Governance:** This team evaluates risk to DocuSign's commitments with third-party vendors and suppliers.
- **Enterprise Resiliency:** This team manages business continuity and disaster recovery programs. The team also performs business continuity tests on a periodic basis.
- **Compliance:** This team manages operational and regulatory compliance. As part of the compliance effort, the team develops and maintains a control framework. This team also manages the annual policy review program.

DocuSign®

Engineering

DocuSign's Engineering department, led by the President, Product and Engineering, has responsibility for the Technical Operations and Engineering departments, which are relevant to the System's controls and are supported by the following teams:

Architecture

DocuSign's Architecture group, led by the Chief Architect, is responsible for the operations that run the System. This department includes following teams:

- **Technical Operations:** This team manages the infrastructure and hardware (e.g. servers, databases, networks, etc.) in data centers, runs code in the production network, and monitors the overall system health. Only Technical Operations team personnel have access to the production environment. There are four groups within this team:
  - **Database Storage Solutions:** Configures and manages SQL databases; applies SQL patches; and monitors database related performance.
  - **DocuSign Operations Center ("DOC"):** Monitors system health 24 hours per day, seven days a week. Also, the DOC team manages disaster recovery testing on a periodic basis. This team also manages site operations.
  - **Network Operations:** This team installs and manages third-party network gear (e.g. routers, firewalls, etc.); configures networks; and monitors network traffic.
  - **Release Management:** Builds release candidates with the new product features, bug fixes, and enhancements to deploy in the production network.

Product Management

Responsible for coordinating enhancements to System features.

Development

Develops the software code related to Public APIs, Web Applications, and Platform Services described in the Software and Infrastructure section of this report.

Quality Assurance

Writes test cases either within an automated testing tool or manual test scripts which are executed to validate new code developed for product features, bug fixes, or enhancement requests. Further, this team validates new releases after being deployed in the development and production networks.

Finance

DocuSign's Finance department, led by the Chief Financial Officer, has responsibility for Internal Audit and Enterprise Risk Management. Below are detailed descriptions:

- **Internal Audit:** Tasked by the Board of Directors to provide assurance of compliance with DocuSign's financial, operational, privacy and security

DocuSign

processes. Audits are executed on an annual basis (and as directed by the Audit Committee of the Board of Directors). Also, the Internal Audit team owns and manages Enterprise Risk Management ("ERM") framework and program.

Customer Success
DocuSign's Group Vice President, Customer Success oversees the Customer Success department summarized below.

- **Technical Support:** Provides multiple tier support to address questions or issues raised by DocuSign users 24 hours per day, seven days per week. In order to assist, this team has write access within the production network.

Human Resources
DocuSign's Human Resources ("HR") department, led by the Chief People Officer, oversees recruiting, learning, and benefits departments. HR is responsible for hiring qualified and appropriate candidates by performing candidate assessments and background checks. Further, HR provides business organizational information including job roles, job descriptions, and up-to-date organizational charts. Additionally, HR manages a learning management system to deliver employee training.

Legal
DocuSign's Legal Department, led by the Chief Legal Officer, is responsible for global contract management, including drafting and negotiation of master service agreements and other customer contracts.

Software and Infrastructure

The Services are hosted on the System, which is comprised of front-end, network layers, and back-end. The front-end layer has web servers for APIs, Web Applications, and Platform Services. The network layer consists of devices (e.g. firewalls, load balancers, etc.) to route traffic from the public Internet to the front-end layer as well as between the front-end and back-end layers. The back-end layer contains database and storage servers to protect the data.

Below are descriptions of each key IT component of the System:

Sender Documents
Senders can create, manage, and send Envelopes as well as upload Documents through the following methods:

- **Third-Party Applications:** The majority of Envelopes are sent into the System via third-party applications that are integrated though Public APIs. There are more than 350 third-party applications which have already integrated with DocuSign as of the end of the reporting period. Further, any licensed developer can integrate other third-party or custom-built applications with these APIs once they obtain a production certified integrator key. By using this method, Senders can create Envelopes, upload Documents, and send Envelopes directly within the third-party applications.

DocuSign®

- **Senders' Devices:** Senders can also manually create Envelopes and upload Documents via Web Applications. By using this method, Senders can upload Documents stored on their computer or mobile device directly into the System.

Public APIs

DocuSign leverages DocuSign Developer Center to allow anyone to integrate third-party applications with Public APIs:

- **SOAP APIs:** DocuSign provides Public APIs based on the Simple Object Access Protocol ("SOAP") specification to allow Senders with legacy and custom built third-party applications to automatically combine the create and send stages of the transaction process into the simple push of a button.
- **REST APIs:** DocuSign also provides Public APIs based on the Representational State Transfer ("REST") specification to provide Senders with third-party applications and cloud based services the same level of customization as the SOAP APIs, but with minimized API call usage and the potential to complete more transactions per hour. DocuSign also provides Software Development Kits (SDKs) to wrap our eSignature REST API with objects, properties, and methods in multiple programming languages.

Web Applications

Web Applications allow Senders to manually create, send, and manage Envelopes. These applications also allow Recipients to enter data into fields, sign Documents, and allow Account Administrators to configure settings in their production accounts. Web Applications are launched within web browsers on the Senders', Recipients', and Account Administrators' computers or mobile devices.

- **Sending Experience:** A web application, based on JavaScript (or similar web-development language) code, for Senders to manually create Envelopes and upload Documents into the Sending System. Senders also add Recipients, define the routing order, and place fields on Documents in Sending Experience.
- **Signing Experience:** A web application, based on JavaScript code, for Recipients to view Envelopes, input data fields, and sign Documents.
- **Administration Experience:** A web application, based on JavaScript code, for Account Administrators to configure production accounts settings (e.g. password policy, document retention policy, etc.).

Platform Services

The following IT components are part of the System's platform layer in production. Only Public APIs and Web Applications can call these platform services:

- **Document Conversion:** This service is the first step in providing protection to Sender Documents. Each time a Sender uploads a Document to the System, a new virtual server is activated for the session. Then, this service converts non .pdf document types into a new .pdf file, to prevent malicious content from being passed through to the converted file. The new .pdf files are stored as BLOB objects which are encrypted and

DocuSign

stored within Network Area Storage (“NAS”) devices in the data centers. At the end of this process this service destroys the virtual server.

- **Tamper-Evident Seal:** This service digitally signs Documents downloaded from the System by Senders or Recipients with an X.509 certificate to create tamper-evident seals. Attempts to manipulate a Document breaks its tamper-evident seal and when opened in a PDF reader displays a warning message about the broken tamper-evident seal.
- **Certificate of Completion:** This service creates a Certificate of Completion (“CoC”) at the completion of every Envelope which provides a summarized audit trail of key information and events related to the Envelopes and helps Senders prove the authenticity of their Envelopes. CoCs are stored as BLOB objects.

In-scope Applications and Systems

DocuSign uses the following applications and systems in support of the eSignature platform:

- **DocuSign eSignature:** Cloud-based platform to electronically sign Documents from any computer or mobile device.
- **BLOB Object:** See *Infrastructure* section below.
- **SQL DB:** See *Infrastructure* section below.
- **Kazmon:** Proprietary Security Incident & Event Management (“SIEM”) tool to monitor the overall system health and produce alerts. Kazmon collects statistics about each BLOB object and SQL metadata, metrics about product features, and operating metrics from the data center infrastructure. Kazmon collects log files, correlates events, and creates alerts about the System. The log files come from numerous sources which includes, but is not limited to, data center infrastructure, logical access attempts, and monitoring software on employee issued assets (e.g. anti-virus, data leakage prevention, etc.). Then, the events are correlated and alerts produced that are automatically entered into the case management tool. Production Kazmon data is stored in Microsoft Azure. This data is geo-distributed by Azure region.
- **Production Active Directory:** DocuSign has set up an Active Directory (“AD”) domain for the production network, which is different from the HQ AD domain for DocuSign employees, that contains the unique credentials for authorized employees on the Technical Operations team to access the System.
- **Internal Admin/Admin Console:** Internal Admin is a web application for authorized DocuSign personnel to perform account management tasks on production and demo accounts.
- **GitHub:** Creates, stores, and tracks code related to APIs and Web Applications. After developing new product features, bug fixes, and enhancements, GitHub is the code repository used to produce the release candidate.

Supporting IT Tools

DocuSign uses the following tools to support the key IT components and controls relevant to this SOC2 report:

DocuSign®

- **DC Auto:** Proprietary software tool to manage server configuration as well as asset inventory.
- **Sawmill:** Proprietary software testing tool to automate test cases. Sawmill runs thousands of test cases in sequence to test the quality of new product features, bug fixes, and enhancements.
- **Crypto Manager:** DocuSign has developed a proprietary tool to generate and manage symmetric keys in the System. DocuSign rotates the symmetric keys on a quarterly basis by following the approved process to segregate roles and responsibilities between different DocuSign teams to ensure no one person or team can create symmetric keys on their own.
- **HSM:** DocuSign has integrated security appliances with a hardware security module ("HSM"). The DocuSign HSM appliance generates unique symmetric keys on-demand for each Envelope.
- **Snort IDS:** Proprietary software tool to monitor for intrusion detection.
- **Information Security Case Management:** DocuSign has implemented an Information Security Case Management ("ISCM") tool to track and manage security incidents.
- **Tenable:** Scanner tool used to perform vulnerability scans of network and OS in the production network.
- **Rapid 7:** Rapid 7 is a tool used to perform web application and new release scanning and dynamic analysis for the System.
- **Clam AV:** Open source antivirus software that is used to detect malicious threats, including trojans, viruses, and malware. It is also used for mail gateway scanning.

Networks

DocuSign has configured the dedicated production network for the System. The production network refers to a segregated network in the data centers that host the System. The production network is not physically or logically connected to the corporate network and access to this network is strictly limited to authorized employees in the Technical Operations team.

Infrastructure

The following infrastructure IT components protect and store data related to Envelopes, Documents, and fields:

- **BLOB Objects:** Represents Document, field, and CoC data stored in the Sender's account. After creating BLOB objects, the System immediately encrypts BLOB objects with a unique symmetric key based on the AES256 algorithm and stores BLOB objects within NAS devices in the data centers.
- **SQL Database:** Represents metadata about Envelopes' status and Recipients' actions and is stored in SQL databases in the data centers.

The production network refers to Public APIs, Web Applications, Platform Services, Production Network, and Infrastructure.

DocuSign®

Data

The System stores Document related data as BLOB objects in the NAS devices, and Envelope metadata in SQL databases. The following table details the Document related data and Envelope metadata captured and stored by the System:

Field	Storage Platform
Documents (files uploaded by Senders)	BLOB Object
Fields (text fields, radio buttons, signatures, etc. placed on documents by Senders)	BLOB Object
Signature Images (images either selected or uploaded by Recipients to represent their handwritten signature and initials)	BLOB Object
Certificate of Completion	BLOB Object
Envelope History (Transaction Log)	BLOB Object
Voice Recordings of Phone Authentication	BLOB Object
Signature GIFs	BLOB Object
Envelope Subject (entered by Senders and seen by Recipients)	SQL Database
Email Message (entered by Senders and seen by Recipients)	SQL Database
Sender's Email Address	SQL Database
Sender's Name	SQL Database
Field Metadata (field name, unique identifier, and assigned Recipient related to fields)	SQL Database
Signer List	SQL Database
Time Stamps (date and time for Envelope events and actions taken by Recipients)	SQL Database
Recipient's Name	SQL Database
Recipient's Email Address	SQL Database
Recipient's Routing Order	SQL Database
Phone Number for SMS and Phone Authentication Recipients	SQL Database

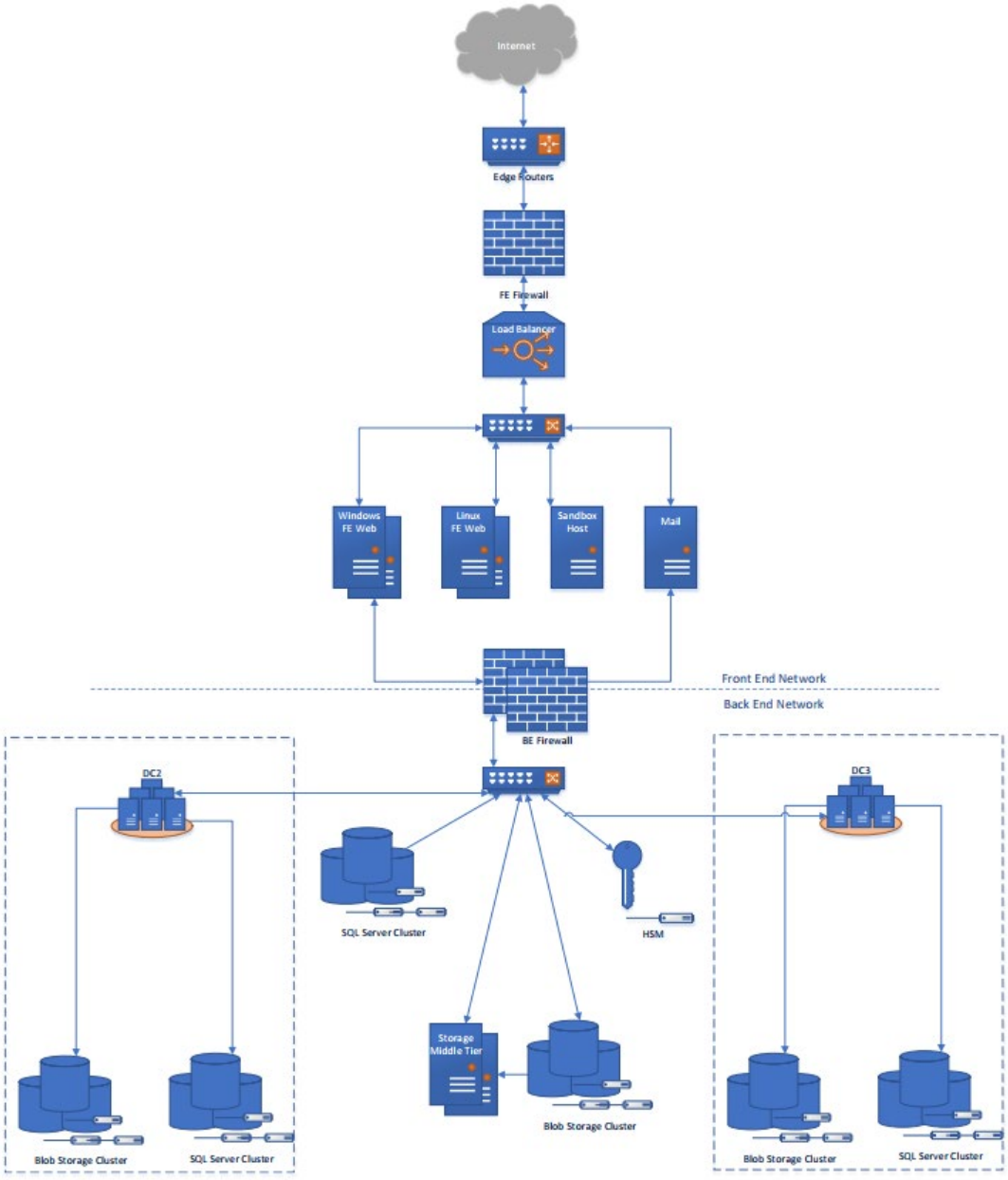
Supported File Formats

DocuSign supports the following file formats:

DOCUMENT	.doc, .docm, .docx, .dot, .dotm, .dotx, .htm, .html, .msg, .pdf, .rtf, .txt, .wpd, .xhtml, .xps
IMAGE	.bmp, .gif, .heic, .jpg, .jpeg, .png, .tif, .tiff
PRESENTATION	.pot, .potx, .pps, .ppt, .pptm, .pptx
SPREADSHEET	.csv, .xls, .xlsm, .xlsx

DocuSign

DocuSign has segmented the production network into multiple segments. Below is a diagram of the production network:



This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign®

Data Centers

DocuSign has multiple data centers in the United States, Europe, Canada, and Australia to provide regional availability. DocuSign has contracted with subservice organizations to provide server hosting services to host the infrastructure (e.g. servers, databases, networks, etc.) required to run the System. As part of data center services, the subservice organizations control physical access to the data center premises, ballistic protections, perimeter controls, badged access (both subservice organizations' personnel and DocuSign's authorized users), and 24x7x365 monitoring (e.g. CCTV, alarms, etc.) In addition, DocuSign performs assessments of the subservice organization controls by obtaining the most recent SOC reports to assess design and operating effectiveness of relevant controls implemented at subservice organizations.

North America (United States)

DocuSign has three data centers in North America with Cyxtera and SunGard as subservice organizations. Cyxtera data centers are located in Chicago, Illinois and Seattle, Washington. SunGard data center is located in Dallas, Texas. DocuSign has established a private wide area network ("WAN") connection between data centers to transfer data seamlessly. While DocuSign remotely manages the System, Cyxtera and SunGard provide physical security protection for the data centers. Only authorized DocuSign employees are permitted physical access to these data centers to perform their job tasks (e.g. set up racks, install servers, etc.). DocuSign has secured cages in each data center which can only be accessed by DocuSign's authorized employees. Additionally, DocuSign North America production devices collect data via the North America Microsoft Azure Kazmon region collectors. For the European Union (EU), Kazmon collectors are on premise devices in the EU datacenters that forward the Kazmon telemetry to North America.

European Union

DocuSign has three data centers within the European Union with Equinix as the subservice organization. The data centers are located in Frankfurt, Germany; Amsterdam, Netherlands; and Paris, France. DocuSign has established a WAN connection between data centers to transfer data seamlessly. While DocuSign remotely manages the System, Equinix provides physical security protection for the data centers. Only authorized DocuSign employees are permitted physical access to these data centers to perform their job tasks. DocuSign has secured cages in each data center which can only be accessed by DocuSign's authorized employees or remote hands services.

Canada

DocuSign uses Microsoft Azure cloud services, which has two Azure data centers in Canada: Central (Toronto) and Canada East (Quebec City). Microsoft Cloud Infrastructure and Operations ("MCIO") and Azure Cloud services provide server hosting and as part of hosting services, SQL server backup service is provided. No DocuSign employees have physical access to Azure data center. Azure data center is managed by Microsoft as part of the Azure Cloud Services.

DocuSign®

Australia
DocuSign uses Microsoft Azure cloud services, which has two Azure data centers in Australia: Australian East (Sydney) and Australian Southeast (Melbourne). MCIO and Azure Cloud services provide server hosting and as part of server hosting services, SQL server backup service is provided. No DocuSign employees have physical access to Azure data center. Azure data center is managed by Microsoft as part of the Azure Cloud Services.

Processes and Procedures

DocuSign has established an extensive combination of automated and manual procedures to ensure that the Company's information is safeguarded throughout its entire lifecycle.

Information security policies address security, availability, and confidentiality principles in various approved and published policies. Security describes the organization of information security; access controls; backup; business continuity; change management; encryption; incident response; monitoring and logging; network security; and physical standards. Information security policies are subject to review and modifications on at least an annual basis. The purpose of the review is to ensure that policies, procedures, and standards are up-to-date with respect to potential threats, changes in regulatory and business environments, technological changes, and other changes that impact information security.

Relevant Aspects of the Control Environment, Risk Assessment, Processes, Information and Communication, and Monitoring

Control Environment

In order to set the right control environment, DocuSign has the following procedures in place to appropriately set the corporate governance and oversight of control activities:

Management Oversight
DocuSign's stockholders elect DocuSign's Board of Directors, a majority of whom are independent as defined under applicable law and exchange listing rules. The Board of Directors provides entity-wide oversight over strategic objectives, business objectives and goals, risk management, external reporting and internal controls established and executed by management and personnel. Prior to election or appointment to the Board, director candidates are interviewed by existing members of the Board; are subject to background checks; and complete a Director and Officer questionnaire.

DocuSign's Board of Directors carries out its oversight responsibilities via regular (generally held quarterly) and ad hoc board meetings. The Executive staff also holds meetings on an as-needed basis (generally monthly) to discuss current operations, results, objectives, and risks.

The DocuSign ISMS (Information Security Management System) Program is also aligned with the core goals of the business and is directly mapped to company objectives. The information security strategy is developed and has been communicated broadly across the Company, with the Executive team, and with the Board of Directors. The ISMS meeting occurs annually to review the Compliance Standard and Information Security Objectives to ensure that scope,

DocuSign

roles, responsibilities, resources, etc. are complete and accurate, and will contribute to the continued, effective operation of the DocuSign ISMS.

Further, DocuSign's Board of Directors is responsible for reviewing and approving the Company's Code of Business Conduct and Ethics ("the Code"), which governs the corporate responsibilities of directors, officers, and employees, contingent workers, agency contractors and independent contractors of the Company (and its direct and indirect subsidiaries). The Code reflects DocuSign's commitment to integrity and ethical values. Material changes to the Code requires written approval of the Board and/or selected Board Committees.

Quarterly, any exceptions to the Code of Conduct relating to Executive Officers or Directors and other governance items are reviewed in the Standing Audit Committee Meeting.

Structure and Responsibilities

DocuSign established reporting lines and appropriate authorities and responsibilities in the pursuit of security, availability, and confidentiality in the organizational chart. The organizational chart is available internally to DocuSign employees and contingent workers, including details about each role, contact details, and system support function. Any changes to key areas of authority and responsibility, including reorganizations, are communicated to employees by organizational leaders.

Policies

DocuSign has defined a number of policies necessary to support the achievement of security, availability, and confidentiality commitments. Moreover, DocuSign's policies are periodically reviewed, approved by management, and communicated to DocuSign personnel via the Company's intranet site. Where policy exceptions are requested, DocuSign reviews, documents, and approves exceptions to policies and standards based on business need and risk and periodically reviews these exceptions.

The Information Security and Compliance teams have published the following policies and standards which are applicable to DocuSign employees and contingent workers. These include, but are not limited to:

- Logging and Monitoring Standard
- Data Classification Standard
- Data Handling Standard
- Incident Management Standard
- Information Security Policy
- Secure Development Life Cycle ("SDLC") Standard
- Third-Party Governance Standard
- Vulnerability Management and Remediation Plan
- Physical Security Standard
- Compliance Standard
- Business Continuity and Resiliency Standard

DocuSign®

The Technical Operations and Information Security teams have written policies and standards applicable to those groups (see *People* section above) including but not limited to:

- Datacenter Standard
- Key Management Procedure
- Product Capacity Procedure
- Product Network Standard
- Product Change Standard
- Technical Operations Procedure

The Human Resources and Legal teams have defined policies which are applicable to DocuSign employees and contingent workers. These include, but are not limited to:

- Employee Lifecycle Policy
- Disciplinary Policy
- Background Check Policy
- Whistleblower and Complaint Policy
- Code of Business Conducts and Ethics (Code of Conduct)

Employee Competency

In addition to corporate governance, DocuSign has procedures to hire, develop, and retain competent employees in alignment with security, availability, and confidentiality commitments such as following:

Hiring Process

The HR team has developed a process for onboarding new DocuSign employees and contingent workers. As part of the onboarding process, the HR team performs an assessment of the roles and responsibilities of the job and pre-employment background checks of each candidate. Where applicable, and as permitted by local law, DocuSign has contracted with a third-party vendor to perform the pre-employment background checks for employees, which cover the following areas and can vary by type of candidate:

- Candidate address history and criminal background checks (Local, State, National)
- National SSN trace and sex offender registry checks
- Global blacklist searches
- Candidate employment and education verifications

Contingent workers are also subject to a background check based on the criteria defined in the Company's background check policy(ies). New employees and contingent workers in the US also need to complete the post hire paperwork (depending on type of worker) including Confidential Information, Mobile Device Policy, and Code of Conduct. Employees and contingent workers in non-US regions need to consent to a Statement of Terms and Conditions of Employment, which includes a confidentiality clause. After onboarding, non-US employees and contingent workers sign the Mobile Device Policy and Code of Conduct. For agency contractors, this is accomplished through either overarching MSA terms and conditions or

DocuSign

individual signature of consent forms. New hires are required to complete a Code of Conduct training or certification through an online portal or other means.

Before the new employee or contingent worker's first day at DocuSign, the background check is initiated and results are obtained by DocuSign or if the results have not been obtained, review and approval from Deputy GC or delegate is required. As of May 31, 2022, review and approval from the Senior Director of Employment, Litigation and Investigations, or above is sufficient. Once the background checks have successfully completed and been approved by the hiring managers, (if applicable), the HR team sends new hire emails to Corporate IT, Security, and Facilities teams to issue company assets (e.g. laptop, desktop, etc.), and enroll employees and contingent workers in corporate systems (e.g. badge, email, payroll, etc.). Corporate IT also provisions new accounts in HQ AD domain to access the corporate network. These accounts are activated by new employees and contingent workers on their first day of employment.

Development and Training

Upon hire and on an annual basis, DocuSign employees complete security and privacy trainings. Upon hire and on an annual basis, DocuSign contingent workers with access to systems, devices, or locations, complete security awareness training. The trainings focus on high risk security topics including social engineering, reporting of suspicious activities, data handling, and data protection. Records of training completion are managed within DocuSign's selected Learning Management System.

In addition, DocuSign employees and contingent workers with access to systems, devices, or locations in development and QA roles are required to complete an annual training on secure coding techniques. Those provided GitHub access are additionally required to complete training checklists tailored to the following areas within DocuSign code: Fundamentals, API, Integrations, DocuSign Signing Experience, Signing & Internal Admin, and Mobile. Records of training completion for all secure coding training are managed within DocuSign's selected Learning Management System.

Employee Accountability

DocuSign holds employees accountable for their internal control responsibilities to meet security, availability, and confidentiality commitments. DocuSign's employees and managers complete an annual assessment of employee performance based on the procedure set forth. The assessment results are collaboratively reviewed between both parties to maintain alignment on role responsibilities and individual goals.

DocuSign does not have a formal progressive discipline policy requiring any set number of warnings or counseling sessions prior to termination. However, DocuSign considers numerous factors in determining disciplinary measures and the situation within. Failure to adhere to the policies, including the Code of Business Conduct and Ethics, is subject to disciplinary action. Also, if performance slips during the year, DocuSign may take formal corrective steps depending on the severity of the occurrence or performance deficiency.

Additionally, the Company has adopted a Whistleblower and Complaint Policy for employees of the Company. The Policy is available via the Company's Intranet Site and helps to ensure that

DocuSign®

the Company maintains a workplace where employees who reasonably believe that they are aware of questionable accounting, auditing, and internal controls and disclosure practices, can raise their concern free of any harassment, discrimination or retaliation. Concern can be raised directly to a HR Business Partner or Compliance Officer or anonymously through a confidential complaint hotline directed to the Compliance Officer and/or Chairman of the Audit Committee. Hotline reports are reviewed and assessed by the Audit Committee.

Risk Assessment

Enterprise Risk Management Program

The DocuSign Enterprise Risk Management (ERM) program provides executive management insight into the strategic risks associated with the Company's overall goals. It is a decision support system that helps management to optimize outcomes, with the goal of preserving and ultimately enhancing value.

The ERM program is divided into five processes:

Context Setting

On an annual basis, ERM interviews top DocuSign executives in a Risk Culture Survey. The Risk Culture Survey articulates which types of risk the Company formally tracks and manages, including documenting corresponding permitted risk thresholds. Risk types are categorized with a High, Moderate, or Low risk level in the assessment.

Annually, ERM interviews key stakeholders in a Value-Add Assessment. The Value-Add Assessment documents existing processes and (1) validates which stakeholders are accountable for managing risk (2) assesses the Company's capability to manage risk levels, and (3) identifies the most valuable opportunities to improve risk management.

Risk Assessment

ERM performs an annual enterprise-wide risk assessment of DocuSign's overall company goals. In this assessment, ERM and its stakeholders identify the top threats to those goals. If the threats are deemed credible, risk scenarios (including the inherent likelihood and impact to the goals) are documented. ERM then documents specific strategy, process, or system-level vulnerabilities that could allow those risks to materialize. Lastly, the processes or controls that reduce the likelihood and/or impact of the risk are documented and a residual risk level is determined. The residual risk level is shown in context of the Company's risk appetite, making any delta between the two measures clearly visible.

Assessment Criteria & Risk Register

The ERM Risk Register captures ERM risk assessment data and provides a repeatable model to assess a wide variety of risk types. The Likelihood and Impact criteria used to estimate risk levels are documented within the ERM Risk Register. ERM Risk Register is a tool that enables the business to evaluate how specific or aggregate risks may affect DocuSign's overall company goals.

Risk Treatment

ERM partners with stakeholders and industry experts to provide treatment recommendations as part of the assessment process. Risks with residual ratings higher than the Company's

DocuSign

acceptable risk levels generally receive recommendations to reduce the risk to an acceptable level.

Risk owners may accept, mitigate, avoid, or transfer risks at their own discretion. ERM does not assign treatment requirements to stakeholders as ERM is not a management function.

Risk Monitoring

ERM partners with stakeholders to monitor risk on an ongoing basis. Risk types with a high threshold are evaluated as part of the annual risk assessment. Risk types with a moderate or low threshold are updated quarterly, or as needed. Risk types with a low threshold are recommended to be continuously monitored by the appropriate and accountable DocuSign stakeholders.

Risk Reporting

At the end of each assessment cycle, DocuSign produces a Risk Assessment Report. The report documents the assessment criteria, identified threat scenarios and risks, risk ratings, and recommended actions. This report is provided to the Audit Committee and senior DocuSign management during the Audit Committee meeting.

Third Party Governance

The Third-Party Governance ("TPG") team manages the DocuSign due diligence process for assessing and monitoring risks associated with the use of third-party products and services.

The TPG managed process helps mitigate undue risk. TPG manages assessment of a variety of risks (including but not limited to cybersecurity, financial, business continuity, legal, regulatory, and privacy) that need to be either accepted, transferred, mitigated, or denied.

The TPG team's due diligence process identifies and tracks the following:

- Third-party product and services with a particular emphasis on SaaS services, data center services, outsourced business processes and critical customer-facing services where sensitive data is directly accessible or processed by the third party. After assessing the third-party, each third party product or service is assigned a tier. Questionnaires and assurance reports (e.g. SOC2, ISO and penetration tests) may also be required depending on the tier. DocuSign reviews controls within subservice organization assurance reports where applicable (e.g. SOC2 reports) to ensure that they meet organization requirements; if control gaps are identified in the assurance reports, the TPG team works with management takes action to address the risk and impact.
- Legal, compliance, security, operational or credit risks that could lead to service disruption, legal issues or adverse media that could negatively impact DocuSign and its ability to onboard and retain customers.

Additionally, the TPG team monitors applicable Tier 1 (highest risk/most critical) products, services, and vendors using tools that are configured to alert against publicly disclosed breaches and critical risk vectors.

DocuSign

Information and Communication

DocuSign utilizes multiple communication channels to convey information to both internal and external audiences:

Internal Communication

DocuSign leverages the following communication channels to inform and get feedback from DocuSign's employees involved with the development and production networks related to the System. Through this communication, DocuSign cultivates a culture that cares about user entities' success. In fact, DocuSign's primary metric is the number of successful transactions completed by user entities.

- **Policy Bank:** DocuSign maintains an internal website containing DocuSign's policies, procedures, and standards.
- **Training:** DocuSign provides training for new employees, as well as annual security awareness training, and role specific training.
- **Platform:** DocuSign has fully digitized our business processes by requiring employees to submit and approve requests (e.g. Infrastructure Change, Release Authorization, etc.) in the System.
- **Email and Slack:** DocuSign relies on corporate email and Slack for communications such as an invitation to review and approve requests in the System; notification of an incident generated by the case management tool; and status updates about the current stage of a new release.
- **Meetings:** Quarterly, Management holds a Company meeting/conference call at Company headquarters. Key discussion items include (as applicable): Core Values, Strategy, Mission, and Critical Success Factors to focus on over the next quarter and remaining fiscal year. During the meeting, select Executives (CEO,CFO,VPs) provide an update of the quarter's activities, financial results, and future goals.

External Communication

DocuSign uses the following communication channels with external Account Administrators, Senders, and Recipients:

- **DocuSign Support Center:** DocuSign operates a Support Center website to support Account Administrators, Senders and Recipients on how to use the System, access documentation (e.g. user guides, admin guides, etc.), and provide updates about incidents or changes.
- **Developer Center**: DocuSign maintains the DocuSign Developer Center website to provide developers with access on how to use the APIs for the System.
- **DocuSign Trust Center:** DocuSign maintains the DocuSign Trust Center (trust.docusign.com) website to publish the current status of the System and updates and alerts about the System.
- **DocuSign Website:** DocuSign provides a contact method on the website for external and internal parties to submit complaints and inquiries and report incidents. DocuSign also publishes product documentation to its public website that describe the purpose, design and boundaries of the System and its components. In addition, DocuSign

DocuSign

publishes Senders' and Account Administrators' responsibilities and other relevant information about the Services in this document available on DocuSign's website (https://www.docusign.com/company/terms-and-conditions/web).

- **Release Notes:** DocuSign generates release notes for all monthly releases to communicate new product features and bug fixes in the System.
- **Contracts:** External party roles and responsibilities which support DocuSign's information security objectives are communicated and imposed via supplier and master service agreements and data processing agreements (if applicable). Also, Agency temporary workers, independent contractors, and supplier entities consent to a non-disclosure agreement.
- **DocuSign Sites & Services Terms and Conditions:** DocuSign communicates Sender responsibilities and other relevant information about the Services in this document available on the company's website to users.
- **Web Applications:** DocuSign provides real time updates to Senders on the current status of Envelopes in the Web Applications. Additionally, Senders can view specific details about Envelope related events and actions taken by Senders and Recipients.
- **Email:** DocuSign emails invitations to Recipients to initiate a signing session in the System. Further, DocuSign emails updates to Senders when Recipients perform an action in the System as well as when signing sessions are completed.
- **Certificate of Completion:** DocuSign generates a summary about the Envelope that describes the number of Documents and fields in the Envelope, key details about Recipients' signing sessions, and date and time stamps for Envelope related events and Recipient actions.

Monitoring and Control Activities

DocuSign operates a continuous monitoring program that includes several forms of management review.

Internal Audit

DocuSign's Internal Audit function is tasked by the Board of Directors to assess and evaluate compliance with DocuSign's financial, operational, privacy and security processes. Audit requirements are established based on laws and regulation applicable to DocuSign, DocuSign's risk tolerance, industry standards, and established control frameworks. Audits are executed on an annual basis (and as directed by the Audit Committee ("AC") of the Board of Directors). Where deficiencies are identified, Internal Audit identifies areas for improvement through management action plans where possible. Once an audit completes, the Internal Audit team prepares a report and communicates the results to key stakeholders and the AC. Annually, Internal Audit will also perform and update the fraud risk assessment for the organization. As a result of the assessment, the IA team communicates the results to the Legal and AC team as necessary. The fraud risk assessment is reviewed and approved by the Chief Accounting Officer.

DocuSign®

Reporting Nonconformities
Deficiencies identified during an audit are documented and tracked by the respective audit team. Deficiencies are validated with the impacted process owners in conjunction with Internal Audit leadership oversight. To remediate deficiencies, Internal Audit teams work with impacted control owners to prepare management action plans. Ongoing progress toward remediation is ensured through periodic monitoring and communication based on the respective management action plan. The status of deficiencies that correlate to areas for which DocuSign has a low risk tolerance are reported to the ERM team for tracking through resolution. Escalation procedures are in place for critical deficiencies or management action plan faults. Internal Audit leadership briefs the AC quarterly on the status of deficiencies undergoing remediation.

Logical and Physical Access

Logical Access Internal Users
DocuSign restricts logical access to the production network running the System to the Production Administrators and DocuSign Operations Center in the Technical Operations team. Also, access to modify source code is restricted to authorized personnel. Further, DocuSign limits administrative access to Senders' production accounts to authorized users of the Internal Admin Web Application. Below are more detailed descriptions about the logical access controls and monitoring of these accounts:

Network Segmentation
DocuSign has designed a production network architecture to prevent unauthorized access to the System (see *Networks* above). When inbound data traffic reaches the network's edge, the border router and front-end firewalls create a demilitarized zone ("DMZ") that prevents peer-to-peer communication from the Internet to services containing sensitive application code and data. After clearing the DMZ, the data traffic hits the front-end servers to process the requests. The System then sends data traffic from front-end servers through back end firewalls to store data as BLOB objects and SQL records.

Further, Network traffic to and from untrusted and wireless networks passes through the DMZ; firewall rules are established in accordance to identified security requirements and business justifications. Changes to firewalls follow DocuSign's change management process, which includes review and approval before being implemented. Wireless access to the DocuSign production network within the datacenters is prohibited. On a quarterly basis, DocuSign performs scanning within the data centers to identify and remove unauthorized wireless access points.

Privileged Accounts
The Technical Operations team has access to the production network. Access is provisioned based on the job responsibilities for two groups in the Technical Operations team: Production Administrators and the DocuSign Operations Center ("DOC"). Production Administrators are granted remote access to manage the servers, databases, and networks in data centers. The DOC is granted access to deploy new release candidates into the production network. Note: the DOC is separate from the Release Management team responsible for building the releases.

DocuSign

DocuSign has provisioned specific Active Directory Domains (ADs) North America, European Union, Australia, and Canada in the production network for privileged accounts to access the System. These accounts have unique credentials for each authorized employee and are prevented from identifier reuse. When new employees join the Technical Operations team or existing Technical Operations employees need different access rights, the employees' managers submit Production Access Authorization requests. These requests are reviewed and approved by the employees' immediate manager, and system owners for any related data and applications. Once approved, a new and unique privileged account is provisioned in this AD and set up with a one time passcode token.

In order to access the System, Production Administrators and DOC team members log in to DocuSign's production network on their company issued computers through virtual private network ("VPN") sessions which require two factor authentication:

- Log in requires a valid AD credential (username and password) that meets the AD's password policy requiring the password length to be at least 14 characters; complexity involving mixed letters, numbers, and symbols; expiration set every 90 days; and reuse prevented for the previous 24 passwords.
- Entering a one time passcode from their assigned token.

After establishing VPN sessions, Technical Operations team members login to jump hosts with their AD credential to perform their job responsibilities. Privileged access activities are monitored as part of the system monitoring process. Refer to *Monitoring and Incident Response* section for the details.

Internal Admin Account

The Global Support team has read access and in limited cases, write access to Senders' production account configurations to help Senders and Account Administrators who contact DocuSign for assistance. To be provisioned access, Global Support management needs to submit Internal Admin Access requests for review and approval. Once approved, DocuSign grants access to the Global Support team members.

Termination of Access

When an employee is terminated or no longer requires access to the system, the access is removed from the System accordingly. The HR team initiates a termination and deactivation process which triggers an alert to system administrators, including the Production Administrators or DOC team members, who remove or disable production systems accounts for terminated employees.

Continuous Monitoring

As a monitoring control, DocuSign sends log files from the VPN, AD, and jump hosts to the SIEM tool to track privileged accounts. SIEM generates alerts for new privileged accounts and any permission changes for existing privileged accounts. If the SIEM generates an alert related to logical access, Incident Response tracks the case in their internal tool and responds by following the playbook and defined SOPs.

DocuSign

Periodic Access Review

DocuSign performs Quarterly Access Reviews ("QAR") to review any access management changes for physical and logical access. During the review, the reviewer ensures any inappropriate access or terminated user is removed from the access. After the review is complete, it is signed off by the reviewer and any other applicable stakeholders.

Logical Access External Users

The System enables Senders to create Envelopes and upload one or more Documents through either Public APIs or Web Applications. Most Senders leverage Public APIs to integrate their custom built applications with SOAP or REST APIs to automatically create Envelopes and upload Documents from these applications. The remaining Senders login to the signing experience Web Application to create and send Envelopes either manually or through Single Sign On ("SSO"). Below is a description of unique credential requirements for each method to identify and authenticate Senders:

Unique Credentials Requirements *(API)*

Senders can create Envelopes and upload Documents from custom built applications by integrating with Public APIs. In the DocuSign Admin Web Application, Account Administrators generate unique integrator keys to register their custom built applications with the System. Each custom built application requires its own integrator key. After the Account Administrator completes a minimum of 20 successful test transactions in compliance with DocuSign API rules and limits, DocuSign promotes the integrator keys into their production accounts. Once the custom built applications are registered in the System, any Sender who successfully authenticates in the custom built applications can automatically create Envelopes and upload Documents to the System.

Unique Credentials Requirements *(Web Applications)*

Senders who plan to create Envelopes and upload Documents via Web Applications must be provisioned with DocuSign user accounts. In the DocuSign Admin Web Application, Account Administrators are responsible for configuring the production account's password policy and managing DocuSign user accounts. Account Administrators select one of the following password policies which is applicable to DocuSign user accounts:

- **Basic:** Password must be at least six characters.
- **Medium:** Password must be seven characters, contain at least one uppercase letter, contain at least one lowercase letter, and contain at least one number or one special character.
- **Strong:** Password must be at least nine characters, contain at least one uppercase letter, contain at least one lowercase letter, contain at least one number, and contain at least one special character.
- **Custom:** Sender configures minimum password length and age as well as rules about uppercase and lowercase letters, digits, and special characters.

Account Administrators manually create an individual DocuSign user membership for Senders who need DocuSign user accounts in the DocuSign Admin Web Application. The System emails invitations to the Senders which contains a web link to activate their DocuSign user account.

DocuSign®

Senders click the web link and enter their password based on the password policy defined for the production account. Senders can then login to the Web Application with their DocuSign credentials to manually create Envelopes and upload Documents from their computers or mobile devices.

Unique Credentials Requirements *(Single Sign On)*

SSO provides the benefit of letting Senders switch between DocuSign and other cloud services quickly and securely, without having to input their DocuSign account credentials each time. Account Administrators are responsible for setting up SSO on accounts via the organization administration features in the DocuSign Admin Web Application. Account Administrators must prove domain ownership in order to claim domains for the accounts. Then, Account Administrators establish interoperability between an Identity Provider and DocuSign by providing a SAML configuration. When Senders, Signers, and Account Administrators try to log on to DocuSign through SSO, the Identity Provider provides a SAML assertion of that user's identity. DocuSign either successfully authenticates the user or rejects the authentication request because they are not permitted to use the System. The setup of SSO accounts is the responsibility of the user entity and is outside the scope of the SOC 2 report.

Multi-Tenant Platform

The System is a multi-tenant platform which restricts access to data, Envelopes, and Documents for user entities. DocuSign sets up unique accounts for Senders in production. These accounts contain the Senders and integrator keys created by the Account Administrators. Additionally, these accounts store Envelopes created and Documents uploaded by the Senders, and related data. Only identified and authenticated Senders can login to their account. The integrator keys and DocuSign credentials ensure only those identified and authenticated Senders can create Envelopes and upload Documents in their accounts.

Unauthorized or Malicious Software Access

DocuSign has implemented controls to prevent and detect the introduction of unauthorized or malicious software to meet the entity's security objectives. DocuSign has managed enterprise antivirus deployment to ensure that signature definitions are updated daily and scans are enabled. In addition, DocuSign has an intrusion detection and prevention system deployed to ensure the system captures any malicious traffic based on the definition updated on a daily basis. Any alerts from the anti-malware scanning as well as intrusion detection and prevention system are reviewed and resolved according to the incident response plan. See 'Production Environment Monitoring' section below for the details around alert review and response.

Physical Access

DocuSign has contracted with several subservice organizations to provide server hosting services to host the infrastructure components of the System. While subservice organizations manage the data centers' physical access security protection, DocuSign has developed processes and controls to monitor the subservice organizations physical security controls and to restrict access to authorized DocuSign users. With these controls, DocuSign further reinforces the security posture of encrypted Sender transactional data. Below are more detailed descriptions of the subservice organizations and processes:

DocuSign®

Subservice Organizations
DocuSign expects server hosting providers to operate controls to restrict physical access to authorized personnel and ensures badged access for both subservice organizations' personnel and DocuSign's authorized users.

In order to ensure data center control operating effectiveness, DocuSign reviews data centers' controls within third-party assurance reports to ensure that they meet organizational requirements annually. If control gaps are identified in the assurance reports, management takes action to address any impact the disclosed gaps have on the organization.

Authorized User Process
DocuSign limits unescorted physical access to cages in the data centers to authorized users within the Technical Operations team. When a user requires unescorted physical access to perform their job tasks, the user's manager needs to submit a Data Center Authorization request which is approved by Technical Operations' senior management. Once approved, DocuSign submits a request to the appropriate subservice organization to issue a permanent data center badge and grant access to DocuSign's cages within the data center. The authorized user then must complete the subservice organization's process to be allowed unescorted access to the data center. In the event an authorized Technical Operations member with access to the subservice organization data center is terminated or transferred, DocuSign contacts the subservice organization to remove the Technical Operations member from the authorized list. DocuSign performs physical access reviews on a quarterly basis. After the review, any inappropriate access is removed where applicable.

System Operations

DocuSign has processes in place to monitor system components and the operation of those components for vulnerabilities or anomalies that may affect the Company's ability to meet security, availability, and confidentiality.

Vulnerability Management
The Vulnerability Management & Application Security teams perform scans and penetration testing on a regular basis to identify vulnerabilities in the System. The Vulnerability Management team scans the system and infrastructure for security vulnerabilities and recommends either patching or secure configuration changes. The team uses Tenable and Rapid7 (see *Software* section above) to perform the scans and track findings. The Application Security team scans the APIs and the Application for security vulnerabilities at the application layer.

After performing vulnerability scans and penetration testing, the Technical Operations team reviews the scan results with vulnerability scores from Common Vulnerability Scoring System ("CVSS") and risk levels and prioritizes remediation of legitimate vulnerabilities according to the assigned risk. In some cases, DocuSign determines a finding may be a false positive or an operational requirement. For other cases, DocuSign notifies and works with system owners to identify a plan to remediate the finding such as incorporating vulnerabilities identified into monthly patch management.

DocuSign

Monitoring and Incident Management
DocuSign defines the procedures required to manage, track, and report incidents.

DocuSign also tests incident response processes on an annual basis to validate the incident response process and adjust the process where necessary. Results from the tests and lessons learned, including improvement points, are documented. Below are detailed descriptions of these processes:

Security Events
The Incident Response team is responsible for monitoring organization-wide security incidents. The Detection Engineering team defines security monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts and uses a centralized SIEM to capture and correlate logs from components within the System. Logs from hosts and servers are sent to the SIEM directly from production system components. The Incident Response team continuously monitors the SIEM and Security Infrastructure team manages configurations and logs in the SIEM. Below are some sample events generated from these logs:

- *Malicious IPs followed by exploits*
- *Firewall Blocks*
- *Antivirus and Malware activity*
- *Network DOS activity*
- *Intrusion Detection System (IDS) activity*
- *Production and Database Access activity*

When alerts are generated, the SIEM automatically creates new cases to identify, track, and report incidents in ISCM tool (see *Software* section above). The Incident Response team follows the DocuSign Incident Response Plan to assign the severity or priority, resolve the incidents, and notify proper stakeholders.

Production Events
The DOC team is responsible for monitoring overall production events related to production health including availability of the System. The Incident Response team is instead responsible for monitoring overall security events generated by the alerts built by the Detection team. The DOC team uses an in-house performance monitoring solution, Kazmon, which deploys local custom agents on hosts which monitors performance and events related to the System. By continuously monitoring the production environment, DocuSign can make informed decisions on how to respond to incidents that potentially affect Sender data in the System. Additionally, DocuSign ensures that the Platform is configured to synchronize information system time clocks based on Centralized Network Time Protocol (“NTP”) to coordinate system network protocol and produce synchronized logs.

When Kazmon produces critical alerts based on pre-defined thresholds, the DOC team resolves the issue according to established work instructions with defined severity and notifies or escalates to the System Administrators group. Similarly, the Incident Response team contacts the DOC team about any incidents above pre-defined thresholds to work together to resolve the issue.

DocuSign®

Additionally, DocuSign tracks issues reported by Senders, Recipients, or Account Administrators. The Global Support team provides updates based on actions taken to resolve these issues.

Root Cause Analysis

When there are high ("SEV1") and medium ("SEV2") severity incidents, the DOC team performs a root cause analysis ("RCA") to determine the underlying problems of incidents. During the RCA analysis, the DOC team focuses on the areas for improvement that includes management processes, system management, application design, human factors, and other significant factors in the System of Agreement Web Applications or Systems. The DOC team looks at incident detection factors (e.g. monitoring systems, human factors, etc.) and incident resolution factors (e.g. incident management, subject matter expert response, etc.) for improvement as well. Finally, the DOC team documents the recommendations for the top areas of improvement that have the most impact to reduce recurrence, mitigate impact, or increase speed of resolution for any events related to the System and presents during the monthly Live Site Review meeting to the product engineering teams including Technical Operations.

Incident Notification

DocuSign makes available to customers the DocuSign Trust Center website in which incidents significantly affecting DocuSign's security, availability, and confidentiality commitments are communicated. When there is an incident which may significantly impact DocuSign's commitments, the Incident Response team escalates it to the Legal team for review. If the Legal team determines it does significantly impact DocuSign's commitments, an alert is posted on the DocuSign Trust Center website and Global Support is briefed on the frequently asked questions ("FAQ") about it.

Change Management

DocuSign has a formal SDLC Policy that governs requirements for the modification to and maintenance of the System. DocuSign has segregated responsibilities for changes to the System between the Product Development and Release Management teams. In addition, there are separate development/staging and production networks in the System. The Development team has access only to the development network and is responsible for writing code for new product features, maintaining existing code and ensuring overall code quality. The Technical Operations team generally has access only to the production network and is responsible for changes to the servers, databases, and networks in data centers; as well as monitoring the System's overall health.

DocuSign has two different change management processes for software (code) and infrastructure (hardware) changes. Below are more detailed descriptions on how DocuSign mitigates the risk of unauthorized or incorrect changes being implemented in the production environment.

DocuSign®

Software Changes

DocuSign follows an approved SDLC process that identifies:

- Requirements for design, approval, implementation, configuration, testing, modification, and deployment
- Approval and authorizations needed for the release to progress through the process
- Responsibilities of personnel to perform during the development process for releases

At the start of the SDLC process, the Development team reviews a prioritized list of features, bugs, and enhancements. Then, the Development team uses a centralized code repository, GitHub, to track code in the development environment. Individual developers create a new branch in the code repository; write the code related for the new product features, bug, or enhancement; and check their branch back into the repository. In parallel, the Quality Assurance ("QA") engineers write either test cases in an automated testing tool, or manual test script depending on the feature, bug, or enhancement. Once an individual developer checks their branch into the code repository, the QA engineer partnering with that developer executes the applicable test cases to verify the proper functionality of the feature, bug, or enhancement.

During the SDLC process, the Development team ensures that any outstanding branches are checked back into the code repository. The release managers then merge branches together in the code repository to produce the first release candidate which is deployed in the Stage area of the development environment. QA engineers perform prerelease testing by executing their test cases for features, bugs, and enhancements against this release candidate. QA engineers only have access to the development environment and customer data is not stored in any non-production environment. Access to production data is restricted through role-based access controls and prohibited otherwise through standard operating procedures. Additionally, production data are encrypted to protect against inadvertent use for testing purposes, such that the data would not be readable or usable. Decrypted production data is not accessible to DocuSign personnel. DocuSign policy prohibits personnel from accessing decrypted production customer data, and also prohibits using production data for testing purposes and storing or processing it on non-production systems through technical restrictions and standard operating procedures. Code changes resulting from testing require approval by the QA engineers.

At the end of the SDLC process, individuals with the responsibility of Release Manager submit a Release Authorization request that has details about the change description, build information, release details, release components, test pass results, backout plan, independent code review and security approval. Change scope, change type, and roles and responsibilities are pre-established and documented in a change workflow. Next, DocuSign's Release Authorization Change Control Board, which includes representatives from Engineering, Product, Quality Assurance, and DOC, reviews and approves this request. Once approved, the Release Managers produce a final release candidate which is made available to the DOC team.

A DOC team member deploys the final release candidate for the System into production. QA engineers perform post deployment tests by executing their test cases again for features, bugs, and enhancements in this release. If there are any P1 (Priority 1 – Critical) issues identified by

either QA engineers or Senders, the release candidate is rejected and production is rolled back to the last known good release. Otherwise, the release is considered live.

DocuSign produces releases on a monthly basis, but major features are often released pursuant to a cadence of three releases a year (March, July, and November). As part of the monthly releases, the Application Security team performs dynamic web application security tests to check the System.

Application scanning includes:

- **Dynamic Application Security Testing:** Analyzes HTML code and API code (REST, SOAP) for the System to identify potential risks. The Application Security team performs monthly system security scans to identify vulnerable software while firmware scanning is done by the Vulnerability Management team. Prior to conducting scans against the production environment, the Application Security team updates vulnerability scanning tools to ensure the version of the tool is up to date and current.

Infrastructure Changes

DocuSign follows an approved Infrastructure Change Management process to authorize any changes to the servers, databases, and networks within the Service data centers. Production Administrators submit an Infrastructure Change request to the Infrastructure Change Management Board that documents the change reason, data center, change start date, change details, validation steps, and roll back steps. DocuSign's Infrastructure Change Management Board, which is comprised of Infrastructure and Technical Operations management members, then reviews and approves applicable requests. Once approved, the Production Administrators group makes changes based on details documented in the requests. Any emergency changes also follow this process.

For any new servers deployed, systems must pass a security acceptance review, which ensures logging and alerting tools are installed and configured properly for system security monitoring. A security scan is also performed on new servers to identify unsafe or unauthorized configurations, including default vendor credentials.

Additional Criteria for Availability

DocuSign has designed resilient processes and architecture to minimize risk of potential data loss (see *Software and Infrastructure* above):

- **Data Centers:** DocuSign has contracted multiple locations with Cyxtera, SunGard, Equinix, and Azure to provide server hosting services to host the System in North America (United States), Europe, Canada, and Australia. If there is an issue with one of the data centers, DocuSign automatically fails over to another data center in the regional ring.
- **Internet Service Provider:** In each data center, DocuSign has contracted with multiple Internet service providers ("ISP") to provide Internet access. If an ISP is experiencing problems, DocuSign automatically fails over to another ISP.

DocuSign®

Capacity Planning
The DOC team periodically assesses the capacity of its production environment and implements the changes necessary to ensure that its services continually meet the organization's availability commitments and requirements.

Backup & Restoration
Below are descriptions of the backup and recovery processes:

- **Azure (Canada and Australia):** Data are replicated to geographically disperse Azure instances. DocuSign stores five perpetual backups of encrypted BLOB data. Metadata are stored in the Azure managed SQL instance. In the event of a disaster or total site failure in any of the active systems, user activity is served by the remaining.
- **Physical (North America and Europe):** Data are replicated to geographically dispersed data centers. DocuSign stores nine perpetual backups of encrypted BLOB data. Metadata are stored in MSSQL. DocuSign maintains SQL Availability Groups with five (5) nodes spread across two data centers. In the event of a disaster or total site failure in any of the active systems, user activity is served by the remaining sites. Further, DocuSign monitors data replication jobs for failures that indicate a data integrity compromise.

Business Continuity
DocuSign has defined a Business Continuity Program (“BCP”) to meet DocuSign’s availability commitments. The BCP focuses on location centric plans with a set of checklists for the business processes which includes:

- **Continuity Planning:** A continuity strategy which defines assumptions, limitations, stakeholders, first actions, continuing actions, return home, communications, and contacts list. DocuSign's business continuity plans are reviewed, approved, and communicated to relevant team members at a minimum on an annual basis.
- **Continuity Testing:** A test determines readiness of a department or location to execute a continuity plan in an adverse situation, and should include, but not limited to one or more of the following elements:
    - Tabletop exercises
    - Simulated or Actual Technology Failover
    - Building evacuations
    - Verification of plan contact information
    - VPN testing
    - Mass communication testing

Disaster Recovery
DocuSign has developed an active-active architecture for the System that automatically replicates BLOB objects and SQL databases (*see Data Replication section above*) across data centers in the geographical ring (*see Data Centers section above*). Per policy, there is a Recovery Point Objective (“RPO”) of five minutes for the System which is the maximum latency in data replication between data centers in the geographical ring. In addition, there is a

DocuSign®

Recovery Time Objective (“RTO”) of 15 minutes for the System to fail over and restore full functionality.

Additional Criteria for Confidentiality

DocuSign has processes in place to identify and ensure confidentiality of data including Documents uploaded into Envelopes, fields added to Documents, and Envelope workflows in the System. Confidentiality of data is core to the System and incorporated into the following areas:

Data Identification

Data is identified and protected in the System’s design, development, testing, implementation, and change processes to ensure confidentiality through the following methods:

Data Classification

DocuSign maintains a Data Classification Standard which is periodically reviewed, approved by management, and communicated internally. The Data Classification Standard defines data classification criteria to properly handle data during the creation, distribution, usage, storage, and disposal lifecycle stages. This standard applies to DocuSign applications including the System. DocuSign has four levels of information classification: Public, Internal, Confidential, and Restricted. Note that while Confidential is noted as a category, other information classifications are treated as confidential where applicable.

Data Encryption

Data within the boundaries of the System is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition by using the following methods:

Data in Transit Protection

Public APIs and Web Applications enable standard TLS connections to protect data in transit. When third-party applications initiate sessions, Public APIs create secure TLS connections with the third-party connections which encrypts data sent during the sessions. Similarly, Web Applications start secure TLS connections with Senders’ web browsers to encrypt data sent in the sessions. DocuSign has deployed secure socket layer (“SSL”) certificates issued by Symantec which is a Certificate Authority (“CA”) automatically trusted by web browsers and operating systems.

DocuSign®

Data at Rest Protection

When Senders upload files into the Sending System, new virtual servers are created to convert the non .pdf files into .pdf documents that are stored in new BLOB objects and encrypted with symmetric keys. By encrypting BLOB objects, the integrity of the Sender's Documents, fields, and CoCs are protected within the Sending System while the data is at rest. Symmetric key encryption is performed in security appliances which use a single key with an AES256 algorithm to scramble data which makes it unreadable to humans. This key and the second symmetric key which is generated simultaneously and required to decrypt the data is stored in separate SQL databases which are also separate from the BLOB objects which are stored in NAS. Only the System has the necessary code logic to find Senders' production accounts in the SQL database, pull the corresponding symmetric keys either from Batch or On Demand security appliances, and fetch BLOB objects from network area storage to decrypt the data.

DocuSign uses security appliances to manage and store the symmetric keys to encrypt the BLOB objects. Access to the cryptographic key stores is limited to authorized personnel. There are currently two methods to generate symmetric keys: Batch and On Demand.

- **Batch:** Canada and Australia follow batch processing for the time being. DocuSign holds key ceremonies to rotate symmetric keys on the security appliances. For each key ceremony, the Production Administrators group member submits an Infrastructure Change Request which is approved by the VP of Technical Operations on a quarterly basis. The Production Administrators group members then schedule a key ceremony to bring together stakeholders from different teams to perform assigned tasks using an in-house tool, DocuSign Crypto Manager, which generates new batches of unique symmetric keys. DocuSign Crypto Manager has been built to segregate roles and responsibilities amongst different group members such that no one member can generate the symmetric keys on their own. Further, DocuSign Crypto Manager is monitored by the Incident Response team for any inappropriate attempts or activities to access the key by non-Production Administrator group members.
- **On Demand:** A majority of key generation is done On Demand, with North America and European Union using this method. DocuSign has integrated security appliances with DocuSign Private Server, which is a hardware security module ("HSM"). The DocuSign Private Server generates a unique symmetric key on-demand for each Envelope. DocuSign is deploying DocuSign Private Servers in FIPS 140-2 Level mode throughout the production environment. When deployed in FIPS 140-2 Level mode, three different Production Administration group members insert smart cards to activate the DocuSign Private Server so that no one member can generate symmetric keys on their own. Similar to the Batch process, access to key manager is monitored by the Incident Response team.

DocuSign®

Data Retention

Account Administrators can set up a custom document retention configuration to store Envelopes and associated data for a specified number of days (e.g. one day, 30 days, etc.) in the DocuSign Admin Web Application. As a default, if Administrators for active accounts do not set a purge schedule, Envelopes are maintained as per service agreements. When there is a custom document retention configuration, Envelopes and associated data are purged from the Web Application, including personal information, after the specified number of days in the Senders' account.

In addition, uploaded Documents are deconstructed in DocuSign's Document conversion environment by virtual machines. Malicious content is not passed through to the converted PDF, which is stored in the BLOB storage system; unsupported file types or files are blocked via an exclusion list configuration. Virtual machines are decommissioned and redeployed upon reaching a configured threshold of conversions.

Data Disposal

DocuSign uses hard drives as the only form of physical media. Hard drives containing customer data are not transported outside of Cyxtera, SunGard, or Equinix data center facilities. DocuSign has contracted with third-party shredding suppliers and oversees destruction of system components and receives certificates of destruction.

DocuSign works closely with SunGard, Cyxtera, and Equinix to ensure new and de-commissioned system components and physical media are appropriately controlled during shipment both to and from the data centers. Also, DocuSign ensures the systems components within the System and physical media are controlled within the data centers.

Complementary Subservice Organization Controls

The description in Section III of this report includes only the processes, policies, and procedures of DocuSign, and does not include the policies, procedures and control activities at the subservice organizations, Azure, Cyxtera, SunGard, and Equinix. Also, the examination by the Independent Service Auditors does not extend to the processes, policies, and procedures at these subservice organizations.

Azure, Cyxtera, SunGard, and Equinix are responsible for operating, managing, and controlling the underlying infrastructure components supporting the services which are utilized by DocuSign. The Description indicates that certain applicable trust services criteria can be met only if Azure's, Cyxtera's, SunGard's, and Equinix's controls, assumed in the design of DocuSign's controls, are suitably designed and operating effectively along with related controls at the service organization. DocuSign assumed that the subservice organizations, Azure, Cyxtera, SunGard, and Equinix, would implement and maintain the following controls necessary, in combination with DocuSign's controls, to achieve DocuSign's service commitments and system requirements based upon the security, availability and confidentiality trust services criteria.

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign®

Related Criteria	Complementary Subservice Organization Control Descriptions
CC6.4	Azure, Cyxtera, SunGard, and Equinix are responsible for restricting data center physical access to authorized personnel and requires badged access for both subservice organizations' personnel and DocuSign's authorized employees.
CC6.4, A1.2	Azure, Cyxtera, SunGard, and Equinix are responsible for ensuring physical security and environmental protections measures are in place including ballistic protections, perimeter controls, badged access (both sub-service organizations' personnel and DocuSign's authorized employees), heating ventilation and air-conditioning, fire detection and suppression and 24x7 monitoring (e.g. CCTV and alarms).
CC6.4	Azure, Cyxtera, SunGard, and Equinix are responsible for issuing a permanent data center badge prior to allowing unescorted access to DocuSign's areas within the data center.
CC6.3	Azure is responsible for appropriately restricting access to customer data. Azure is responsible for appropriately restricting access to modify configurations to customer backup.
CC6.5	Azure is responsible for establishing Hard Disk Drive destruction guidelines and following the guidelines for the disposal of Hard Drives.
CC8.1	Azure is responsible for the formal change management process and performing the appropriate testing, approval, and review prior to deployment.
A1.2	Azure is responsible for performing periodic backups and monitoring and resolving backup failures (relevant to SQL customer data).

Complementary User Entity Controls

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust service criteria.

DocuSign®

Section IV – Trust Services Categories, Criteria, DocuSign, Inc.'s Related Controls, and PricewaterhouseCoopers' Tests of Operating Effectiveness and Results of Tests

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

46

DocuSign®

Description of Tests Performed by PricewaterhouseCoopers

Our tests of operating effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the specified the trust services security, availability, and confidentiality criteria were achieved throughout the period November 1, 2021 to October 31, 2022. In selecting particular tests of the operating effectiveness of the controls, we considered (i) the nature of the controls being tested; (ii) the types of available evidential matter; (iii) the nature of the trust services categories and criteria to be achieved; (iv) the assessed level of control risk; and (v) the expected efficiency and effectiveness of the test. Such tests were used to evaluate fairness of the presentation of the description of DocuSign's eSignature system and to evaluate the operating effectiveness of specified controls.

The following clarifies certain terms used in this section to describe the nature of the tests performed:

- Inquiry: Inquiry of appropriate personnel and corroboration with management
- Observation: Observation of the application, performance, or existence of the control
- Inspection: Inspection of documents and reports indicating performance of the control
- Reperformance: Reperformance of the control

Additionally, observation and inspection procedures were performed as it relates to system generated reports and queries within DocuSign's Description to assess the completeness and accuracy (reliability) of the information utilized in the performance of our testing of the control activities.

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
Control Environment			
Trust Services Criteria 1.1: **COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.**			
CG-01-02	DocuSign's Board of Directors provides strategic oversight via: • periodic meetings to discuss management's decisions, major transactions, and past results • quarterly board meetings to align on core values, strategy, and mission.	**Inspection** Inspected a sample of quarterly Board of Directors meeting minutes and All Hands meeting agendas to determine whether DocuSign's Board of Directors provide strategic oversight through periodic meetings to discuss management's decisions, major transactions, and past results and quarterly board meetings to align core values, strategy, and mission.	No exceptions noted.
CG-01-05	The Company has adopted a Code of Conduct for directors, officers, and employees of the Company (and its direct and indirect subsidiaries). Material changes to these Codes require the written approval of the BOD and/or selected Board Committees.	**Inspection** Inspected DocuSign's Code of Conduct to determine whether it communicated the governing corporate responsibilities to directors, officers, and employees of the Company (and its direct and indirect subsidiaries). Inspected DocuSign's Board Meeting Minutes for approval of material changes to the Code of Conduct.	No exceptions noted.
CG-02-05	Quarterly, review of any exceptions and granting of exceptions to the Code of Conduct relating to Executive Officers or Directors and other	**Inquiry** Inquired with management to determine whether any exceptions and granting of	There were no exceptions and granting of exceptions to the Code of Conduct relating to

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	governance items is reviewed in the Standing Audit Committee Meeting.	exceptions to the Code of Conduct relating to Executive Officers or Directors and other governance items is reviewed in the quarterly Standing Audit Committee Meeting. **Inspection** Inspected the quarterly Standing Audit Committee Meeting minutes to identify if there were any exceptions and granting of exceptions to the Code of Conduct relating to Executive Officers or Directors and other governance items during the period.	Executive Officers or Directors and other governance items requested during the period. Therefore, the operating effectiveness of this control activity could not be tested.
TA-01-02	New hires are required to complete the Code of Conduct Certification or Training through online portal or other means.	**Inspection** Inspected a sample of new DocuSign employees to determine whether the Code of Conduct Certification or Training was completed.	No exceptions noted.
CG-01-06	The Company has adopted a Whistleblower and Complaint Policy for employees of the Company. The Policy is available via the Company's Intranet Site and helps to ensure that the Company maintains a workplace where employees, who reasonably believe that they are aware of questionable accounting, auditing, and internal controls and disclosure practices, can raise their	**Inspection** Inspected the Whistleblower and Complaint Policy for evidence of review and approval. Inspected DocuSign's Policy Bank to determine whether DocuSign employees were able to access and view the Whistleblower and Complaint Policy.	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	concern free of any harassment, discrimination or retaliation. Concern can be raised directly to a HR Business Partner or Compliance Officer or anonymously through a confidential complaints hotline directed to the Compliance Officer and/or Chairman of the Audit Committee. Hotline reports are reviewed and assessed by the Audit Committee.	Inspected a sample of quarterly Audit Committee minutes to determine whether confidential complaints were reviewed and assessed by the Audit Committee. **Observation** Observed a test complaint submitted through the confidential complaints hotline to determine whether the complaint was communicated to the Compliance Officer and/or Chairman of the Audit Committee.	
Trust Services Criteria 1.2: **COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.**			
CG-01-01	DocuSign stockholders elect a Board of Directors to oversee DocuSign's Executive management and set the Company's strategic direction.	**Inspection** Inspected DocuSign's Board of Directors, Nominating and Corporate Governance Committee Charter and Audit Committee Charter to determine whether the Board of Directors were elected to oversee and communicate the Company's financial goals, strategic objectives, and internal control operations in accordance with defined charters.	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
CG-01-01 (01)	Prior to election, DocuSign interviews board member candidates and conducts background checks to verify each candidate's experience and qualifications.	**Inspection** Inspected a sample of new board members to determine whether DocuSign conducted background checks to verify each candidate's experience and qualifications prior to election.	No exceptions noted.
CG-03-01	The ISMS Owner conducts a formal management review of the DocuSign ISMS on an annual basis; key decisions relating to continual improvement and ISMS changes are documented and actioned.	**Inspection** Inspected the annual DocuSign ISMS Management Review meeting agenda to determine whether key decisions relating to continual improvement and ISMS changes were documented and actioned.	No exceptions noted.
Trust Services Criteria 1.3: **COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**			
CG-01-04	The Company has established appropriate lines of reporting, in part on the size and the nature of their activities, as evidenced by the functional group and organizational charts.	**Inspection** Inspected DocuSign's organizational charts to determine whether the Company has established lines of reporting.	No exceptions noted.
CG-02-01	DocuSign's policies, which define roles and responsibilities that support company objectives, are periodically reviewed, approved by management, and communicated to DocuSign personnel.	**Inspection** Inspected DocuSign's Security Policies and Procedures to determine whether DocuSign has established Policies and Procedures that defines roles and responsibilities and address Security,	No exceptions noted.

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		Availability, and Confidentiality objectives. Inspected DocuSign's Policy Bank to determine whether DocuSign Policies and Procedures were reviewed and approved periodically and communicated to DocuSign's personnel.	
CG-01-03	Changes to key areas of authority & responsibility, reorganizations or key new hires (for example: where the individual is a General Manager, VP level or above); are communicated throughout the applicable organizations via a written communication from the organizational leaders.	**Inspection** Inspected a sample of changes to DocuSign's key areas of authority & responsibility, reorganizations or key new hires (for example: where the individual is a General Manager, VP level or above) to determine whether changes were communicated to employees by organizational leaders.	No exceptions noted.
TPM-02-02	Customer roles and responsibilities which support DocuSign's information security objectives are communicated via a master services, or equivalent, agreement.	**Inspection** Inspected DocuSign's Master Service Agreement to determine whether the agreement included customer roles and responsibilities which support DocuSign's information security objectives.	No exceptions noted.
Trust Services Criteria 1.4: **COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**			

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
PR-01-01	As a condition of full-time employment, all future permanent employees are subject to a background check based on the criteria defined in the Company's background check policy(ies). Exceptions to proceed with onboarding an employee without a completed background check require review and approval and can be granted following certain circumstances.	**Inspection** Inspected a sample of new permanent employees to determine whether background verification checks were initiated, and results obtained before the employee's first day or if the results were not obtained there was review and approval from the authorized personnel.	No exceptions noted.
PR-01-03	All agency contractor personnel are subject to a background check based on the criteria defined in the Company's background check policy(ies). This requirement may be satisfied by background check(s) performed by the agency in the following circumstances: • The agency contractor has successfully completed a qualifying background check performed by the agency, • The agency contractor has remained continuously employed by the agency since the completion of the qualified background check, and • The agency contractor has successfully completed a global sanctions check in the 30 day period prior to commencing their assignment at DocuSign.	**Inspection** Inspected a sample of new agency contractor personnel to determine whether background verification checks were initiated based on the criteria defined in the Company's background check policy(ies) and the requirement was satisfied by background check(s) performed by the agency or if the results were not obtained there was review and approval from the Deputy GC or delegate.	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	Exceptions to proceed with onboarding an agency contractor without meeting these criteria or completing a DocuSign background check requires review and approval from Deputy GC or delegate and can be granted in the following circumstances: • the individual agency service provider has signed or is expected to sign in a timely manner the Code of Conduct and other policies presented as part of agency personnel onboarding process, and • a background check has been initiated for the individual agency service provider.		
TA-01-02	New hires are required to complete the Code of Conduct Certification or Training through online portal or other means.	**Inspection** Inspected a sample of new DocuSign employees to determine whether the Code of Conduct Certification or Training was completed.	No exceptions noted.
TA-01-01	Upon hire and on an annual basis, DocuSign employees complete security and privacy awareness trainings. Upon hire and on an annual basis, DocuSign contingent workers with access to systems, devices, or locations, complete security awareness training. Records of training completion are managed within DocuSign's selected Learning Management System.	**Inspection** Inspected the training records for a sample of new hires and employees, including contingent workers with access to systems, devices, or locations to determine whether the security and/or privacy awareness trainings were completed.	PwC Inspection Testing: No exceptions noted. Subsequent to PwC's inspection testing performed, management identified the following exceptions for individuals that did not complete the security and/or

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
			privacy awareness training: • fourteen (14) out of a sample of 25 existing contingent workers • twelve (12) out of a sample of 25 new contingent workers • one (1) out of a sample of 25 existing employees.
TA-02-01	On an annual basis, DocuSign employees, including contingent workers with access to systems, devices or locations, in development and QA roles are required to complete training on secure coding techniques.	**Inspection** Inspected the training records for a sample of employees, including contingent workers with access to systems, devices or locations, with product and QA roles to determine whether the training on secure coding techniques was completed. Inspected the Fundamental Coding Checklist to determine whether security awareness topics and best coding practice techniques were included.	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
CG-02-01	DocuSign's policies, which define roles and responsibilities that support company objectives, are periodically reviewed, approved by management, and communicated to DocuSign personnel.	**Inspection** Inspected DocuSign's Security Policies and Procedures to determine whether DocuSign has established Policies and Procedures that defines roles and responsibilities and address Security, Availability, and Confidentiality objectives. Inspected DocuSign's Policy Bank to determine whether DocuSign Policies and Procedures were reviewed and approved periodically and communicated to DocuSign's personnel.	No exceptions noted.
Trust Services Criteria 1.5: **COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**			
PR-01-02	DocuSign's employees and managers complete an annual assessment of employee performance. The assessment results are collaboratively reviewed between both parties to maintain alignment on role responsibilities and individual goals.	**Inspection** Inspected a sample of employees' performance assessments to determine whether the assessments were completed and reviewed to maintain alignment on role responsibilities and individual goals.	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
PR-03-01	Employees that fail to comply with DocuSign policies are subject to a disciplinary process.	**Inspection** Inspected DocuSign's Disciplinary Action Policy to determine whether disciplinary actions were defined. Inspected a sample of employees that failed to comply with DocuSign policies to determine whether they were subjected to a disciplinary process.	No exceptions noted.
TA-01-02	New hires are required to complete the Code of Conduct Certification or Training through online portal or other means.	**Inspection** Inspected a sample of new DocuSign employees to determine whether the Code of Conduct Certification or Training was completed.	No exceptions noted.
Control Environment			
Trust Services Criteria 2.1: **COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.**			
CG-02-01	DocuSign's policies, which define roles and responsibilities that support company objectives, are periodically reviewed, approved by management, and communicated to DocuSign personnel.	**Inspection** Inspected DocuSign's Security Policies and Procedures to determine whether DocuSign has established Policies and Procedures that defines roles and responsibilities and address Security, Availability, and Confidentiality objectives. Inspected DocuSign's Policy Bank to determine	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		whether DocuSign Policies and Procedures were reviewed and approved periodically and communicated to DocuSign's personnel.	
CFM-02-04	Systems are configured to synchronize information system time clocks based on authorized time sources; access to modify time data is restricted to authorized personnel.	**Inspection** Inspected DocuSign's network time configuration to determine whether the system was running the correct time configuration aligned with policy. Inspected the Quarterly Access Reviews for a sample of quarters to determine whether AD admin access was appropriately restricted.	No exceptions noted.
CG-02-01 (07)	DocuSign defines information classification and categorization levels to facilitate the appropriate protection of data.	**Inspection** Inspected DocuSign's Data Classification Standard to determine whether DocuSign defined information classification and categorization levels to facilitate the appropriate protection of data.	No exceptions noted.
SDD-01-01	System boundary documentation is maintained and communicated to authorized DocuSign personnel.	**Inspection** Inspected TechOps's internal documentation page to determine whether the system boundary documentation was maintained and communicated to the authorized DocuSign personnel.	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
Trust Services Criteria 2.2: **COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**			
CG-01-04	The Company has established appropriate lines of reporting, in part on the size and the nature of their activities, as evidenced by the functional group and organizational charts.	**Inspection** Inspected DocuSign's organizational charts to determine whether the Company has established lines of reporting.	No exceptions noted.
CG-02-01	DocuSign's policies, which define roles and responsibilities that support company objectives, are periodically reviewed, approved by management, and communicated to DocuSign personnel.	**Inspection** Inspected DocuSign's Security Policies and Procedures to determine whether DocuSign has established Policies and Procedures that defines roles and responsibilities and address Security, Availability, and Confidentiality objectives. Inspected DocuSign's Policy Bank to determine whether DocuSign Policies and Procedures were reviewed and approved periodically and communicated to DocuSign's personnel.	No exceptions noted.
TA-01-02	New hires are required to complete the Code of Conduct Certification or Training through online portal or other means.	**Inspection** Inspected a sample of new DocuSign employees to determine whether the Code of Conduct Certification or Training was completed.	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
TA-01-01	Upon hire and on an annual basis, DocuSign employees complete security and privacy awareness trainings. Upon hire and on an annual basis, DocuSign contingent workers with access to systems, devices, or locations, complete security awareness training. Records of training completion are managed within DocuSign's selected Learning Management System.	**Inspection** Inspected the training records for a sample of new hires and employees, including contingent workers with access to systems, devices, or locations to determine whether the security and/or privacy awareness trainings were completed.	PwC Inspection Testing: No exceptions noted. Subsequent to PwC's inspection testing performed, management identified the following exceptions for individuals that did not complete the security and/or privacy awareness training: • fourteen (14) out of a sample of 25 existing contingent workers • twelve (12) out of a sample of 25 new contingent workers • one (1) out of a sample of 25 existing employees.
TA-02-01	On an annual basis, DocuSign employees, including contingent workers with access to systems, devices or locations, in development and QA roles are required to complete	**Inspection** Inspected the training records for a sample of employees, including contingent workers with access to systems, devices or locations, with product	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	training on secure coding techniques.	and QA roles to determine whether the training on secure coding techniques was completed. Inspected the Fundamental Coding Checklist to determine whether security awareness topics and best coding practice techniques were included.	
CG-01-03	Changes to key areas of authority & responsibility, reorganizations or key new hires (for example: where the individual is a General Manager, VP level or above); are communicated throughout the applicable organizations via a written communication from the organizational leaders.	**Inspection** Inspected a sample of changes to DocuSign's key areas of authority & responsibility, reorganizations or key new hires (for example: where the individual is a General Manager, VP level or above) to determine whether changes were communicated to employees by organizational leaders.	No exceptions noted.
SDD-01-01	System boundary documentation is maintained and communicated to authorized DocuSign personnel.	**Inspection** Inspected TechOps's internal documentation page to determine whether the system boundary documentation was maintained and communicated to the authorized DocuSign personnel.	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
CG-03-01	The ISMS Owner conducts a formal management review of the DocuSign ISMS on an annual basis; key decisions relating to continual improvement and ISMS changes are documented and actioned.	**Inspection** Inspected the annual DocuSign ISMS Management Review meeting agenda to determine whether key decisions relating to continual improvement and ISMS changes were documented and actioned.	No exceptions noted.
CHM-01-01	Change scope, change type, and roles and responsibilities are pre-established within DocuSign's change control workflow. The following documentation is required, where applicable, for a change to be approved and committed into the DocuSign live environment: • change description • impact of change • test results • back-out plan • independent code review • change implementer • validation steps & success criteria	**Inspection** Inspected the Product Change Standard to determine whether defined change management procedures were in place to control changes to the IT environment. Inspected a sample of change release Envelopes to determine whether change description, impact of change, test results, back-out plan, independent code review, change implementer, validation steps & success criteria were documented and approved before the change was deployed.	No exceptions noted.
IR-02-03	DocuSign provides a contact method for external parties to: • submit complaints and inquiries • report incidents	**Inspection** Inspected DocuSign's external support site to determine whether DocuSign provided a contact method for external parties to submit complaints, inquiries, and incidents.	No exceptions noted.

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
SDD-02-01	DocuSign publishes product documentation to its public websites that describe the purpose, design, and functionality of the system.	**Observation** Observed DocuSign's Resource, Trust Center, and Product sites to determine whether product documentation was published on the public website and describe the purpose, design, and functionality of the system and system components.	No exceptions noted.
Trust Services Criteria 2.3: **COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.**			
TPM-02-01	DocuSign enters into legal agreements with suppliers. DocuSign ensures that each agreement imposes appropriate supplier obligations and responsibilities based on the services provided by the supplier that support DocuSign's information security, confidentiality, and privacy objectives, including, where applicable, required data privacy and security terms.	**Inspection** Inspected the DocuSign Supplier Service Agreement document to determine whether a policy document exists where suppliers agree to data protection guidelines. Inspected a sample of a recently signed Supplier Service Agreement to determine whether the document was properly reviewed by the Legal team and supplier.	No exceptions noted.
TPM-02-02	Customer roles and responsibilities which support DocuSign's information security objectives are communicated via a master services, or equivalent, agreement.	**Inspection** Inspected DocuSign's Master Service Agreement to determine whether the agreement included customer roles and responsibilities which support DocuSign's	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		information security objectives.	
CG-05-02	DocuSign contingent workers, agency contractors, and independent contractors consent to a Confidentiality or Non-Disclosure Agreement, Mobile Device Policy, and Code of Conduct. This is accomplished through either overarching MSA terms and conditions or individual signature of consent forms.	**Inspection** Inspected a sample of contingent workers, agency contractors, and independent contractors to determine whether the worker/contractor consented to the Confidentiality Agreement, Mobile Device Policy, and Code of Conduct as part of their onboarding.	No exceptions noted.
SDD-02-02	DocuSign publishes product documentation in guides to its public website, which defines implementation requirements for data input and output.	**Inspection** Inspected DocuSign's Support Center site to determine whether articles and guides were published on their public website that define the implementation requirements for data input and output.	No exceptions noted.
IR-02-02	In accordance with defined notification requirements, DocuSign communicates incident information to external stakeholders.	**Inquiry** Inquired with management to determine whether DocuSign would communicate incidents in accordance with defined notification requirements on the Alerts and System Status on DocuSign's Trust Center site. **Inspection**	There were no incidents that required external notification per DocuSign's requirements during the period. Therefore, the operating effectiveness of this control activity could not be tested.

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		Inspected the Board of Director meeting minutes to identify if there were any incidents that needed to be communicated to external stakeholders.	
IR-02-03	DocuSign provides a contact method for external parties to: • submit complaints and inquiries • report incidents	**Inspection** Inspected DocuSign's external support site to determine whether DocuSign provided a contact method for external parties to submit complaints, inquiries, and incidents.	No exceptions noted.
Risk Assessment			
Trust Services Criteria 3.1: **COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.**			
RM-01-01	At least annually, the Internal Audit Department performs or updates a risk assessment for the organization.	**Inspection** Inspected the annual risk assessment report to determine whether Internal Audit performed and updated the risk assessment for the organization on an annual basis.	No exceptions noted.
CG-01-07	As needed, Executive Staff meetings are held to review current operations, results, objectives/risks.	**Inspection** Inspected the agenda created for an Executive Staff meeting to determine	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		whether the following items were addressed in the meeting: current operations, results, and objectives/risks. Inspected an invitation to an Executive Staff meeting to determine whether executive staff members were listed as required attendees.	
CG-01-08	Quarterly, Management holds a Company meeting or conference call at Company headquarters. Key discussion items include (as applicable): Core Values, Strategy, Mission, and Critical Success Factors to focus on over the next quarter and remaining fiscal year. During the meeting, select Executives (CEO, CFO, VPs) provide an update of the quarter's activities, financial results and future goals.	**Inspection** Inspected the slide deck presented at a quarterly company All Hands meeting to determine whether the following discussion items are addressed: Core Values, Strategy, Mission, and Critical Success Factors and was presented by select Executives (CEO, CFO, VPs). Inspected an email sent to DocuSign employees to determine that DocuSign's employees are informed of the All Hands meeting and invited to attend. Inspected a sample of meeting minutes during the quarterly update to determine whether financial results and future goals were presented during the meeting.	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
Trust Services Criteria 3.2: **COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.**			
RM-01-01	At least annually, the Internal Audit Department performs or updates a risk assessment for the organization.	**Inspection** Inspected the annual risk assessment report to determine whether Internal Audit performed and updated the risk assessment for the organization on an annual basis.	No exceptions noted.
TPM-01-03	On a periodic basis, DocuSign reviews controls within third party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address any impact the disclosed gaps have on the organization.	**Inspection** Inspected evidence of management review of SOC reports from subservice organizations to determine whether management assessed the design and operating effectiveness of relevant controls implemented at subservice organizations and to determine whether design or operating effectiveness gaps were assessed and addressed by management.	No exceptions noted.
TPM-01-02	DocuSign performs a risk assessment and reviews the security and privacy practices of suppliers who access, collect, process, transfer, or store data on behalf of DocuSign; non-compliance is tracked through remediation.	**Inspection** Inspected a sample of new suppliers who access, collect, process, transfer, or store data on behalf of DocuSign to determine whether DocuSign performed a risk assessment and reviewed their security and privacy practices and that non-	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		compliance was tracked through remediation, if applicable.	
Trust Services Criteria 3.3: **COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.**			
CG-01-02	DocuSign's Board of Directors provides strategic oversight via: • periodic meetings to discuss management's decisions, major transactions, and past results • quarterly board meetings to align on core values, strategy, and mission	**Inspection** Inspected a sample of quarterly Board of Directors meeting minutes and All Hands meeting agendas to determine whether DocuSign's Board of Directors provide strategic oversight through periodic meetings to discuss management's decisions, major transactions, and past results and quarterly board meetings to align core values, strategy, and mission.	No exceptions noted.
RM-05-01	Annually, Internal Audit performs a fraud risk assessment for the organization. As a result of the assessment, the IA team communicates the result to the Legal and AC team as necessary. The assessment is reviewed and approved by the Chief Accounting Officer (CAO).	**Inspection** Inspected the fraud risk assessment to determine whether the results of the assessment were communicated to the Legal team and the Audit Committee as necessary. Inspected the fraud risk assessment to determine whether the risk assessment was reviewed and approved by the Chief Accounting Officer (CAO).	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
RM-01-01	At least annually, the Internal Audit Department performs or updates a risk assessment for the organization.	**Inspection** Inspected the annual risk assessment report to determine whether Internal Audit performed and updated the risk assessment for the organization on an annual basis.	No exceptions noted.
CG-01-06	The Company has adopted a Whistleblower and Complaint Policy for employees of the Company. The Policy is available via the Company's Intranet Site and helps to ensure that the Company maintains a workplace where employees, who reasonably believe that they are aware of questionable accounting, auditing, and internal controls and disclosure practices, can raise their concern free of any harassment, discrimination or retaliation. Concern can be raised directly to a HR Business Partner or Compliance Officer or anonymously through a confidential complaints hotline directed to the Compliance Officer and/or Chairman of the Audit Committee. Hotline reports are reviewed and assessed by the Audit Committee.	**Inspection** Inspected the Whistleblower and Complaint Policy for evidence of review and approval. Inspected DocuSign's Policy Bank to determine whether DocuSign employees were able to access and view the Whistleblower and Complaint Policy. Inspected a sample of quarterly Audit Committee minutes to determine whether confidential complaints were reviewed and assessed by the Audit Committee. **Observation** Observed a test complaint submitted through the confidential complaints hotline to determine whether the complaint was communicated to the Compliance Officer and/or Chairman of the Audit Committee.	No exceptions noted.

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
TPM-01-02	DocuSign performs a risk assessment and reviews the security and privacy practices of suppliers who access, collect, process, transfer, or store data on behalf of DocuSign; non-compliance is tracked through remediation.	**Inspection** Inspected a sample of new suppliers who access, collect, process, transfer, or store data on behalf of DocuSign to determine whether DocuSign performed a risk assessment and reviewed their security and privacy practices and that non-compliance was tracked through remediation, if applicable.	No exceptions noted.
Trust Services Criteria 3.4: **COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.**			
RM-01-01	At least annually, the Internal Audit Department performs or updates a risk assessment for the organization.	**Inspection** Inspected the annual risk assessment report to determine whether Internal Audit performed and updated the risk assessment for the organization on an annual basis.	No exceptions noted.
TPM-01-02	DocuSign performs a risk assessment and reviews the security and privacy practices of suppliers who access, collect, process, transfer, or store data on behalf of DocuSign; non-compliance is tracked through remediation.	**Inspection** Inspected a sample of new suppliers who access, collect, process, transfer, or store data on behalf of DocuSign to determine whether DocuSign performed a risk assessment and reviewed their security and privacy practices and that non-compliance was tracked through remediation, if applicable.	No exceptions noted.

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
TPM-01-03	On a periodic basis, DocuSign reviews controls within third party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address any impact the disclosed gaps have on the organization.	**Inspection** Inspected evidence of management review of SOC reports from subservice organizations to determine whether management assessed the design and operating effectiveness of relevant controls implemented at subservice organizations and to determine whether design or operating effectiveness gaps were assessed and addressed by management.	No exceptions noted.
Monitoring Activities			
Trust Services Criteria 4.1:COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CG-01-07	As Needed, Executive Staff meetings are held to review current operations, results, objectives/risks.	**Inspection** Inspected the agenda created for an Executive Staff meeting to determine whether the following items were addressed in the meeting: current operations, results, and objectives/risks. Inspected an invitation to an Executive Staff meeting to determine whether executive staff members were listed as required attendees.	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
RM-01-01	At least annually, the Internal Audit Department performs or updates a risk assessment for the organization.	**Inspection** Inspected the annual risk assessment report to determine whether Internal Audit performed and updated the risk assessment for the organization on an annual basis.	No exceptions noted.
SM-06-01	Capacity planning and analysis is periodically performed by DocuSign management to maintain the reliability, performance, and capacity of systems required for the operation of DocuSign's live environment.	**Inspection** Inspected a sample of DocuSign management's monthly capacity planning and analysis meetings to determine whether the review assessed the reliability, performance, and capacity of systems required for the operation of DocuSign's live environment. Inspected a sample of DocuSign management's monthly capacity planning and analysis meeting deck to determine whether follow-up action was identified to enable the implementation of additional capacity.	No exceptions noted.
VM-02-01	DocuSign facilitates a penetration test, which validates network segmentation, on an annual basis.	**Inspection** Inspected the annual third-party application penetration testing reports to determine whether assessment was performed on an annual basis. Inspected the annual penetration test reports to	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		determine whether the identified vulnerabilities were assessed by management and resolved timely.	
Trust Services Criteria 4.2: **COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.**			
RM-03-01	Management prepares a remediation plan to manage the resolution of nonconformities identified during audits that are executed as part of the annual audit plan.	**Inspection** Inspected the results of completed technical audits to determine whether management prepared a remediation plan for nonconformities identified, if any.	No exceptions noted.
CG-03-01	The ISMS Owner conducts a formal management review of the DocuSign ISMS on an annual basis; key decisions relating to continual improvement and ISMS changes are documented and actioned.	**Inspection** Inspected the annual DocuSign ISMS Management Review meeting agenda to determine whether key decisions relating to continual improvement and ISMS changes were documented and actioned.	No exceptions noted.
CG-01-06	The Company has adopted a Whistleblower and Complaint Policy for employees of the Company. The Policy is available via the Company's Intranet Site and helps to ensure that the Company maintains a workplace where employees, who reasonably believe that they are aware of questionable accounting, auditing, and internal controls and disclosure	**Inspection** Inspected the Whistleblower and Complaint Policy for evidence of review and approval. Inspected DocuSign's Policy Bank to determine whether DocuSign employees were able to access and view the	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	practices, can raise their concern free of any harassment, discrimination or retaliation. Concern can be raised directly to a HR Business Partner or Compliance Officer or anonymously through a confidential complaints hotline directed to the Compliance Officer and/or Chairman of the Audit Committee. Hotline reports are reviewed and assessed by the Audit Committee.	Whistleblower and Complaint Policy. Inspected a sample of quarterly Audit Committee minutes to determine whether confidential complaints were reviewed and assessed by the Audit Committee. **Observation** Observed a test complaint submitted through the confidential complaints hotline to determine whether the complaint was communicated to the Compliance Officer and/or Chairman of the Audit Committee.	
CG-02-05	Quarterly, review of any exceptions and granting of exceptions to the Code of Conduct relating to Executive Officers or Directors and other governance items is reviewed in the Standing Audit Committee Meeting.	**Inquiry** Inquired with management to determine whether any exceptions and granting of exceptions to the Code of Conduct relating to Executive Officers or Directors and other governance items is reviewed in the quarterly Standing Audit Committee Meeting. **Inspection** Inspected the quarterly Standing Audit Committee Meeting minutes to identify if there were any exceptions and granting of exceptions to the Code of Conduct relating to Executive Officers or Directors and	There were no exceptions and granting of exceptions to the Code of Conduct relating to Executive Officers or Directors and other governance items requested during the period. Therefore, the operating effectiveness of this control activity could not be tested.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		other governance items during the period.	
TPM-01-03	On a periodic basis, DocuSign reviews controls within third party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address any impact the disclosed gaps have on the organization.	**Inspection** Inspected evidence of management review of SOC reports from subservice organizations to determine whether management assessed the design and operating effectiveness of relevant controls implemented at subservice organizations and to determine whether design or operating effectiveness gaps were assessed and addressed by management.	No exceptions noted.
Control Activities			
Trust Services Criteria 5.1 **COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.**			
RM-01-01	At least annually, the Internal Audit Department performs or updates a risk assessment for the organization.	**Inspection** Inspected the annual risk assessment report to determine whether Internal Audit performed and updated the risk assessment for the	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		organization on an annual basis.	
TPM-01-02	DocuSign performs a risk assessment and reviews the security and privacy practices of suppliers who access, collect, process, transfer, or store data on behalf of DocuSign; non-compliance is tracked through remediation.	**Inspection** Inspected a sample of new suppliers who access, collect, process, transfer, or store data on behalf of DocuSign to determine whether DocuSign performed a risk assessment and reviewed their security and privacy practices and that non-compliance was tracked through remediation, if applicable.	No exceptions noted.
TPM-01-03	On a periodic basis, DocuSign reviews controls within third party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address any impact the disclosed gaps have on the organization.	**Inspection** Inspected evidence of management review of SOC reports from subservice organizations to determine whether management assessed the design and operating effectiveness of relevant controls implemented at subservice organizations and to determine whether design or operating effectiveness gaps were assessed and addressed by management.	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
RM-05-01	Annually, Internal Audit performs a fraud risk assessment for the organization. As a result of the assessment, the IA team communicates the result to the Legal and AC team as necessary. The assessment is reviewed and approved by the Chief Accounting Officer (CAO).	**Inspection** Inspected the fraud risk assessment to determine whether the results of the assessment were communicated to the Legal team and the Audit Committee as necessary. Inspected the fraud risk assessment to determine whether the risk assessment was reviewed and approved by the Chief Accounting Officer (CAO).	No exceptions noted.
Trust Services Criteria 5.2 **COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.**			
CG-02-03	DocuSign reviews exceptions to policies; exceptions are documented and approved based on business need and removed when no longer required.	**Inspection** Inspected the policy exception listing to determine if there were any policy exceptions granted and removed when no longer required during the period.	There were no exceptions to policies requested and removed during the period. Therefore, the operating effectiveness of this control activity could not be tested.
TPM-01-02	DocuSign performs a risk assessment and reviews the security and privacy practices of suppliers who access, collect, process, transfer, or store data on behalf of DocuSign; non-compliance is tracked through remediation.	**Inspection** Inspected a sample of new suppliers who access, collect, process, transfer, or store data on behalf of DocuSign to determine whether DocuSign performed a risk assessment and reviewed their security and privacy practices and that non-compliance was tracked	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		through remediation, if applicable.	
TPM-01-03	On a periodic basis, DocuSign reviews controls within third party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address any impact the disclosed gaps have on the organization.	**Inspection** Inspected evidence of management review of SOC reports from subservice organizations to determine whether management assessed the design and operating effectiveness of relevant controls implemented at subservice organizations and to determine whether design or operating effectiveness gaps were assessed and addressed by management.	No exceptions noted.
Trust Services Criteria 5.3 **COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**			
CG-02-01	DocuSign's policies, which define roles and responsibilities that support company objectives, are periodically reviewed, approved by management, and communicated to DocuSign personnel.	**Inspection** Inspected DocuSign's Security Policies and Procedures to determine whether DocuSign has established Policies and Procedures that defines roles and responsibilities and address Security, Availability, and Confidentiality objectives. Inspected DocuSign's Policy Bank to determine whether DocuSign Policies	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		and Procedures were reviewed and approved periodically and communicated to DocuSign's personnel.	
CG-02-03	DocuSign reviews exceptions to policies; exceptions are documented and approved based on business need and removed when no longer required.	**Inspection** Inspected the policy exception listing to determine if there were any policy exceptions granted during the period.	There were no exceptions to policies requested during the period. Therefore, the operating effectiveness of this control activity could not be tested.
PR-01-02	DocuSign's employees and managers complete an annual assessment of employee performance. The assessment results are collaboratively reviewed between both parties to maintain alignment on role responsibilities and individual goals.	**Inspection** Inspected a sample of employees' performance assessments to determine whether the assessments were completed and reviewed to maintain alignment on role responsibilities and individual goals.	No exceptions noted.
PR-03-01	Employees that fail to comply with DocuSign policies are subject to a disciplinary process.	**Inspection** Inspected DocuSign's Disciplinary Action Policy to determine whether disciplinary actions were defined. Inspected a sample of employees that failed to comply with DocuSign policies to determine whether they were subjected to a disciplinary process.	No exceptions noted.
TA-01-02	New hires are required to complete the Code of	**Inspection**	No exceptions noted.

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	Conduct Certification or Training through online portal or other means.	Inspected a sample of new DocuSign employees to determine whether the Code of Conduct Certification or Training was completed.	
RM-05-01	Annually, Internal Audit performs a fraud risk assessment for the organization. As a result of the assessment, the IA team communicates the result to the Legal and AC team as necessary. The assessment is reviewed and approved by the Chief Accounting Officer (CAO).	**Inspection** Inspected the fraud risk assessment to determine whether the results of the assessment were communicated to the Legal team and the Audit Committee as necessary. Inspected the fraud risk assessment to determine whether the risk assessment was reviewed and approved by the Chief Accounting Officer (CAO).	No exceptions noted.
Logical and Physical Access Controls			
Trust Services Criteria 6.1 **The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.**			
DM-04-02	DocuSign encrypts sensitive data including uploaded Documents and their associated form data and signatures at rest.	**Inspection** Inspected the configuration to determine whether customer data was stored as BLOB using AES256 encryption. Inspected a sample of a BLOB object on the NAS server to determine whether data was encrypted and non-readable while at rest. Inspected the configuration of the HSM Private Server	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		to determine whether it was set to the FIPS Mode for hardware security module ("HSM").	
DM-06-05	DocuSign Envelopes are accessed via unique URLs which are delivered to authorized Recipients, or by authenticating to the DocuSign API or DocuSign Web Application.	**Observation** Observed a sample of signing Envelopes to determine whether Recipients were accurately authenticated based on the unique URL. Observed a user who was not sent the envelope clicking the Sender or Recipient's unique URL to determine whether they could not access the Envelope.	No exceptions noted.
IAM-02-01	DocuSign requires unique identifiers for user accounts and prevents identifier reuse.	**Inspection** Inspected DocuSign Technical Operations Procedure to determine whether DocuSign required a unique identification mechanism for access to programs, transactions, and data, and prohibited the use of shared accounts or passwords. **Observation** Observed the configuration to determine whether unique identifiers were required for user accounts and identifier reuse was prevented.	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
IAM-02-02	Access to the DocuSign live environment is restricted to identified and authenticated accounts. User and device authentication to DocuSign's internal information systems is protected by passwords that meet DocuSign's password complexity requirements.	**Inspection** Inspected DocuSign's password configuration for user and device authentication to DocuSign's internal information system to determine whether the password configuration complied with DocuSign's password complexity requirements.	No exceptions noted.
IAM-02-03	DocuSign applications secure user data and maintain confidentiality by default or according to permissions set by the individual; DocuSign authenticates individuals with unique identifiers and passwords prior to enabling access to the application or their data.	**Observation** Observed a DocuSign user log into the System to determine whether DocuSign authenticates individuals with unique identifiers and passwords prior to enabling them access to the application or their data. **Inspection** Inspected the password parameters for Basic, Medium, Strong, and Custom password policies to determine whether the password policies adhere to DocuSign's policy for Basic, Medium, Strong, and Custom.	No exceptions noted.
IAM-02-04	Multi-factor authentication is required for: • remote VPN sessions • access to live environments	**Observation** Observed a DocuSign Technical Operations team member attempt to start a remote VPN session and access servers on the production network to	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		determine whether multi-factor authentication was required to gain access.	
IAM-03-01	Access to modify source code is restricted to authorized personnel.	**Inspection** Inspected a sample of GitHub quarterly system access review to determine whether access to modify source code was restricted to authorized personnel and the users who maintained access to the system were appropriate.	No exceptions noted.
KM-01-01	Access to the cryptographic keystores is limited to authorized personnel.	**Inspection** Inspected a sample of quarterly access reviews to determine whether access to the cryptographic keystores was limited to authorized personnel.	No exceptions noted.
KM-02-05	API Integrator keys must process the minimum number of successful API test transactions prior to being deployed to the live environment.	**Inspection** Inspected API integrator key test checklists for a sample of new or modified API integrator keys to determine whether API integrator keys were tested and passed a minimum amount of test transactions prior to promotion into production.	No exceptions noted.
NO-01-01	Network traffic to and from untrusted networks passes through a DMZ; firewall rules are established in accordance to identified	**Inspection** Inspected a review of the recent network segmentation diagrams to	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	security requirements and business justifications are reviewed on a semiannual basis.	determine whether traffic was designed to pass through a demilitarized zone. Inspected a sample of semi-annual review of firewall rules to determine whether the firewall configurations were reviewed by management against identified security requirements and business justifications.	**Exception Noted:** For one (1) of one (1) semiannual review selected for testing, the firewall rules review was not performed.
NO-01-02	Changes to firewalls follow DocuSign's change management process, which includes review and approval before being implemented.	**Inspection** Inspected a sample of changes to firewalls to determine whether the changes followed DocuSign's change management process which includes review and approval before being implemented.	No exceptions noted.
NO-01-04	Account actions performed via API calls are limited to authorized integrator keys.	**Inspection** Inspected a sample invalid integrator key to determine whether the API call was not authenticated. Inspected a sample valid integrator key to determine whether the API call was successful.	No exceptions noted.
NO-02-01	Production environments are: • segregated from corporate environments • logically separated from the staging environment	**Inspection** Inspected DocuSign's network diagram to determine whether the production network was segregated from the	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		corporate network and were logically separated from the staging environment. Inspected URL addresses of production, staging and demo environment to determine whether DocuSign production and stage environments were logically separated. **Observation** Observed a DocuSign engineer attempt to access a production server while logged into DocuSign's corporate environment to determine whether the corporate and production environments were segregated.	
NO-03-01	Wireless access to the DocuSign network within the data centers is prohibited. On a quarterly basis, DocuSign performs scanning to identify and remove unauthorized wireless access points.	**Inspection** Inspect a sample of quarterly reviews of the wireless network scans to determine whether DocuSign production scan occurred and if any unauthorized wireless access points were identified they were removed.	No exceptions noted.
IAM-01-02	HR or respective personnel manager notifies IT of terminated users. A termination checklist is completed via email and user access is revoked.	**Inspection** Inspected a sample of terminated users to determine whether access was revoked, and a termination checklist was completed.	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
IAM-01-03	DocuSign performs account and access reviews on a quarterly basis; corrective action is taken where applicable.	**Inspection** Inspected a sample of quarterly reviews of user access to determine whether the reviews were performed by appropriate personnel and that any identified inappropriate access rights were removed in a timely manner as a result of the review.	No exceptions noted.
Trust Services Criteria 6.2 **Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.**			
IAM-01-01	Logical access provisioning to information systems is based on the concept of least privilege and requires approval from authorized personnel prior to provisioning system access; permissions are granted based on the documented and approved access request.	**Inspection** Inspected a sample of users granted access to production to determine whether users were approved by the VP of Technical Operations or designee prior to provisioning.	No exceptions noted.
IAM-01-03	DocuSign performs account and access reviews on a quarterly basis; corrective action is taken where applicable.	**Inspection** Inspected a sample of quarterly reviews of user access to determine whether the reviews were performed by appropriate personnel and that any identified inappropriate access rights were removed	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		in a timely manner as a result of the review.	
IAM-01-02	HR or respective personnel manager notifies IT of terminated users. A termination checklist is completed via email and user access is revoked.	**Inspection** Inspected a sample of terminated users to determine whether access was revoked, and a termination checklist was completed.	No exceptions noted.
Trust Services Criteria 6.3 **The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.**			
CHM-01-01	Change scope, change type, and roles and responsibilities are pre-established within DocuSign's change control workflow. The following documentation is required, where applicable, for a change to be approved and committed into the DocuSign live environment: • change description • impact of change • test results • back-out plan • independent code review • change implementer • validation steps & success criteria	**Inspection** Inspected the Product Change Standard to determine whether defined change management procedures were in place to control changes to the IT environment. Inspected a sample of change release Envelopes to determine whether change description, impact of change, test results, back-out plan, independent code review, change implementer, validation steps & success criteria were documented and approved before the change was deployed.	No exceptions noted.
IAM-01-01	Logical access provisioning to information systems is based on the concept of least privilege and requires approval from authorized personnel prior to	**Inspection** Inspected a sample of users granted access to production to determine whether users were	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	provisioning system access; permissions are granted based on the documented and approved access request.	approved by the VP of Technical Operations or designee prior to provisioning.	
IAM-01-03	DocuSign performs account and access reviews on a quarterly basis; corrective action is taken where applicable.	**Inspection** Inspected a sample of quarterly reviews of user access to determine whether the reviews were performed by appropriate personnel and that any identified inappropriate access rights were removed in a timely manner as a result of the review.	No exceptions noted.
TPM-01-03	On a periodic basis, DocuSign reviews controls within third party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address any impact the disclosed gaps have on the organization.	**Inspection** Inspected evidence of management review of SOC reports from subservice organizations to determine whether management assessed the design and operating effectiveness of relevant controls implemented at subservice organizations and to determine whether design or operating effectiveness gaps were assessed and addressed by management.	No exceptions noted.
IAM-01-02	HR or respective personnel manager notifies IT of terminated users. A termination checklist is completed via email and user access is revoked.	**Inspection** Inspected a sample of terminated users to determine whether access was revoked, and a termination checklist was completed.	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
Trust Services Criteria 6.4 **The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.**			
SO-02-01	Physical access provisioning requires management approval and documented specification of: • access privileges granted • intended business purpose	**Inspection** Inspected a sample of physical access requests to determine whether it was documented and approved.	No exceptions noted.
SO-02-03	DocuSign performs physical account and access reviews on a quarterly basis; corrective action is taken where applicable.	**Inspection** Inspected a sample of quarterly physical access reviews to determine whether physical account and access reviews were performed, and corrective action was taken where applicable.	No exceptions noted.
TPM-01-03	On a periodic basis, DocuSign reviews controls within third party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address any impact the disclosed gaps have on the organization.	**Inspection** Inspected evidence of management review of SOC reports from subservice organizations to determine whether management assessed the design and operating effectiveness of relevant controls implemented at subservice organizations and to determine whether design or operating effectiveness gaps were assessed and addressed by management.	No exceptions noted.
Trust Services Criteria 6.5 **The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.**			

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
DM-07-01	DocuSign securely destroys media authorized to be decommissioned or purges stored data from media authorized to be repurposed.	**Inspection** Inspected the certificate of destruction for a sample of decommissioned media to determine whether the media was securely destroyed, and the stored data was purged.	No exceptions noted.
SO-02-03	DocuSign performs physical account and access reviews on a quarterly basis; corrective action is taken where applicable.	**Inspection** Inspected a sample of quarterly physical access reviews to determine whether physical account and access reviews were performed, and corrective action was taken where applicable.	No exceptions noted.
TPM-01-03	On a periodic basis, DocuSign reviews controls within third party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address any impact the disclosed gaps have on the organization.	**Inspection** Inspected evidence of management review of SOC reports from subservice organizations to determine whether management assessed the design and operating effectiveness of relevant controls implemented at subservice organizations and to determine whether design or operating effectiveness gaps were assessed and addressed by management.	No exceptions noted.
Trust Services Criteria 6.6 **The entity implements logical access security measures to protect against threats from sources outside its system boundaries.**			
IAM-02-02	Access to the DocuSign live environment is restricted to identified and authenticated accounts. User and device	**Inspection** Inspected DocuSign's password configuration for	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	authentication to DocuSign's internal information systems is protected by passwords that meet DocuSign's password complexity requirements.	user and device authentication to DocuSign's internal information system to determine whether the password configuration complied with DocuSign's password complexity requirements.	
IAM-02-03	DocuSign applications secure user data and maintain confidentiality by default or according to permissions set by the individual; DocuSign authenticates individuals with unique identifiers and passwords prior to enabling access to the application or their data.	**Observation** Observed a DocuSign user log into the System to determine whether DocuSign authenticates individuals with unique identifiers and passwords prior to enabling them access to the application or their data. **Inspection** Inspected the password parameters for Basic, Medium, Strong, and Custom password policies to determine whether the password policies adhere to DocuSign's policy for Basic, Medium, Strong, and Custom.	No exceptions noted.
NO-01-01	Network traffic to and from untrusted networks passes through a DMZ; firewall rules are established in accordance to identified security requirements and business justifications are reviewed on a semiannual basis.	**Inspection** Inspected a review of the recent network segmentation diagrams to determine whether traffic was designed to pass through a demilitarized zone.	No exceptions noted. **Exception Noted:** For one (1) of one (1) semiannual review selected for testing, the firewall rules review was not performed.

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		Inspected a sample of semi-annual review of firewall rules to determine whether the firewall configurations were reviewed by management against identified security requirements and business justifications.	
NO-01-02	Changes to firewalls follow DocuSign's change management process, which includes review and approval before being implemented.	**Inspection** Inspected a sample of changes to firewalls to determine whether the changes followed DocuSign's change management process which includes review and approval before being implemented.	No exceptions noted.
Trust Services Criteria 6.7 **The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.**			
DM-04-01	DocuSign's transmission of data over public networks is encrypted.	**Inspection** Inspected the certificate website details to determine whether HTTPS/TLS certificate was used and current.	No exceptions noted.
Trust Services Criteria 6.8 **The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.**			
CHM-01-01	Change scope, change type, and roles and responsibilities are pre-established within DocuSign's change control workflow. The following documentation is required, where applicable, for a	**Inspection** Inspected the Product Change Standard to determine whether defined change management procedures were in place to control changes to the IT	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	change to be approved and committed into the DocuSign live environment: • change description • impact of change • test results • back-out plan • independent code review • change implementer • validation steps & success criteria.	environment. Inspected a sample of change release Envelopes to determine whether change description, impact of change, test results, back-out plan, independent code review, change implementer, validation steps & success criteria were documented and approved before the change was deployed.	
CHM-01-04	Prior to an infrastructure change, systems must pass a security acceptance review, which identifies unsafe or unauthorized configurations, including default vendor credentials.	**Inspection** Inspected the executed security acceptance review template for a sample of deployments to determine whether the proper review had been performed before the actual deployment, including checking safe/unauthorized configurations or including default vendor credentials.	No exceptions noted.
SM-03-01	DocuSign defines security monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel to receive and respond to alerts.	**Inspection** Inspected DocuSign's Incident Management Standard and Information Security Policy to determine whether DocuSign had defined security monitoring alert criteria to be flagged and had identified authorized personnel for flagged system alerts.	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
SM-04-01	Critical systems are monitored in accordance to predefined security criteria and alerts are sent to authorized personnel.	**Inspection** Inspected the configuration of the SIEM to determine whether critical systems were monitored in accordance to predefined security criteria and alerts were generated and sent authorized personnel when incidents were identified.	No exceptions noted.
SM-05-01	Intrusion detection systems are deployed between DocuSign networks and untrusted networks, and are configured to ensure: • signature definitions are up-to-date • the system captures signature malicious traffic • alerts are reviewed and resolved by authorized personnel.	**Inspection** Inspected the configuration of the intrusion detection system to determine whether signature definitions were updated on a daily basis. Inspected the configuration of the SIEM to determine whether authorized personnel were alerted if any incidents are detected. Inspected a sample of incident tickets to determine whether actions were taken to prioritize, investigate, and resolve each incident.	No exceptions noted.
VM-04-01	DocuSign has managed enterprise antivirus deployments and ensures the following: • signature definitions are updated automatically • scans are scheduled to run on a periodic basis • audit logs are forwarded to a centralized repository • alerts are reviewed and resolved by authorized	**Inspection** Inspected DocuSign policies and procedures to determine whether antivirus software was required to be installed on production systems. Inspected the antivirus configuration for a sample of DocuSign production	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	personnel • real-time scanning is performed on files received from external sources.	servers to determine whether antivirus software was installed with signature definitions and configured to update automatically, scheduled to run daily, and configured for real-time scanning on files received from external sources. Inspected antivirus software settings to determine whether scans were performed daily and alerts were sent to the Security team for resolution. Inspected a sample of incident tickets to determine whether the incident was assigned a priority level, investigated, and resolved.	
System Operations			
Trust Services Criteria 7.1 **To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.**			
CHM-01-04	Prior to an infrastructure change, systems must pass a security acceptance review, which identifies unsafe or unauthorized configurations, including default vendor credentials.	**Inspection** Inspected the executed security acceptance review template for a sample of deployments to determine whether the proper review had been performed before the actual deployment, including checking safe/unauthorized configurations or including default vendor credentials.	No exceptions noted.
SM-03-01	DocuSign defines security monitoring alert criteria, how alert criteria will be flagged,	**Inspection** Inspected DocuSign's	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	and identifies authorized personnel to receive and respond to alerts.	Incident Management Standard and Information Security Policy to determine whether DocuSign had defined security monitoring alert criteria to be flagged and had identified authorized personnel for flagged system alerts.	
SM-04-01	Critical systems are monitored in accordance to predefined security criteria and alerts are sent to authorized personnel.	**Inspection** Inspected the configuration of the SIEM to determine whether critical systems were monitored in accordance to predefined security criteria and alerts were generated and sent authorized personnel when incidents were identified.	No exceptions noted.
SM-05-01	Intrusion detection are deployed between DocuSign networks and untrusted networks, and are configured to ensure: • signature definitions are up-to-date • the system captures signature and non-signature malicious traffic • alerts are reviewed and resolved by authorized personnel.	**Inspection** Inspected the configuration of the intrusion detection system to determine whether signature definitions were updated on a daily basis. Inspected the configuration of the SIEM to determine whether authorized personnel were alerted if any incidents are detected. Inspected a sample of incident tickets to determine whether actions were taken to prioritize, investigate, and resolve each incident.	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
VM-01-01	DocuSign periodically updates vulnerability scanning tools used to conduct scans against the live environment.	**Inspection** Inspected a sample of monthly network scans to determine whether DocuSign periodically updates vulnerability scanning tools used to conduct scans against the live environment.	No exceptions noted.
VM-02-01	DocuSign facilitates a penetration test, which validates network segmentation, on an annual basis.	**Inspection** Inspected the annual third-party application penetration testing reports to determine whether assessment was performed on an annual basis. Inspected the annual penetration test reports to determine whether the identified vulnerabilities were assessed by management and resolved timely.	No exceptions noted.
VM-03-01	Vulnerability scans are performed weekly on the environment to identify control gaps and vulnerabilities.	**Inspection** Inspected a sample of weekly network scans to determine whether DocuSign performed monthly system security scans to identify vulnerable software or firmware.	No exceptions noted.
VM-05-02	On a recurring basis, DocuSign conducts dynamic vulnerability scans against web applications prior to deployment into live environments.	**Inspection** Inspected a sample of vulnerability scans to determine whether the scans were performed against web applications	No exceptions noted.

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		prior to deployment into live environments.	
Trust Services Criteria 7.2 **The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.**			
CHM-01-04	Prior to an infrastructure change, systems must pass a security acceptance review, which identifies unsafe or unauthorized configurations, including default vendor credentials.	**Inspection** Inspected the executed security acceptance review template for a sample of deployments to determine whether the proper review had been performed before the actual deployment, including checking safe/unauthorized configurations or including default vendor credentials.	No exceptions noted.
IR-01-02	Confirmed incidents are assigned a priority level, investigated, and resolved.	**Inspection** Inspected a sample of incident tickets to determine whether the incident was assigned a priority level, investigated, and resolved.	No exceptions noted.
SM-03-01	DocuSign defines security monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel to receive and respond to alerts.	**Inspection** Inspected DocuSign's Incident Management Standard and Information Security Policy to determine whether DocuSign had defined security monitoring alert criteria to be flagged	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		and had identified authorized personnel for flagged system alerts.	
SM-04-01	Critical systems are monitored in accordance to predefined security criteria and alerts are sent to authorized personnel.	**Inspection** Inspected the configuration of the SIEM to determine whether critical systems were monitored in accordance to predefined security criteria and alerts were generated and sent authorized personnel when incidents were identified.	No exceptions noted.
SM-05-01	Intrusion detection systems are deployed between DocuSign networks and untrusted networks, and are configured to ensure: • signature definitions are up-to-date • the system captures signature and non-signature malicious traffic • alerts are reviewed and resolved by authorized personnel.	**Inspection** Inspected the configuration of the intrusion detection system to determine whether signature definitions were updated on a daily basis. Inspected the configuration of the SIEM to determine whether authorized personnel were alerted if any incidents are detected. Inspected a sample of incident tickets to determine whether actions were taken to prioritize, investigate, and resolve each incident.	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
RM-01-01	At least annually, the Internal Audit Department performs or updates a risk assessment for the organization.	**Inspection** Inspected the annual risk assessment report to determine whether Internal Audit performed and updated the risk assessment for the organization on an annual basis.	No exceptions noted.
VM-02-01	DocuSign facilitates a penetration test, which validates network segmentation, on an annual basis.	**Inspection** Inspected the annual third-party application penetration testing reports to determine whether assessment was performed on an annual basis. Inspected the annual penetration test reports to determine whether the identified vulnerabilities were assessed by management and resolved timely.	No exceptions noted.
Trust Services Criteria 7.3 **The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.**			
IR-01-01	DocuSign defines the procedures required to manage, track, and report incidents.	**Inspection** Inspected the Information Security Policy and Incident Management Standard to determine whether there were procedures to manage, track, and report incidents.	No exceptions noted.
IR-01-01 (01)	DocuSign documents and tests incident response	**Inspection** Inspected the incident	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	processes on an annual basis.	response processes to determine whether DocuSign documented and tested the processes on an annual basis.	
IR-01-02	Confirmed incidents are assigned a priority level, investigated, and resolved.	**Inspection** Inspected a sample of incident tickets to determine whether the incident was assigned a priority level, investigated, and resolved.	No exceptions noted.
IR-01-02 (02)	DocuSign performs a root cause analysis for high degradation incidents to detect and correct or prevent prior incidents from recurring.	**Inspection** Inspected evidence of a Root Cause Analysis (RCA) performed for a sample of high degradation incidents to determine whether corrective and preventive actions were taken.	No exceptions noted.
VM-09-01	DocuSign assigns a risk rating to identified vulnerabilities and prioritizes remediation of legitimate vulnerabilities according to the assigned risk.	**Inspection** Inspected a sample of identified vulnerabilities to determine whether DocuSign assigned a risk rating to prioritize the remediation efforts of legitimate vulnerabilities.	No exceptions noted.
SM-04-01	Critical systems are monitored in accordance to predefined security criteria and alerts are sent to authorized personnel.	**Inspection** Inspected the configuration of the SIEM to determine whether critical systems were monitored in accordance to predefined security criteria and alerts were generated and sent authorized personnel when incidents were identified.	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
Trust Services Criteria 7.4 **The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.**			
IR-01-01	DocuSign defines the procedures required to manage, track, and report incidents.	**Inspection** Inspected the Information Security Policy and Incident Management Standard to determine whether there were procedures to manage, track, and report incidents.	No exceptions noted.
IR-01-01 (01)	DocuSign documents and tests incident response processes on an annual basis.	**Inspection** Inspected the incident response processes to determine whether DocuSign documented and tested the processes on an annual basis.	No exceptions noted.
IR-01-02	Confirmed incidents are assigned a priority level, investigated, and resolved.	**Inspection** Inspected a sample of incident tickets to determine whether the incident was assigned a priority level, investigated, and resolved.	No exceptions noted.
IR-02-02	In accordance with defined notification requirements, DocuSign communicates incident information to external stakeholders.	**Inquiry** Inquired with management to determine whether DocuSign would communicate incidents in accordance with defined notification requirements on the Alerts and System Status on DocuSign's Trust Center site. **Inspection**	There were no incidents that required external notification per DocuSign's requirements during the period. Therefore, the operating effectiveness of this control activity could not be tested.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		Inspected the Board of Director meeting minutes to identify if there were any incidents that needed to be communicated to external stakeholders.	
VM-09-01	DocuSign assigns a risk rating to identified vulnerabilities and prioritizes remediation of legitimate vulnerabilities according to the assigned risk.	**Inspection** Inspected a sample of identified vulnerabilities to determine whether DocuSign assigned a risk rating to prioritize the remediation efforts of legitimate vulnerabilities.	No exceptions noted.
Trust Services Criteria 7.5 **The entity identifies, develops, and implements activities to recover from identified security incidents.**			
IR-01-01	DocuSign defines the procedures required to manage, track, and report incidents.	**Inspection** Inspected the Information Security Policy and Incident Management Standard to determine whether there were procedures to manage, track, and report incidents.	No exceptions noted.
IR-01-02	Confirmed incidents are assigned a priority level, investigated, and resolved.	**Inspection** Inspected a sample of incident tickets to determine whether to the incident was assigned a priority level, investigated, and resolved.	No exceptions noted.
IR-01-01 (01)	DocuSign documents and tests incident response processes on an annual basis.	**Inspection** Inspected the incident response processes to determine whether DocuSign documented and tested the processes on an annual basis.	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
Change Management			
Trust Services Criteria 8.1 **The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.**			
CHM-01-01	Change scope, change type, and roles and responsibilities are pre-established within DocuSign's change control workflow. The following documentation is required, where applicable, for a change to be approved and committed into the DocuSign live environment: • change description • impact of change • test results • back-out plan • independent code review • change implementer • validation steps & success criteria.	**Inspection** Inspected the Product Change Standard to determine whether defined change management procedures were in place to control changes to the IT environment. Inspected a sample of change release Envelopes to determine whether change description, impact of change, test results, back-out plan, independent code review, change implementer, validation steps & success criteria were documented and approved before the change was deployed.	No exceptions noted.
CHM-01-02	DocuSign performs pre-release testing for code changes to validate that proposed changes meet business requirements.	**Inspection** Inspected a sample of DocuSign Envelopes to determine whether pre-release testing was performed to validate that proposed changes met business requirements.	No exceptions noted.
CHM-01-04	Prior to an infrastructure change, systems must pass a security acceptance review, which identifies unsafe or unauthorized configurations, including default vendor credentials.	**Inspection** Inspected the executed security acceptance review template for a sample of deployments to determine whether the proper review had been performed before	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		the actual deployment, including checking safe/unauthorized configurations or including default vendor credentials.	
SDLC-01-01	Requirements for the secure development, modification, and maintenance of DocuSign software are governed via the DocuSign SDLC Policy.	**Inspection** Inspected DocuSign Software Design Life Cycle Policy to determine whether requirements for the secure development, modification, and maintenance of DocuSign software were governed within the policy.	No exceptions noted.
TPM-01-03	On a periodic basis, DocuSign reviews controls within third party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address any impact the disclosed gaps have on the organization.	**Inspection** Inspected evidence of management review of SOC reports from subservice organizations to determine whether management assessed the design and operating effectiveness of relevant controls implemented at subservice organizations and to determine whether design or operating effectiveness gaps were assessed and addressed by management.	No exceptions noted.
Risk Mitigation			
Trust Services Criteria 9.1 **The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.**			
RM-02-01	DocuSign establishes internal audit requirements based on the established control framework and annual audit plan, and executes audits on information systems and	**Inspection** Inspected the Technical Audit plan to determine whether DocuSign established an internal audit plan.	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	processes at planned intervals.	Inspected the results of completed technical audit to determine whether DocuSign executed audits on information systems processes.	
RM-01-01	At least annually, the Internal Audit Department performs or updates a risk assessment for the organization.	**Inspection** Inspected the annual risk assessment report to determine whether Internal Audit performed and updated the risk assessment for the organization on an annual basis.	No exceptions noted.
Trust Services Criteria 9.2 **The entity assesses and manages risks associated with vendors and business partners.**			
CG-05-02	DocuSign contingent workers, agency contractors, and independent contractors consent to a Confidentiality or Non-Disclosure Agreement, Mobile Device Policy, and Code of Conduct. This is accomplished through either overarching MSA terms and conditions or individual signature of consent forms.	**Inspection** Inspected a sample of contingent workers, agency contractors, and independent contractors to determine whether the worker/contractor consented to the Confidentiality Agreement, Mobile Device Policy, and Code of Conduct as part of their onboarding.	No exceptions noted.
TPM-01-02	DocuSign performs a risk assessment and reviews the security and privacy practices of suppliers who access, collect, process, transfer, or store data on behalf of DocuSign; non-compliance is tracked through remediation.	**Inspection** Inspected a sample of new suppliers who access, collect, process, transfer, or store data on behalf of DocuSign to determine whether DocuSign performed a risk assessment and reviewed	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		their security and privacy practices and that non-compliance was tracked through remediation, if applicable.	
TPM-01-03	On a periodic basis, DocuSign reviews controls within third party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address any impact the disclosed gaps have on the organization.	**Inspection** Inspected evidence of management review of SOC reports from subservice organizations to determine whether management assessed the design and operating effectiveness of relevant controls implemented at subservice organizations and to determine whether design or operating effectiveness gaps were assessed and addressed by management.	No exceptions noted.
TPM-02-02	Customer roles and responsibilities which support DocuSign's information security objectives are communicated via a master services, or equivalent, agreement.	**Inspection** Inspected DocuSign's Master Service Agreement to determine whether the agreement included customer roles and responsibilities which support DocuSign's information security objectives.	No exceptions noted.
Additional Criterial for Availability			
Availability Criteria 1.1 **The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.**			
SM-06-01	Capacity planning and analysis is periodically performed by DocuSign management to maintain the reliability, performance, and	**Inspection** Inspected a sample of DocuSign management's monthly capacity planning	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	capacity of systems required for the operation of DocuSign's live environment.	and analysis meetings to determine whether the review assessed the reliability, performance, and capacity of systems required for the operation of DocuSign's live environment. Inspected a sample of DocuSign management's monthly capacity planning and analysis meeting deck to determine whether follow-up action was identified to enable the implementation of additional capacity.	
Availability Criteria 1.2 **The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.**			
BC-01-01	DocuSign's business continuity plans are reviewed and approved by the plan owner and management on an annual basis or upon material change. Plans are made available to relevant team members.	**Inspection** Inspected a sample of DocuSign's Business Continuity Plans to determine whether they were reviewed on an annual basis and was made available to team members.	No exceptions noted.
BC-01-02	DocuSign performs business continuity and disaster recovery exercises on an annual basis and ensures the following: • exercises are executed with relevant teams	**Inspection** Inspected DocuSign's business continuity and disaster recovery exercises to determine whether the following were performed:	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	• exercise results are documented • corrective actions are taken for exceptions noted • plans are updated based on results.	• exercises are executed with relevant teams • exercise results are documented • corrective actions are taken for exceptions noted • plans are updated based on results.	
BM-01-01	DocuSign replicates data to multiple datacenters within a geographical ring.	**Inspection** Inspected the BLOB storage system and SQL Availability Groups configurations to determine whether production data received from a server was simultaneously replicated to the regional ring data centers. Inspected system monitoring logs to determine whether data replication was performed across the regional ring data centers.	No exceptions noted.
CG-02-01	DocuSign's policies, which define roles and responsibilities that support company objectives, are periodically reviewed, approved by management, and communicated to DocuSign personnel.	**Inspection** Inspected DocuSign's Security Policies and Procedures to determine whether DocuSign has established Policies and Procedures that defines roles and responsibilities and address Security, Availability, and Confidentiality objectives. Inspected DocuSign's Policy Bank to determine whether DocuSign Policies and Procedures were reviewed and approved	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		periodically and communicated to DocuSign's personnel.	
IR-01-02	Confirmed incidents are assigned a priority level, investigated, and resolved.	**Inspection** Inspected a sample of incident tickets to determine whether the incident was assigned a priority level, investigated, and resolved.	No exceptions noted.
SM-06-02	DocuSign defines availability monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	**Inspection** Inspected the configuration of the Kazmon monitoring system to determine whether the production environment was monitored and alerts were recorded in the Case Management System. Inspected a sample of availability monitoring alerts to determine whether they were flagged, identified, and resolved by authorized personnel.	No exceptions noted.
SM-06-03	Critical systems are monitored in accordance to predefined availability criteria and alerts are sent to authorized personnel.	**Inspection** Inspected the configuration of the Kazmon tool to determine whether a monitoring dashboard was in place to monitor key IT production environments. Inspected Kazmon to determine whether the health checks were set up to alert the team in the case of processing errors or performance falling outside of predefined thresholds.	No exceptions noted.

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
TPM-01-03	On a periodic basis, DocuSign reviews controls within third party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address any impact the disclosed gaps have on the organization.	**Inspection** Inspected evidence of management review of SOC reports from subservice organizations to determine whether management assessed the design and operating effectiveness of relevant controls implemented at subservice organizations and to determine whether design or operating effectiveness gaps were assessed and addressed by management.	No exceptions noted.
Availability Criteria 1.3 **The entity tests recovery plan procedures supporting system recovery to meet its objectives.**			
BC-01-02	DocuSign performs business continuity and disaster recovery exercises on an annual basis and ensures the following: • exercises are executed with relevant teams • exercise results are documented • corrective actions are taken for exceptions noted • plans are updated based on results.	**Inspection** Inspected DocuSign's business continuity and disaster recovery exercises to determine whether the following were performed: • exercises are executed with relevant teams • exercise results are documented • corrective actions are taken for exceptions noted • plans are updated based on results.	No exceptions noted.
BM-02-01	DocuSign monitors data replication jobs for failures that indicate a data integrity compromise.	**Inspection** Inspected a sample of data replication failures to determine whether DocuSign monitors and validates the integrity of stored data upon retrieval.	No exceptions noted.

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
SM-06-01	Capacity planning and analysis is periodically performed by DocuSign management to maintain the reliability, performance, and capacity of systems required for the operation of DocuSign's live environment.	**Inspection** Inspected a sample of DocuSign management's monthly capacity planning and analysis meetings to determine whether the review assessed the reliability, performance, and capacity of systems required for the operation of DocuSign's live environment. Inspected a sample of DocuSign management's monthly capacity planning and analysis meeting deck to determine whether follow-up action was identified to enable the implementation of additional capacity.	No exceptions noted.
Additional Criteria for Confidentiality			
Confidentiality Criteria 1.1 **The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.**			
CG-05-01	DocuSign employees consent to a Confidentiality Agreement, Mobile Device Policy, and Code of Conduct.	**Inspection** Inspected a sample of new hires to determine whether the employees consented to the Confidentiality Agreement, Mobile Device Policy, and Code of Conduct as part of their onboarding.	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
CG-05-02	DocuSign contingent workers, agency contractors, and independent contractors consent to a Confidentiality or Non-Disclosure Agreement, Mobile Device Policy, and Code of Conduct. This is accomplished through either overarching MSA terms and conditions or individual signature of consent forms.	**Inspection** Inspected a sample of contingent workers, agency contractors, and independent contractors to determine whether the worker/contractor consented to the Confidentiality Agreement, Mobile Device Policy, and Code of Conduct as part of their onboarding.	No exceptions noted.
CG-02-01 (07)	DocuSign defines information classification and categorization levels to facilitate the appropriate protection of data.	**Inspection** Inspected DocuSign's Data Classification Standard to determine whether DocuSign defined information classification and categorization levels to facilitate the appropriate protection of data.	No exceptions noted.
DM-04-01	DocuSign's transmission of data over public networks is encrypted.	**Inspection** Inspected the certificate website details to determine whether HTTPS/TLS certificate was used and current.	No exceptions noted.
DM-04-02	DocuSign encrypts sensitive data including uploaded Documents and their associated form data and signatures at rest.	**Inspection** Inspected the configuration to determine whether customer data was stored as BLOB using AES256 encryption. Inspected a sample of a BLOB object on the NAS server to determine whether data was encrypted and non-readable while at rest.	No exceptions noted.

DocuSign

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		Inspected the configuration of the HSM Private Server to determine whether it was set to the FIPS Mode for hardware security module ("HSM").	
KM-01-01	Access to the cryptographic keystores is limited to authorized personnel.	**Inspection** Inspected sample of quarterly access reviews to determine whether access to the cryptographic keystores was limited to authorized personnel.	No exceptions noted.
KM-02-01	Dual control and split knowledge are required to generate and access data encryption keys.	**Inspection** Inspected the encryption keys configurations to determine dual control and split knowledge were required to generate and access data encryption keys.	No exceptions noted.
Confidentiality Criteria 1.2 **The entity disposes of confidential information to meet the entity's objectives related to confidentiality.**			
DM-07-03	Account administrators are provided with functionality to automatically purge selected Envelope Documents, including their fields and contents. Account Administrators have the option to redact sensitive information prior to the purge, and additionally configure recurring Envelope purge activities against a defined schedule. If Administrators for active accounts do not set a purge	**Inspection** Inspected the Account Administrators purge configurations to determine whether there was functionality provided to automatically purge select Envelope Documents, including their fields and contents. Inspected the purge schedule configuration to determine whether the Account Administrators	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
	schedule, Envelopes are maintained.	have the option to redact sensitive information prior to purge and schedule recurring Envelope purge activities. Inspected a sample Envelope for an active account where the Administrator had not set a purge schedule to determine whether the Document was maintained. **Observation** Observed an Account Administrator set up an automatic purge preference in the DocuSign settings page to determine whether the selected Envelopes and associated data were purged per the defined schedule.	
DM-07-04	Uploaded non-pdf Documents are deconstructed in DocuSign's Document conversion environment by virtual machines (VM). Malicious content is not passed through to the converted PDF, which is stored in the BLOB storage system; unsupported file types or files are blocked via an exclusion list configuration. VMs are decommissioned and redeployed upon reaching a configured threshold of conversions.	**Inspection** Inspected the system configuration to determine whether document processing servers were purged and re-imaged after reaching the defined threshold. Inspected the virtual machine connection within the system to determine whether anti-malware software was installed and configured in order to block any malicious content prior to storing the converted PDF into the Blob storage.	No exceptions noted.

DocuSign®

Control ID	Control Activities	PwC's Test Procedures	PwC's Test Results
		Observation Observed a user upload a non-pdf Document into the system to determine whether the system deconstructed the Document and that unsupported file types or files were blocked via an exclusion list configuration.	
TPM-01-03	On a periodic basis, DocuSign reviews controls within third party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address any impact the disclosed gaps have on the organization.	**Inspection** Inspected evidence of management review of SOC reports from subservice organizations to determine whether management assessed the design and operating effectiveness of relevant controls implemented at subservice organizations and to determine whether design or operating effectiveness gaps were assessed and addressed by management.	No exceptions noted.

DocuSign®

Section V – Other Information Provided by DocuSign, Inc. that is Not Covered by the Service Auditors' Report

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign

The information included in Section V is intended to provide additional information to user organizations and is not part of the description of controls that may be relevant to user organizations' internal control as it relates to an audit of financial statements. The information in Section V has not been subjected to the procedures applied in the examination of the description of our eSignature system.

Control ID	Control Activities	Tests Results	Management Response
NO-01-01	Network traffic to and from untrusted networks passes through a DMZ; firewall rules are established in accordance to identified security requirements and business justifications are reviewed on a semiannual basis.	**Exception Noted:** For one (1) of one (1) semiannual review selected for testing, the firewall rules review was not performed.	Due to changes in process and responsibility, this function was not properly initiated. Following a root cause investigation, the process was redesigned and streamlined to ensure it can be completed in a timely fashion. In addition, checkpoints have been initiated to ensure that sufficient time is allowed for the review to complete. DocuSign continually reviews firewall rules, both through automation, and through the pull request/change requests process for each update. Access to update the firewall rules is also restricted. Additionally, although the review was not timely, it was determined that there were no changes needed as part of the review.
TA-01-01	Upon hire and on an annual basis, DocuSign employees complete security and privacy awareness trainings. Upon hire and on an annual basis, DocuSign contingent	PwC Inspection Testing: No exceptions noted.	For the contingent workers, management attributed the exception to ineffective oversight of training completion for contingent workers. For

DocuSign®

Control ID	Control Activities	Tests Results	Management Response
	workers with access to systems, devices, or locations, complete security awareness training. Records of training completion are managed within DocuSign's selected Learning Management System.	Subsequent to PwC's inspection testing performed, management identified the following exceptions for individuals that did not complete the security and/or privacy awareness training: • fourteen (14) out of a sample of 25 existing contingent workers • twelve (12) out of a sample of 25 new contingent workers • one (1) out of a sample of 25 existing employees.	the employee, management attributed the exception to the employee's decision to leave DocuSign without completing the training. Employees and contingent workers at DocuSign are exposed to various additional reinforcement of security and privacy best practices and awareness. Additionally, background checks are conducted on employees and contingent workers. They are also required to sign and oblige with onboarding documents detailing Code of Conduct, Mobile Device Policy, and Confidentiality agreements. As a result of the exception, the necessity for employees and contingent workers with access to our systems, devices or locations to complete annual security training has been reiterated and will be reinforced in hiring manager onboarding and expectations.

DocuSign®

This page intentionally left blank.

This report is intended solely for use by the management of DocuSign, Inc. and the specified parties, and is not intended to be, and should not be, used by anyone other than these parties.

DocuSign®

Reports and Attestations:

PCI DSS

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments - Service Providers

Version 3.2.1

Using the PCI Security Standards Council Template dated **June 2018**

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information					
Part 1a. Service Provider Organization Information					
Company Name:	DocuSign, Inc.		DBA (doing business as):	Not Applicable.	
Contact Name:	Suzy Wanja		Title:	Director – Security Compliance	
Telephone:	+1 (510) 259-8126		E-mail:	suzy.wanja@docusign.com	
Business Address:	221 Main Street, Suite 1550		City:	San Francisco	
State/Province:	CA	Country:	USA	Zip:	94105
URL:	https://www.docusign.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	A-LIGN Compliance and Security, Inc. dba A-LIGN				
Lead QSA Contact Name:	Nick Wedel		Title:	Senior Consultant	
Telephone:	+1 (888) 702-5446		E-mail:	nick.wedel@a-lign.com	
Business Address:	400 N. Ashley Drive, Suite 1325		City:	Tampa	
State/Province:	Florida	Country:	United States	Zip:	33602
URL:	https://www.a-lign.com				

PCI Security Standards Council

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	DocuSign eSignature	
Type of service(s) assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / card present ☒ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☐ Fraud and Chargeback	☒ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☒ Others (specify): Document, file management and storage for DocuSign clients.		

***Note**: These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

PCI Security Standards Council

Part 2a. Scope Verification *(continued)*		
Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):		
Name of service(s) not assessed:	DocuSign CLM, DocuSign Rooms, DocuSign Insight, DocuSign LiveOak, DocuSign Click, Guided Forms powered by SmartIQ, DocuSign Monitor, Standards-Based Signatures, DocuSign Identify, Hybrid Cloud Appliances, DocuSign Admin Tools	
Type of service(s) not assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☒ Others (specify): Document and business process management, and collaboration applications.		
Provide a brief explanation why any checked services were not included in the assessment:	Only the DocuSign eSignature product was included within the scope of this assessment. All other applicable DocuSign products were assessed in separate PCI engagements.	

PCI Security Standards Council

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	DocuSign, Inc. is a Software as a Service (SaaS) company that helps organizations connect and automate how they prepare, sign, act on, and manage agreements through the DocuSign Agreement Cloud. DocuSign eSignature, including the Payments and eCommerce process, acts as an interface to assist customers with completing various business-related workflows, some of which may include cardholder data, from a personal computer or mobile device. Customers have the option to use the Payments feature as part of the eSignature product to receive payments as part of business transactions. The eSignature product is offered as a SaaS business model and is hosted within United States and European colocation data centers, and various cloud regions in the United States, Australia, and Canada. Front-end connections into the eSignature product occur through the colocation data centers whereas IT support networks and infrastructure reside within the cloud regions. DocuSign also operates an eCommerce environment in order to accept payment for the various products and services provided to their customers.

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	DocuSign eSignature customers have the option to use the “Payments” feature as part of the eSignature product to receive payments as part of business transactions. Within this feature, the customer selects one of seven payment processors/gateways to receive cardholder data (CHD). On behalf of the customer, DocuSign will transmit CHD to the selected entity for payment authorization and processing. No CHD is stored by DocuSign as part of this function. Customers can use "save payment details” functionality within the product and use the payment gateway's “subscriptions” functionality to create recurring credit card payments. DocuSign stores tokens that can be used for these recurring payments once the token has been transmitted to Zuora, a third-party service provider that specializes in processing recurring payments. DocuSign also receives CHD via their eCommerce website for initial and one-time payments by customers for DocuSign services. In the event a customer payment is unsuccessful at the time of submission, DocuSign will store encrypted CHD until the transaction can be successfully authorized and processed, or for a maximum of 180 days. Once the payment transaction has completed, or when the 180-day limit has been reached, an automated daily cleanup function will securely purge the cardholder data from DocuSign systems. DocuSign customers also have the ability to include cardholder data within their eSignature transactions which are stored by DocuSign as encrypted Binary Large Objects (or encrypted “BLOBs”). DocuSign does not have visibility into the BLOB data.

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
Corporate Offices	12	North America: • Chicago, IL, USA • Seattle, WA, USA • San Francisco, CA, USA • Warrenville, IL, USA EMEA: • Dublin, Ireland • Paris, France • Giv’at Shmuel, Israel • Tokyo, Japan • Singapore • Sydney, Australia • Melbourne, Australia

		• Sao Paulo, Brazil
Data Centers	12	North America: • Tukwila, WA, USA (SE2 / SEA1) • Chicago, IL, USA (CH / CH4) • Chicago (Elk Grove), IL, USA (NA11) • Richardson, TX, USA (DA / DFW) • Quebec City, Quebec, Canada (Azure) • Toronto, Ontario, Canada (Azure) EMEA: • Amsterdam, Netherlands (AM / AM3) • Frankfurt, Germany (FR / FR2) • Paris, France (PA4) • AWS: US-West-2 (Oregon) • AWS: US-East-2 (Ohio) APAC: • Melbourne, Australia (Azure) • Sydney, Australia (Azure)

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☐ Yes ☒ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Not Applicable.	Not Applicable.	Not Applicable.	☐ Yes ☐ No	Not Applicable.

Part 2e. Description of Environment

Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	DocuSign eSignature is hosted globally within colocation data centers and the cloud. A combination of Palo Alto firewalls and F5 load balancers are utilized for external traffic management whereas Arista, Cisco, and Juniper routers and switches provide internal traffic management. Administrative connections into the eSignature environment require the user to follow multi-factor authentication procedures in the form of a user account, password, and an authentication token. DocuSign requires customer connections to the eSignature product to occur over secure connections. Furthermore, data transmitted via eSignature, including customer transaction BLOBs, are encrypted at rest using strong cryptographic algorithms. Each BLOB is assigned a unique encryption key, and encryption keys are managed, maintained, and

	controlled within DocuSign Multi-Tenant Security Appliances (MTSAs) and Hardware Security Modules (HSMs).
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes ☐ No

Part 2f. Third-Party Service Providers

Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?	☐ Yes ☒ No
If Yes:	
Name of QIR Company:	Not Applicable.
QIR Individual Name:	Not Applicable.
Description of services provided by QIR:	Not Applicable.
Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?	☒ Yes ☐ No

If Yes:

Name of service provider:	**Description of services provided:**
Amazon Web Services ("AWS")	Cloud service provider. Customer cardholder data could potentially be stored and/or transmitted within AWS. DocuSign does not have knowledge of what cardholder data elements customers are transmitting or storing.
Google Cloud Platform ("GCP")	Cloud service provider. Customer cardholder data could potentially be stored and/or transmitted within Google Cloud Platform. DocuSign does not have knowledge of what cardholder data elements customers are transmitting or storing.
Microsoft Azure ("Azure")	Cloud service provider. Customer cardholder data could potentially be stored and/or transmitted within Microsoft Azure. DocuSign does not have knowledge of what cardholder data elements customers are transmitting or storing.
Cyxtera, Inc. ("Cyxtera")	Colocation provider. Customer cardholder data could potentially be store and/or transmitted within Cyxtera's colocation facilities. DocuSign does not have visibility into what cardholder data elements customers are transmitting or storing.
Equinix, Inc. ("Equinix")	Colocation provider. Customer cardholder data could potentially be store and/or transmitted within Equinix's colocation facilities. DocuSign does not have visibility into what cardholder data elements customers are transmitting or storing.
Sungard Availability Services, LP ("Sungard")	Colocation provider. Customer cardholder data could potentially be store and/or transmitted within Sungard's colocation facilities. DocuSign does not have visibility into what cardholder data elements customers are transmitting or storing.
Switch, LTD ("Switch")	Colocation provider. Customer cardholder data could potentially be store and/or transmitted within Switch's colocation facilities. DocuSign does not have

	visibility into what cardholder data elements customers are transmitting or storing.
Adyen N.V.	Transaction Processing
Elavon, Inc.	Transaction Processing
CyberSource (Authorize.net)	Transaction Processing
PayPal (Braintree)	Transaction Processing
Stripe, Inc.	Transaction Processing
Salesforce.com, Inc.	Transaction Processing
Zuora, Inc.	Transaction Processing
Spreedly, Inc.	Transaction Processing
Note: *Requirement 12.8 applies to all entities in this list.*	

PCI Security Standards Council

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** - The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC
- **Partial** - One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC
- **None** - All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

Note: *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

Name of Service Assessed:	DocuSign eSignature			
PCI DSS Requirement	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☒	☐	☐	
Requirement 2:	☐	☒	☐	2.1.1 – Not Applicable. DocuSign does not utilize wireless devices within the CDE. 2.2.3 – Not Applicable. DocuSign does not utilize insecure services, protocols, or daemons. 2.6 – Not Applicable. DocuSign is not a shared hosting provider.
Requirement 3:	☐	☒	☐	3.4.1 – Not Applicable. DocuSign does not utilize disk encryption. 3.6.a – Not Applicable. DocuSign does not share encryption keys with customers.
Requirement 4:	☐	☒	☐	4.1.1 – Not Applicable. DocuSign does not utilize wireless devices within the CDE.
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	6.4.6 – Not Applicable. No significant changes occurred within the review period.
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.1.5 – Not Applicable. DocuSign does not permit third-party access into the CDE.

				8.5.1 – Not Applicable. DocuSign does not have remote access to customer premises.
Requirement 9:	☐	☒	☐	9.5 – 9.8.2 – Not Applicable. DocuSign does not maintain removable media that contain cardholder data. 9.9 – 9.9.3 – Not Applicable. DocuSign does not utilize POS/POI devices.
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	11.2.3 – Not Applicable. No significant changes occurred within the review period.
Requirement 12:	☐	☒	☐	12.3.9 – Not Applicable. DocuSign does not permit access into the CDE for vendors or business partners.
Appendix A1:	☐	☐	☒	Not Applicable. DocuSign is not a shared hosting provider.
Appendix A2:	☐	☐	☒	Not Applicable. DocuSign does not utilize SSL/Early TLS or POI/POS devices.

PCI Security Standards Council

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	19 September 2022	
Have compensating controls been used to meet any requirement in the ROC?	☒ Yes	☐ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes	☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated 19 September 2022.

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (***check one):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby **DocuSign, Inc.** has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby **(Service Provider Company Name)** has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

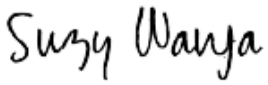
(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2.1*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

PCI Security Standards Council

Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor (Tenable.io – 5049-01-10)

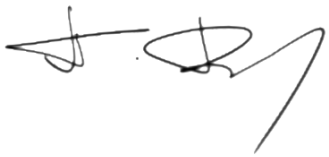
Part 3b. Service Provider Attestation



Signature of Service Provider Executive Officer ↑	*Date:* September 29, 2022
Service Provider Executive Officer Name: Suzy Wanja	*Title:* Director – Security Compliance

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	The assessor provided PCI DSS advisory and assessment services, which included observation of controls, interviews with key personnel, and review of policies and procedures.



Signature of Duly Authorized Officer of QSA Company ↑	*Date:* September 29, 2022
Duly Authorized Officer Name: Petar Besalev, EVP Cybersecurity and Compliance Services	*QSA Company:* A-LIGN

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel, and describe the role performed:	Not Applicable.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☐	☐	Not Applicable. DocuSign is not a shared hosting provider.
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	Not Applicable. DocuSign does not utilize SSL/Early TLS or POI POS devices.

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments - Merchants

Version 3.2.1

Created with the PCI Security Standards Council Template dated **June 2018**

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the merchant's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact your acquirer (merchant bank) or the payment brands for reporting and submission procedures.

Part 1. Merchant and Qualified Security Assessor Information					
Part 1a. Merchant Organization Information					
Company Name:	DocuSign, Inc.		DBA (doing business as):	Not Applicable.	
Contact Name:	Suzy Wanja		Title:	Director – Security Compliance	
Telephone:	+1 (510) 259-8126		E-mail:	suzy.wanja@docusign.com	
Business Address:	221 Main Street, Suite 1550		City:	San Francisco	
State/Province:	CA	Country:	USA	Zip:	94105
URL:	https://www.docusign.com				
Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	A-LIGN Compliance and Security, Inc. dba A-LIGN				
Lead QSA Contact Name:	Nick Wedel		Title:	Senior Consultant	
Telephone:	+1 (888) 702-5446		E-mail:	nick.wedel@a-lign.com	
Business Address:	400 N. Ashley Drive, Suite 1325		City:	Tampa	
State/Province:	Florida	Country:	USA	Zip:	33602
URL:	https://www.a-lign.com				

PCI Security Standards Council

Part 2. Executive Summary

Part 2a. Type of Merchant Business (check all that apply)

☐ Retailer	☐ Telecommunication	☐ Grocery and Supermarkets
☐ Petroleum	☒ E-Commerce	☐ Mail order/telephone order (MOTO)
☒ Others (please specify): Business Transaction Management Platform Provider		

What types of payment channels does your business serve?	Which payment channels are covered by this assessment?
☐ Mail order/telephone order (MOTO)	☐ Mail order/telephone order (MOTO)
☒ E-Commerce	☒ E-Commerce
☐ Card-present (face-to-face)	☐ Card-present (face-to-face)

Note: *If your organization has a payment channel or process that is not covered by this assessment, consult your acquirer or payment brand about validation for the other channels.*

Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?	DocuSign, Inc. is a Software as a Service (SaaS) company that helps organizations connect and automate how they prepare, sign, act on, and manage agreements through the DocuSign Agreement Cloud. DocuSign eSignature, including the Payments and eCommerce processes, acts as an interface to assist customers with completing various business-related workflows, some of which may include account data (PAN and SAD), from a personal computer or mobile device. The eSignature product is offered as a SaaS business model and is hosted within the United States, European colocation data centers, and various cloud regions in the United States, Australia, and Canada. For the eCommerce service, DocuSign receives cardholder data via the eCommerce website for initial and one-time payments. In the event a payment cannot be successfully processed at the time of submission, DocuSign will store cardholder data until the transaction can be processed or for a maximum of 180 days. Once the transaction has completed or the 180-day limit has been reached, an automated daily cleanup function will remove the cardholder data from DocuSign systems. DocuSign will store tokens that can be used for reoccurring credit card payments once the token has been transmitted to Zuora, a third-party service provider that specializes in processing reoccurring payments.

PCI Security Standards Council

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
Corporate Offices	12	North America: • Chicago, IL, USA • Seattle, WA, USA • San Francisco, CA, USA • Warrenville, IL, USA EMEA: • Dublin, Ireland • Paris, France • Giv'at Shmuel, Israel • Tokyo, Japan • Singapore • Sydney, Australia • Melbourne, Australia • Sao Paulo, Brazil
Data Centers	12	North America: • Tukwila, WA, USA (SE2 / SEA1) • Chicago, IL, USA (CH / CH4) • Chicago (Elk Grove), IL, USA (NA11) • Richardson, TX, USA (DA / DFW) • Quebec City, Quebec, Canada (Azure) • Toronto, Ontario, Canada (Azure) • AWS: US-West-2 (Oregon) • AWS: US-East-2 (Ohio) EMEA: • Amsterdam, Netherlands (AM / AM3) • Frankfurt, Germany (FR / FR2) • Paris, France (PA4) APAC: • Melbourne, Australia (Azure) • Sydney, Australia (Azure)

Part 2d. Payment Application

Does the organization use one or more Payment Applications? ☒ Yes ☐ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Sparky	9/12/22 Release	Not Applicable.	☐ Yes ☒ No	Not Applicable.

Part 2e. Description of Environment	
Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	DocuSign eSignature is hosted globally within colocation data centers and in the cloud. A combination of Palo Alto firewalls and F5 load balancers are utilized for external network traffic management, whereas Arista, Cisco, and Juniper routers and switches provide internal traffic management and routing. Administrative connections into the eSignature environment require multi-factor authentication in the form of a user account, password, and an authentication token. Furthermore, all data transmitted via eSignature, including customer transaction BLOBs, are encrypted at rest using strong cryptographic algorithms. Each BLOB is assigned a unique encryption key, and encryption keys are managed, maintained, and controlled within DocuSign Multi-Tenant Security Appliances (MTSAs) and HSMs.
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes ☐ No

Part 2f. Third-Party Service Providers	
Does your company use a Qualified Integrator & Reseller (QIR)?	☐ Yes ☒ No
If Yes:	
Name of QIR Company:	Not Applicable.
QIR Individual Name:	Not Applicable.
Description of services provided by QIR:	Not Applicable.
Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?	☒ Yes ☐ No

If Yes:

Name of service provider:	**Description of services provided:**
Amazon Web Services ("AWS")	Cloud service provider. Customer cardholder data could potentially be store and/or transmitted within AWS. DocuSign does not have knowledge of what cardholder data elements customers are transmitting or storing.
Microsoft Azure ("Azure")	Cloud service provider. Customer cardholder data could potentially be store and/or transmitted within Microsoft Azure.

	DocuSign does not have knowledge of what cardholder data elements customers are transmitting or storing.
Cyxtera, Inc. (“Cyxtera”)	Colocation provider. Customer cardholder data could potentially be store and/or transmitted within Cyxtera’s colocation facilities. DocuSign does not have visibility into what cardholder data elements customers are transmitting or storing.
Equinix (EMEA) B.V.	Colocation provider. Customer cardholder data could potentially be store and/or transmitted within Equinix’s colocation facilities. DocuSign does not have visibility into what cardholder data elements customers are transmitting or storing.
Sungard Availability Services, LP (“Sungard”)	Colocation provider. Customer cardholder data could potentially be store and/or transmitted within Sungard’s colocation facilities. DocuSign does not have visibility into what cardholder data elements customers are transmitting or storing.
Switch, LTD (“Switch”)	Colocation provider. Customer cardholder data could potentially be store and/or transmitted within Switch’s colocation facilities. DocuSign does not have visibility into what cardholder data elements customers are transmitting or storing.
Adyen N.V.	Transaction Processing
CyberSource (Authorize.net)	Transaction Processing
Zuora	Transaction Processing
Note: *Requirement 12.8 applies to all entities in this list.*	

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	19 September 2022
Have compensating controls been used to meet any requirement in the ROC?	☒ Yes ☐ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes ☐ No
Were any requirements not tested?	☐ Yes ☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No

PCI Security Standards Council

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated 19 September 2022.

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (***check one):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby **DocuSign, Inc.** has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby **(Merchant Company Name)** has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2.1*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☒	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

PCI Security Standards Council

Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor (tenable.io – 5049-01-10)

Part 3b. Merchant Attestation

Suzy Wanja

Signature of Merchant Executive Officer ↑	*Date:* September 29, 2022
Merchant Executive Officer Name: Suzy Wanja	*Title:* Director – Security Compliance

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	The assessor provided PCI DSS advisory and assessment services, which included observation of controls, interviews with key personnel, and review of policies and procedures.

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* September 29, 2022
Duly Authorized Officer Name: Petar Besalev, EVP Cybersecurity and Compliance Services	*QSA Company:* A-LIGN

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel, and describe the role performed:	Not Applicable.

PCI Security Standards Council

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with your acquirer or the payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements *(Select One)*		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	Not Applicable. DocuSign, Inc. does not utilize any POS/ POI Terminal Connections.

DocuSign PCI Responsibility Matrix June 2022
General Information Regarding the DocuSign PCI Responsibility Matrix
DocuSign is predominantly a PCI Service Provider. The DocuSign Agreement Cloud allows customers to upload documents for signing, collaboration, analysis, etc. Given that agreements naturally contain sensitive information and potentially cardholder data, DocuSign secures its operations, infrastructure, and customer data in accordance with PCI DSS. Customers have full control over their uploaded documents including access, retention, and modification; DocuSign does not have visibility to the contents of uploaded documents. DocuSign manages and protects all of the below products, features, and workflows in accordance with PCI DSS, even if they do not explicitly collect cardholder data.
The scope of DocuSign's PCI responsibility matrix covers the following: • eSignature • Payments* • CLM • Insight • Analyzer** • Liveoak • Rooms • Gen, Negotiate, and DocuSign Apps Launcher***
*Payments is an eSignature feature that allows envelope Senders to request and issue payment from Signers via the Sender's payment gateway. The Signer submits their credit card information, which is protected during transit to the selected processor and is never stored on DocuSign systems.
**Analyzer is a Microsoft Word plugin that provides connectivity to the Insight infrastructure. Customers can process files from their desktop through the Insight infrastructure based on workflows and configurations from their account. The customer is responsible for the receipt, installation, testing, and deployment of the plugin, including the infrastructure in which it resides. Both the plugin software development and the transfer of information between the local document and Insight infrastructure are protected in accordance with PCI DSS requirements.
***DocuSign Gen, Negotiate, and DocuSign Apps Launcher (DAL) are Salesforce applications available via the Salesforce AppExchange. These allow customers to interact with DocuSign eSignature and CLM from their Salesforce account. DocuSign is responsible for the development of these applications, including the protection of data between DocuSign and Salesforce, both which are compliant with PCI DSS requirements.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
Requirement 1: Install and maintain a firewall configuration to protect cardholder data			
1.1 Establish and implement firewall and router configuration standards that include the following:	DocuSign		DocuSign is responsible for the management of its network.
1.1.1. A formal process for approving and testing all network connections and changes to the firewall and router configurations	DocuSign		DocuSign is responsible for the management of its network.
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	DocuSign		DocuSign is responsible for the management of its network.
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	DocuSign		DocuSign is responsible for the management of its network.
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	DocuSign		DocuSign is responsible for the management of its network.
1.1.5 Description of groups, roles, and responsibilities for management of network components	DocuSign		DocuSign is responsible for the management of its network.
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	DocuSign		DocuSign is responsible for the management of its network.
1.1.7 Requirement to review firewall and router rule sets at least every six months	DocuSign		DocuSign is responsible for the management of its network.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.	DocuSign		DocuSign is responsible for the management of its network.
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	DocuSign		DocuSign is responsible for the management of its network.
1.2.2 Secure and synchronize router configuration files.	Not Applicable	DocuSign does not use routers to perform filtering.	
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	Not Applicable	DocuSign does not allow wireless networks to connect to any cardholder data environment.	
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	DocuSign		DocuSign is responsible for the management of its network.
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	DocuSign		DocuSign is responsible for the management of its network.
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	DocuSign		DocuSign is responsible for the management of its network.
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	DocuSign		DocuSign is responsible for the management of its network.
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	DocuSign		DocuSign is responsible for the management of its network.
1.3.5 Permit only "established" connections into the network.	DocuSign		DocuSign is responsible for the management of its network.
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	DocuSign		DocuSign is responsible for the management of its network.
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties. - Network Address Translation (NAT) - Placing servers containing cardholder data behind proxy servers/firewalls, - Removal or filtering of route advertisements for private networks that employ registered addresses. - Internal use of RFC1918 address space instead of registered addresses.	DocuSign		DocuSign is responsible for the management of its network.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: - Specific configuration settings are defined for personal firewall software. - Personal firewall (or equivalent functionality) is actively running. - Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	DocuSign		DocuSign is responsible for the security of workstations which access the cardholder data environment.
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	DocuSign		DocuSign is responsible for the management of its network and educating employees on internal operational procedures.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters			
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).	DocuSign		DocuSign is responsible for the management of its systems and network.
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	DocuSign		DocuSign does not allow wireless networks to connect to any cardholder data environment.
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: - Center for Internet Security (CIS) - International Organization for Standardization (ISO) - SysAdmin Audit Network Security (SANS) Institute - National Institute of Standards Technology (NIST).	DocuSign		DocuSign is responsible for the management of its systems and network.
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.	DocuSign		DocuSign is responsible for the management of its systems and network.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	DocuSign		DocuSign is responsible for the management of its systems and network.
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.	DocuSign		DocuSign does not support insecure services.
2.2.4 Configure system security parameters to prevent misuse.	DocuSign		DocuSign is responsible for the management of its systems and network.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	DocuSign		DocuSign is responsible for the management of its systems and network.
2.3 Encrypt all non-console administrative access using strong cryptography.	DocuSign		DocuSign is responsible for the management of its systems and network.
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	DocuSign		DocuSign is responsible for the management of its systems and network.
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	DocuSign		DocuSign is responsible for the management of its systems and network.
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.	Not Applicable	DocuSign does not provide shared hosting services.	
Requirement 3: Protect stored cardholder data			
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: - Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements - Processes for secure deletion of data when no longer needed - Specific retention requirements for cardholder data - A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	Shared	The customer is responsible for managing (1) data storage and retention policies for their cardholder data and (2) data retention configuration(s) within the DocuSign products. Customers who utilize the DocuSign Payments feature are responsible for managing their accounts with their selected processor(s) to ensure data stored meets this requirement.	DocuSign is responsible to ensure that customer documents and data are deleted in accordance with the retention and deletions settings established by the customer within the application.
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: - There is a business justification and - The data is stored securely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	Shared	The customer is responsible for managing the data they store within DocuSign envelopes and for maintaining appropriate data retention policies and procedures in accordance with PCI DSS requirements. Customers who utilize the DocuSign Payments feature are responsible for managing their accounts with their selected processor(s) to ensure data stored meets this requirement. Sensitive authentication data should never be stored by the Customer anywhere within the DocuSign environment, including envelopes and uploaded documents.	DocuSign is responsible to ensure that explicitly collected sensitive authentication data is not stored after authorization. DocuSign does not have visibility regarding the contents of customer envelopes or documents. As such, customers are responsible to ensure that sensitive authentication data is only submitted when explicitly collected (e.g., the DocuSign Payments feature).

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic- stripe data. Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained: - The cardholder's name - Primary account number (PAN) - Expiration date - Service code To minimize risk, store only these data elements as needed for business.	Customer	The customer is responsible for managing the data they store within DocuSign envelopes and for maintaining appropriate data retention policies and procedures in accordance with PCI DSS requirements. Customers who utilize the DocuSign Payments feature are responsible for managing their accounts with their selected processor(s) to ensure data stored meets this requirement. Full track contents should never be stored by the Customer anywhere within the DocuSign environment, including envelopes and uploaded documents.	DocuSign systems do not collect full track data
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.	Shared	The customer is responsible for managing the data they store within DocuSign envelopes and for maintaining appropriate data retention policies and procedures in accordance with PCI DSS requirements. Customers who utilize the DocuSign Payments feature are responsible for managing their accounts with their selected processor(s) to ensure data stored meets this requirement. Card verification codes or values should never be stored by the Customer anywhere within the DocuSign environment, including envelopes and uploaded documents.	DocuSign is responsible to ensure that explicitly collected card verification codes or values are not stored after authorization. DocuSign does not have visibility regarding the contents of customer envelopes or documents. As such, customers are responsible to ensure that card verification codes and values are only submitted when explicitly collected (e.g., the DocuSign Payments feature).

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	Shared	The customer is responsible for managing the data they store within DocuSign envelopes and for maintaining appropriate data retention policies and procedures in accordance with PCI DSS requirements. Customers who utilize the DocuSign Payments feature are responsible for managing their accounts with their selected processor(s) to ensure data stored meets this requirement. Personal identification numbers should never be stored by the Customer anywhere within the DocuSign environment, including envelopes and uploaded documents.	DocuSign is responsible to ensure that explicitly collected personal identification numbers are not stored after authorization. DocuSign does not have visibility regarding the contents of customer envelopes or documents. As such, customers are responsible to ensure that personal identification numbers are only submitted when explicitly collected (e.g., the DocuSign Payments feature).
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN. Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.	Shared	When primary account numbers are stored in envelopes or uploaded documents, the customer is responsible to ensure that only personnel with a legitimate business need have access to the envelope or document.	DocuSign is responsible to ensure that primary account numbers which are explicitly collected are masked when displayed.
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: - One-way hashes based on strong cryptography, (hash must be of the entire PAN) - Truncation (hashing cannot be used to replace the truncated segment of PAN) - Index tokens and pads (pads must be securely stored) - Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	DocuSign		DocuSign is responsible for the encryption of envelopes and documents which customers store within DocuSign systems.
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.	DocuSign		When disk encryption is used, DocuSign is responsible to ensure that (1) logical access to the disk is independent of native operating system authentication mechanisms and (2) decryption keys are not associated with user accounts.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: **Note:** This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys- such key-encrypting keys must be at least as strong as the data-encrypting key.	DocuSign		Within the DocuSign cardholder data environment, DocuSign is responsible to implement encryption mechanisms and key management processes in accordance with PCI DSS requirements.
3.5.1 Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: - Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date - Description of the key usage for each key - Inventory of any HSMs and other SCDs used for key management	DocuSign		DocuSign maintains documentation associated with the cryptographic architecture used to protect the cardholder data environment.
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.	DocuSign		DocuSign is responsible for the management of cryptographic solutions used to protect cardholder data within its systems and network.
3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: - Encrypted with a key-encrypting key that is at least as strong as the dataencrypting key, and that is stored separately from the data-encrypting key - Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) - As at least two full-length key components or key shares, in accordance with an industryaccepted method Note: It is not required that public keys be stored in one of these forms.	DocuSign		DocuSign is responsible for the management of cryptographic solutions used to protect cardholder data within its systems and network.
3.5.4 Store cryptographic keys in the fewest possible locations.	DocuSign		DocuSign is responsible for the management of cryptographic solutions used to protect cardholder data within its systems and network.
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.	DocuSign		DocuSign is responsible for the management of cryptographic solutions used to protect cardholder data within its systems and network.
3.6.1 Generation of strong cryptographic keys	DocuSign		DocuSign is responsible for the management of cryptographic solutions used to protect cardholder data within its systems and network.
3.6.2 Secure cryptographic key distribution	DocuSign		DocuSign is responsible for the management of cryptographic solutions used to protect cardholder data within its systems and network.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
3.6.3 Secure cryptographic key storage	DocuSign		DocuSign is responsible for the management of cryptographic solutions used to protect cardholder data within its systems and network.
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher- text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	DocuSign		DocuSign is responsible for the management of cryptographic solutions used to protect cardholder data within its systems and network.
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.	DocuSign		DocuSign is responsible for the management of cryptographic solutions used to protect cardholder data within its systems and network.
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. **Note**: Examples of manual key- management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.	DocuSign		DocuSign is responsible for the management of cryptographic solutions used to protect cardholder data within its systems and network.
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	DocuSign		DocuSign is responsible for the management of cryptographic solutions used to protect cardholder data within its systems and network.
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	DocuSign		DocuSign is responsible for the management of cryptographic solutions used to protect cardholder data within its systems and network.
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	DocuSign		DocuSign is responsible for the management of cryptographic solutions used to protect cardholder data within its systems and network.
Requirement 4: Encrypt transmission of cardholder data across open, public networks			

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: • The Internet • Wireless technologies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA) • General Packet Radio Service (GPRS). • Satellite communications.	DocuSign		DocuSign is responsible for the management of cryptographic solutions used to protect cardholder data within its systems and network.
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	Not Applicable		DocuSign does not allow use of wireless networks to transmit cardholder data or connect to the cardholder data environment.
4.2 Never send unprotected PANs by end- user messaging technologies (for example, e- mail, instant messaging, SMS, chat, etc.).	Shared	The customer is responsible to ensure that unencrypted PANs are not distributed via end-user messaging technologies or when engaging with DocuSign personnel (e.g., Support, Account Executive, Customer Service Manager).	DocuSign is responsible to ensure that unencrypted PANs are not distributed via end-user messaging technologies.
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	DocuSign		DocuSign is responsible for managing policies and procedures related to encryption utilized in managing the DocuSign systems.
Requirement 5: Use and regularly update anti-virus software or programs			
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Shared	The customer is responsible to ensure that workstations and systems which interact with DocuSign services (e.g., web application, API) have anti-virus software deployed.	DocuSign is responsible for the management of its systems and network.
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	Shared	The customer is responsible to ensure that workstations and systems which interact with DocuSign services (e.g., web application, API) have anti-virus software deployed.	DocuSign is responsible for the management of its systems and network.
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	DocuSign		DocuSign is responsible for the management of its systems and network.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
5.2 Ensure that all anti-virus mechanisms are maintained as follows: - Are kept current, - Perform periodic scans - Generate audit logs which areretained per PCI DSS Requirement 10.7.	Shared	The customer is responsible to ensure that workstations and systems which interact with DocuSign services (e.g., web application, API) have anti-virus software deployed.	DocuSign is responsible for the management of its systems and network.
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. **Note**: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.	Shared	The customer is responsible to ensure that workstations and systems which interact with DocuSign services (e.g., web application, API) have anti-virus software deployed.	DocuSign is responsible for the management of its systems and network.
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	DocuSign		DocuSign is responsible for the management of its systems and network.
Requirement 6: Develop and maintain secure systems and applications			
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities. Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk- assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.	DocuSign		DocuSign is responsible to establish and maintain a vulnerability management program for its cardholder data environment, including the identification, triage, and remediation of vulnerabilities.
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release. **Note:** Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.	DocuSign		DocuSign is responsible to establish and maintain a vulnerability management program for its cardholder data environment, including the identification, triage, and remediation of vulnerabilities.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle **Note**: this applies to all software developed internally as well as bespoke or custom software developed by a third party.	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: - Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. - Code reviews ensure code is developed according to secure coding guidelines - Appropriate corrections are implemented prior to release. - Code-review results are reviewed and approved by management prior to release. **Note:** This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
6.4.2 Separation of duties between development/test and production environments	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.4.3 Production data (live PANs) are not used for testing or development	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.4.4 Removal of test data and accounts before production systems become active	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.4.5 Change control procedures for the implementation of security patches and software modifications must include the following:	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.4.5.1 Documentation of impact.	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.4.5.2 Documented change approval by authorized parties.	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.4.5.4 Back-out procedures.	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.5 Address common coding vulnerabilities in software-development processes as follows: - Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. - Develop applications based on secure coding guidelines. **Note**: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.5.2 Buffer overflows	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.5.3 Insecure cryptographic storage	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.5.4 Insecure communications	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.5.5 Improper error handling	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
6.5.6 All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.5.7 Cross-site scripting (XSS)	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.5.9 Cross-site request forgery (CSRF)	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.5.10 Broken authentication and session management	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: - Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes - Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic. Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2.	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	DocuSign		DocuSign is responsible for developing internal and external software applications which manage cardholder data in accordance with PCI DSS, industry standards, and internal security requirements.
Requirement 7: Restrict access to cardholder data by business need to know			

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	Shared	The customer is responsible for managing access to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
7.1.1 Define access needs for each role, including: - System components and data resources that each role needs to access for their job function - Level of privilege required (for example, user, administrator, etc.) for accessing resources.	Shared	The customer is responsible for managing access to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	Shared	The customer is responsible for managing access to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
7.1.3 Assign access based on individual personnel's job classification and function.	Shared	The customer is responsible for managing access to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
7.1.4 Require documented approval by authorized parties specifying required privileges.	Shared	The customer is responsible for managing access to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
7.2 Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	DocuSign		DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
7.2.1 Coverage of all system components	DocuSign		DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
7.2.2 Assignment of privileges to individuals based on job classification and function.	DocuSign		DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
7.2.3 Default “deny-all” setting.	DocuSign		DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
Requirement 8: Assign a unique ID to each person with computer access			
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	DocuSign	The customer is responsible for managing identifiation, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	DocuSign	The customer is responsible for managing identifiation, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	DocuSign	The customer is responsible for managing identification, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.1.3 Immediately revoke access for any terminated users.	DocuSign	The customer is responsible for managing identification, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.1.4 Remove/disable inactive user accounts at least every 90 days.	DocuSign	The customer is responsible for managing identification, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.1.5 Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: - Enabled only during the time period needed and disabled when not in use. - Monitored when in use.	DocuSign	The customer is responsible for managing identification, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign does not allow vendors to access the Cardholder Data Environment.
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	DocuSign	The customer is responsible for managing identification, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	DocuSign	The customer is responsible for managing identification, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	DocuSign	The customer is responsible for managing identification, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: - Something you know, such as a password or passphrase - Something you have, such as a token device or smart card - Something you are, such as a biometric.	DocuSign	The customer is responsible for managing identification, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	DocuSign	The customer is responsible for managing identification, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	DocuSign	The customer is responsible for managing identification, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.2.3 Passwords/phrases must meet the following: - Require a minimum length of at least seven characters. - Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.	DocuSign	The customer is responsible for managing identification, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.2.4 Change user passwords/passphrases at least every 90 days.	DocuSign	The customer is responsible for managing identification, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	DocuSign	The customer is responsible for managing identifiation, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.2.6 Set passwords/phrases for first- time use and upon reset to a unique value for each user, and change immediately after the first use.	DocuSign	The customer is responsible for managing identifiation, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. Note: Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.	DocuSign		DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	DocuSign		DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.	DocuSign		DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.4 Document and communicate authentication procedures and policies to all users including: - Guidance on selecting strong authentication credentials - Guidance for how users should protect their authentication credentials - Instructions not to reuse previously used passwords - Instructions to change passwords if there is any suspicion the password could be compromised.	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: - Generic user IDs are disabled or removed. - Shared user IDs do not exist for system administration and other critical functions. - Shared and generic user IDs are not used to administer any system components.	DocuSign	The customer is responsible to ensure that group, shared, or generate authentication methods are not used to access DocuSign services.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.5.1 Additional requirement for service providers: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. **Note:** This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.	Not Applicable		DocuSign does not have remote access to customer premises.
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: - Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. - Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	DocuSign	The customer is responsible for managing identifiation, authentication, and authorization to their DocuSign account, including the documents and data contained within, to individuals whose job requires such access.	DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: - All user access to, user queries of, and user actions on databases are through programmatic methods. - Only database administrators have the ability to directly access or query databases. - Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	DocuSign		DocuSign is responsible to provide the customer with administrative acounts purposed to manage access to their DocuSign account, documents, and data. DocuSign is responsible for manage access to its systems and network.
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
Requirement 9: Restrict physical access to cardholder data			
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	DocuSign		DocuSign is responsible to manage physical access to its cardholder data environment.
9.1.1 Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: “Sensitive areas” refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of- sale terminals are present, such as the cashier areas in a retail store.	DocuSign		DocuSign is responsible to manage physical access to its cardholder data environment.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.	DocuSign		DocuSign is responsible to manage physical access to its cardholder data environment.
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	DocuSign		DocuSign is responsible to manage physical access to its cardholder data environment.
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: - Identifying new onsite personnel or visitors (for example, assigning badges) - Changes to access requirements - Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).	DocuSign		DocuSign is responsible to manage physical access to its cardholder data environment.
9.3 Control physical access for onsite personnel to the sensitive areas as follows: - Access must be authorized and based on individual job function. - Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.	DocuSign		DocuSign is responsible to manage physical access to its cardholder data environment.
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:	DocuSign		DocuSign is responsible to manage physical access to its cardholder data environment.
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	DocuSign		DocuSign is responsible to manage physical access to its cardholder data environment.
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	DocuSign		DocuSign is responsible to manage physical access to its cardholder data environment.
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	DocuSign		DocuSign is responsible to manage physical access to its cardholder data environment.
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	DocuSign		DocuSign is responsible to manage physical access to its cardholder data environment.
9.5 Physically secure all media.	DocuSign		DocuSign is responsible for securing media used to manage or support the cardholder data environment.
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	DocuSign		DocuSign is responsible for securing media used to manage or support the cardholder data environment.
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:	DocuSign		DocuSign is responsible for securing media used to manage or support the cardholder data environment.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
9.6.1 Classify media so the sensitivity of the data can be determined.	DocuSign		DocuSign is responsible for securing media used to manage or support the cardholder data environment.
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.	DocuSign		DocuSign is responsible for securing media used to manage or support the cardholder data environment.
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	DocuSign		DocuSign is responsible for securing media used to manage or support the cardholder data environment.
9.7 Maintain strict control over the storage and accessibility of media.	DocuSign		DocuSign is responsible for securing media used to manage or support the cardholder data environment.
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	DocuSign		DocuSign is responsible for securing media used to manage or support the cardholder data environment.
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:	DocuSign		DocuSign is responsible for securing media used to manage or support the cardholder data environment.
9.8.1 Shred, incinerate, or pulp hard- copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	DocuSign		DocuSign is responsible for securing media used to manage or support the cardholder data environment.
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	DocuSign		DocuSign is responsible for securing media used to manage or support the cardholder data environment.
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. Note: These requirements apply to card- reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.	Not Applicable		DocuSign does not use POS terminals.
9.9.1 Maintain an up-to-date list of devices. The list should include the following: - Make, model of device - Location of device (for example, the address of the site or facility where the device is located) - Device serial number or other method of unique identification.	Not Applicable		DocuSign does not use POS terminals.
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.	Not Applicable		POS terminals are not part of the DocuSign service offering.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: - Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. - Do not install, replace, or return devices without verification. - Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). - Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	Not Applicable		POS terminals are not part of the DocuSign service offering.
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
Requirement 10: Track and monitor all access to network resources and cardholder data			
10.1 Implement audit trails to link all access to system components to each individual user.	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.2 Implement automated audit trails for all system components to reconstruct the following events:	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.2.1 All individual user accesses to cardholder data	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.2.2 All actions taken by any individual with root or administrative privileges	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.2.3 Access to all audit trails	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.2.4 Invalid logical access attempts	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.2 5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.2.6 Initialization, stopping, or pausing of the audit logs	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
10.2.7 Creation and deletion of system- level objects	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.3 Record at least the following audit trail entries for all system components for each event:	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.3.1 User identification	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.3.2 Type of event	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.3.3 Date and time	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.3.4 Success or failure indication	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.3.5 Origination of event	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.3.6 Identity or name of affected data, system component, or resource.	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).	DocuSign		DocuSign is responsible for the management of its systems and network.
10.4.1 Critical systems have the correct and consistent time.	DocuSign		DocuSign is responsible for the management of its systems and network.
10.4.2 Time data is protected.	DocuSign		DocuSign is responsible for the management of its systems and network.
10.4.3 Time settings are received from industry-accepted time sources.	DocuSign		DocuSign is responsible for the management of its systems and network.
10.5 Secure audit trails so they cannot be altered.	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
10.5.1 Limit viewing of audit trails to those with a job-related need.	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.5.2 Protect audit trail files from unauthorized modifications.	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	DocuSign		DocuSign is responsible to monitor audit trails to identify unauthorized or suspicious activity.
10.6.1 Review the following at least daily: - All security events - Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD - Logs of all critical system components - Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	DocuSign		DocuSign is responsible to monitor audit trails to identify unauthorized or suspicious activity.
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	DocuSign		DocuSign is responsible to monitor audit trails to identify unauthorized or suspicious activity.
10.6.3 Follow up exceptions and anomalies identified during the review process.	DocuSign		DocuSign is responsible to investigate and remediate unauthorized or suspicious activity.
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)	DocuSign		DocuSign is responsible to implement, manage, and maintain audit trails for the DocuSign cardholder data environment. DocuSign is responsible to monitor audit trails to identify unauthorized or suspicious activity.
10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls	DocuSign		DocuSign is responsible to investigate and remediate unauthorized or suspicious activity.
10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
Requirement 11: Regularly test security systems and processes			
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.	DocuSign		DocuSign is responsible for the identification and management of wireless access points connected to the cardholder data environment. DocuSign does not allow wireless networks to connect to any cardholder data environment.
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	DocuSign		DocuSign is responsible for the identification and management of wireless access points connected to the cardholder data environment. DocuSign does not allow wireless networks to connect to any cardholder data environment.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.	DocuSign		DocuSign is responsible for the identification and management of wireless access points connected to the cardholder data environment. DocuSign does not allow wireless networks to connect to any cardholder data environment.
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed. For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.	DocuSign		DocuSign is responsible to establish and maintain a vulnerability management program for its cardholder data environment, including the identification, triage, and remediation of vulnerabilities.
11.2.1 Perform quarterly internal vulnerability scans and rescans as needed, until all “high-risk” vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.	DocuSign		DocuSign is responsible to establish and maintain a vulnerability management program for its cardholder data environment, including the identification, triage, and remediation of vulnerabilities.
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.	DocuSign		DocuSign is responsible to establish and maintain a vulnerability management program for its cardholder data environment, including the identification, triage, and remediation of vulnerabilities.
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	DocuSign		DocuSign is responsible to establish and maintain a vulnerability management program for its cardholder data environment, including the identification, triage, and remediation of vulnerabilities.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
11.3 Implement a methodology for penetration testing that includes the following: - Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) - Includes coverage for the entire CDE perimeter and critical systems - Includes testing from both inside and outside the network - Includes testing to validate any segmentation and scope-reduction controls - Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 - Defines network-layer penetration tests to include components that support network functions as well as operating systems - Includes review and consideration of threats and vulnerabilities experienced in the last 12 months - Specifies retention of penetration testing results and remediation activities results.	DocuSign		DocuSign is responsible to establish and maintain a vulnerability management program for its cardholder data environment, including the identification, triage, and remediation of vulnerabilities.
11.3.1 Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	DocuSign		DocuSign is responsible to establish and maintain a vulnerability management program for its cardholder data environment, including the identification, triage, and remediation of vulnerabilities.
11.3.2 Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	DocuSign		DocuSign is responsible to establish and maintain a vulnerability management program for its cardholder data environment, including the identification, triage, and remediation of vulnerabilities.
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	DocuSign		DocuSign is responsible to establish and maintain a vulnerability management program for its cardholder data environment, including the identification, triage, and remediation of vulnerabilities.
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE	DocuSign		DocuSign is responsible to establish and maintain a vulnerability management program for its cardholder data environment, including the identification, triage, and remediation of vulnerabilities.
11.3.4.1 Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.	DocuSign		DocuSIgn is responsible to perform penetrating testing for its cardholder data environment, including the identification, triage, and remediation of vulnerabilities.
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	DocuSign		DocuSign is responsible to establish and maintain a vulnerability management program for its cardholder data environment, including the identification, triage, and remediation of vulnerabilities.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre- configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).	DocuSign		DocuSign is responsible to establish and maintain a vulnerability management program for its cardholder data environment, including the identification, triage, and remediation of vulnerabilities.
11.5.1 Implement a process to respond to any alerts generated by the change- detection solution.	DocuSign		DocuSign is responsible to investigate and remediate unauthorized or suspicious activity.
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
Requirement 12: Maintain a policy that addresses information security for all personnel			
12.1 Establish, publish, maintain, and disseminate a security policy.	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
12.1.1 Review the security policy at least annually and update the policy when the environment changes.	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
12.2 Implement a risk-assessment process that: - Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), - Identifies critical assets, threats, and vulnerabilities, and - Results in a formal risk assessment. Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.	DocuSign		DocuSign is responsible to implement and maintain a risk assessment process specific to the DocuSign services.
12.3 Develop usage policies for critical technologies and define proper use of these technologies. Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e- mail usage and Internet usage. Ensure these usage policies require the following:	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
12.3.1 Explicit approval by authorized parties	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
12.3.2 Authentication for use of the technology	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
12.3.3 A list of all such devices and personnel with access	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
12.3.5 Acceptable uses of the technology	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
12.3.6 Acceptable network locations for the technologies	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
12.3.7 List of company-approved products	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.
12.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program and communication to executive management	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
12.5 Assign to an individual or team the following information security management responsibilities:	DocuSign		DocuSign is responsible to assign security roles and responsibilities to appropriate personnel.
12.5.1 Establish, document, and distribute security policies and procedures.	DocuSign		DocuSign is responsible to assign security roles and responsibilities to appropriate personnel.
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	DocuSign		DocuSign is responsible to assign security roles and responsibilities to appropriate personnel.
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	DocuSign		DocuSign is responsible to assign security roles and responsibilities to appropriate personnel.
12.5.4 Administer user accounts, including additions, deletions, and modifications.	DocuSign		DocuSign is responsible to assign security roles and responsibilities to appropriate personnel.
12.5.5 Monitor and control all access to data.	DocuSign		DocuSign is responsible to assign security roles and responsibilities to appropriate personnel.
12.6 Implement a formal security awareness program to make all personnel aware of the importance of the cardholder data security policy and procedures.	Shared	The customer is responsible to ensure that individuals who manage cardholder data within DocuSign systems complete security awareness training upon hire and annually thereafter.	DocuSign is responsible for managing security awareness training for its employees as related to the DocuSign product and services.
12.6.1 Educate personnel upon hire and at least annually. Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.	Shared	The customer is responsible to ensure that individuals who manage cardholder data within DocuSign systems complete security awareness training upon hire and annually thereafter.	DocuSign is responsible for managing security awareness training for its employees as related to the DocuSign product and services.
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	Shared	The customer is responsible to ensure that individuals who manage cardholder data within DocuSign systems complete security awareness training upon hire and annually thereafter.	DocuSign is responsible for managing security awareness training for its employees as related to the DocuSign product and services.
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.	Shared	The customer is responsible to screen potential personnel who will have access to cardholder data prior to employment.	DocuSign is responsible for managing background screening of its employees.
12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	DocuSign		DocuSign is responsible to maintain policies and procedures related to the management of cardholder data.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
12.8.1 Maintain a list of service providers.	DocuSign		DocuSign is responsible for governing service providers that it shares cardholder data with or might otherwise affect the security of cardholder data.
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.	DocuSign		DocuSign is responsible for governing service providers that it shares cardholder data with or might otherwise affect the security of cardholder data.
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	DocuSign		DocuSign is responsible for governing service providers that it shares cardholder data with or might otherwise affect the security of cardholder data.
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	DocuSign		DocuSign is responsible for governing service providers that it shares cardholder data with or might otherwise affect the security of cardholder data.
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	DocuSign		DocuSign is responsible for governing service providers that it shares cardholder data with or might otherwise affect the security of cardholder data.
12.9 **Additional requirement for service providers only**: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.	DocuSign		DocuSign is responsible to acknowledge its responsibility to protect customers' cardholder data that is stored or processed by DocuSign services in accordance with PCI DSS.
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	DocuSign		DocuSign is responsible to document, implement, and maintain a security incident response program and respond to incidents related to cardholder data.

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: - Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum - Specific incident response procedures - Business recovery and continuity procedures - Data backup processes - Analysis of legal requirements forreporting compromises - Coverage and responses of all critical system components - Reference or inclusion of incident response procedures from the payment brands.	DocuSign		DocuSign is responsible to document, implement, and maintain a security incident response program and respond to incidents related to cardholder data.
12.10.2 Test the plan at least annually.	DocuSign		DocuSign is responsible to document, implement, and maintain a security incident response program and respond to incidents related to cardholder data.
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	DocuSign		DocuSign is responsible to document, implement, and maintain a security incident response program and respond to incidents related to cardholder data.
12.10.4 Provide appropriate training to staff with security breach response responsibilities.	DocuSign		DocuSign is responsible to document, implement, and maintain a security incident response program and respond to incidents related to cardholder data.
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion- prevention, firewalls, and file-integrity monitoring systems.	DocuSign		DocuSign is responsible to document, implement, and maintain a security incident response program and respond to incidents related to cardholder data.
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	DocuSign		DocuSign is responsible to document, implement, and maintain a security incident response program and respond to incidents related to cardholder data.
12.11 Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: - Daily log reviews - Firewall rule-set reviews - Applying configuration standards to new systems - Responding to security alerts - Change management processes	DocuSign		DocuSign is responsible to perform quarterly PCI security assessments.
12.11.1 Additional requirement for service providers only: Maintain documentation of quarterly review process to include: - Documenting results of the reviews - Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program	DocuSign		DocuSign is responsible to perform quarterly PCI security assessments.
Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers			

PCI DSS REQUIREMENTS v3.2.1	Responsible Party *(DocuSign, Customer, Shared, or Not Applicable)*	Customer Responsibility Description	DocuSign Responsibility Description
A.1 Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.	Not Applicable	DocuSign is not a Shared Hosting Provider.	
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	Not Applicable	DocuSign is not a Shared Hosting Provider.	
A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only.	Not Applicable	DocuSign is not a Shared Hosting Provider.	
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	Not Applicable	DocuSign is not a Shared Hosting Provider.	
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	Not Applicable	DocuSign is not a Shared Hosting Provider.	
Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections			
A2.1 Where POS POI terminals (at the merchant or payment acceptance location) use SSL and/or early TLS, the entity must confirm the devices are not susceptible to any known exploits for those protocols. Note: This requirement is intended to apply to the entity with the POS POI terminal, such as a merchant. This requirement is not intended for service providers who serve as the termination or connection point to those POS POI terminals. Requirements A2.2 and A2.3 apply to POS POI service providers.	Not Applicable	DocuSign does not use POS terminals.	
A2.2 Requirement for Service Providers Only: All service providers with existing connection points to POS POI terminals referred to in A2.1 that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.	Not Applicable	DocuSign does not use POS terminals.	
A2.3 Requirement for Service Providers Only: All service providers must provide a secure service offering.	Not Applicable	DocuSign does not use POS terminals.	

Attestation of Scan Compliance

tenable.io

A.1 Scan Customer Information	
Company:	DocuSign
Contact Name:	Gary Masnica
Job Title:	Information Security Engineer
Telephone:	18777202040
Email:	gary.masnica@docusign.com
Business Address:	221 Main St #1550
City:	San Francisco
State/Province:	CA
ZIP/Postal Code:	94105
Country:	
Website/URL:	docusign.com

A.2 Approved Scanning Vendor Information	
Company:	Tenable Network Security
Contact Name:	Jonah Goldsmith
Job Title:	PCI Analyst
Telephone:	(410) 872-0555
Email:	jgoldsmith@tenable.com
Business Address:	7021 Columbia Gateway Drive Suite 500
City:	Columbia
State/Province:	MD
ZIP/Postal Code:	21046
Country:	US
Website/URL:	www.tenable.com

A.3 Scan Status - eSig PCI ASV External - September 2022			
Date scan completed:	09/09/2022	Scan expiration date:	12/08/2022
Compliance status:	PASS	Scan report type:	Full scan
Number of unique in-scope components scanned:			774
Number of identified failing vulnerabilities:			0
Number of components found by ASV but not scanned because customer confirmed they were out of scope:			0

A.4 Scan Customer Attestation

DocuSign attests on 09/16/2022 that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.3, "Scan Status") includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions—including compensating controls if applicable—is accurate and complete. DocuSign also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

A.5 ASV Attestation

This scan and report was prepared and conducted by Tenable Network Security under certificate number 5049-01-11, according to internal processes that meet PCI DSS Requirement 11.2.2 and the ASV Program Guide. Tenable Network Security attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by Jonah Goldsmith.

tenable

Attestation of Scan Compliance

A.1 Scan Customer Information	
Company:	DocuSign
Contact Name:	Gary Masnica
Job Title:	Information Security Engineer
Telephone:	18777202040
Email:	gary.masnica@docusign.com
Business Address:	221 Main St #1550
City:	San Francisco
State/Province:	CA
ZIP/Postal Code:	94105
Country:	
Website/URL:	docusign.com

A.2 Approved Scanning Vendor Information	
Company:	Tenable Network Security
Contact Name:	Bin Rong
Job Title:	PCI Analyst
Telephone:	(410) 872-0555
Email:	brong@tenable.com
Business Address:	6100 Merriweather Drive 12th Floor
City:	Columbia
State/Province:	MD
ZIP/Postal Code:	21044
Country:	US
Website/URL:	www.tenable.com

A.3 Scan Status - New Attestation			
Date scan completed:	12/03/2022	Scan expiration date:	03/03/2023
Compliance status:	PASS	Scan report type:	Full scan
Number of unique in-scope components scanned:			803
Number of identified failing vulnerabilities:			0
Number of components found by ASV but not scanned because customer confirmed they were out of scope:			0

A.4 Scan Customer Attestation

DocuSign attests on 12/09/2022 that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.3, "Scan Status") includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions—including compensating controls if applicable—is accurate and complete. DocuSign also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

A.5 ASV Attestation

This scan and report was prepared and conducted by Tenable Network Security under certificate number 5049-01-11, according to internal processes that meet PCI DSS Requirement 11.2.2 and the ASV Program Guide. Tenable Network Security attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by Bin Rong.

Cobalt Labs Inc.
575 Market Street
San Francisco, CA 94105
415-651-7028
hello@cobalt.io

03/02/2023

To whom it may concern,

Cobalt conducted a gray box pentest of the eSignature Platform application and API to assess the risk posture and identify security issues that could negatively affect DocuSign's data, systems, or reputation. The scope of the assessment covered eSignature Platform and included credentials for various levels of privilege within the scope. The pentest was conducted by 6 pentesters between Feb 6, 2023 and Feb 27, 2023.

This pentest was a manual assessment of the security of the application's functionality, business logic, and vulnerabilities, such as those cataloged in the Open Web Application Security Project (OWASP) Top 10. The assessment also included a review of security controls and requirements listed in the OWASP Application Security Verification Standard (ASVS). The pentesters leveraged tools to facilitate their work. However, the majority of the assessment involved manual analysis.

During testing, Cobalt's pentesters tested for vulnerabilities and rated them based on the following categories:

Critical	High	Medium	Low	Informational
0	0	3	2	1

As the pentesting team identified vulnerabilities, they reported all of these issues to DocuSign for remediation.

Sincerely,

The Cobalt Team

DocuSign

Reports and Attestations:

Certificate of Liability Insurance

CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY) 04/28/23

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	CONTACT NAME:	
Aon Risk Insurance Services West, Inc. San Francisco CA Office 425 Market Street Suite 2800 San Francisco CA 94105 USA	PHONE (A/C. No. Ext): (866) 283-7122	FAX (A/C. No.): (800) 363-0105
	E-MAIL ADDRESS:	

INSURED	INSURER(S) AFFORDING COVERAGE	NAIC #
DocuSign, Inc. 221 Main Street, Suite 1000 San Francisco CA 941051925 USA	INSURER A: StarNet Insurance Company	40045
	INSURER B: Berkley National Insurance Company	38911
	INSURER C: Endurance American Specialty Ins Co.	41718
	INSURER D:	
	INSURER E:	
	INSURER F:	

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS. **Limits shown are as requested**

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X **COMMERCIAL GENERAL LIABILITY** CLAIMS-MADE [X] OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: POLICY [ ] PRO-JECT [X] LOC OTHER:			TCP700795717	04/27/2023	04/27/2024	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG	$1,000,000 $1,000,000 $15,000 $1,000,000 $3,000,000 $3,000,000
A	**AUTOMOBILE LIABILITY** ANY AUTO OWNED AUTOS ONLY X HIRED AUTOS ONLY SCHEDULED AUTOS X NON-OWNED AUTOS ONLY			TCP700795717	04/27/2023	04/27/2024	COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)	$1,000,000
A	X **UMBRELLA LIAB** X OCCUR **EXCESS LIAB** CLAIMS-MADE DED RETENTION			TCP700795717	04/27/2023	04/27/2024	EACH OCCURRENCE AGGREGATE	$5,000,000 $5,000,000
B	**WORKERS COMPENSATION AND EMPLOYERS' LIABILITY** ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? Y / N: N **(Mandatory in NH)** If yes, describe under DESCRIPTION OF OPERATIONS below	N / A		TWC700795519	04/27/2023	04/27/2024	X PER STATUTE OTH-ER E.L. EACH ACCIDENT E.L. DISEASE-EA EMPLOYEE E.L. DISEASE-POLICY LIMIT	 $1,000,000 $1,000,000 $1,000,000
C	E&O-PL-Primary			NRO30006187402 Claims-Made SIR applies per policy terms & conditions	04/27/2023	04/27/2024	Policy Aggregate	$10,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Evidence of Insurance. Professional Liability policy includes Network Security, Privacy Protection and Cyber Liability policy.

CERTIFICATE HOLDER

DocuSign, Inc.
221 Main Street, Suite 1000
San Francisco CA 94105-1925 USA

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Aon Risk Insurance Services West, Inc.

Holder Identifier :

Certificate No :

ACORD 25 (2016/03) The ACORD name and logo are registered marks of ACORD

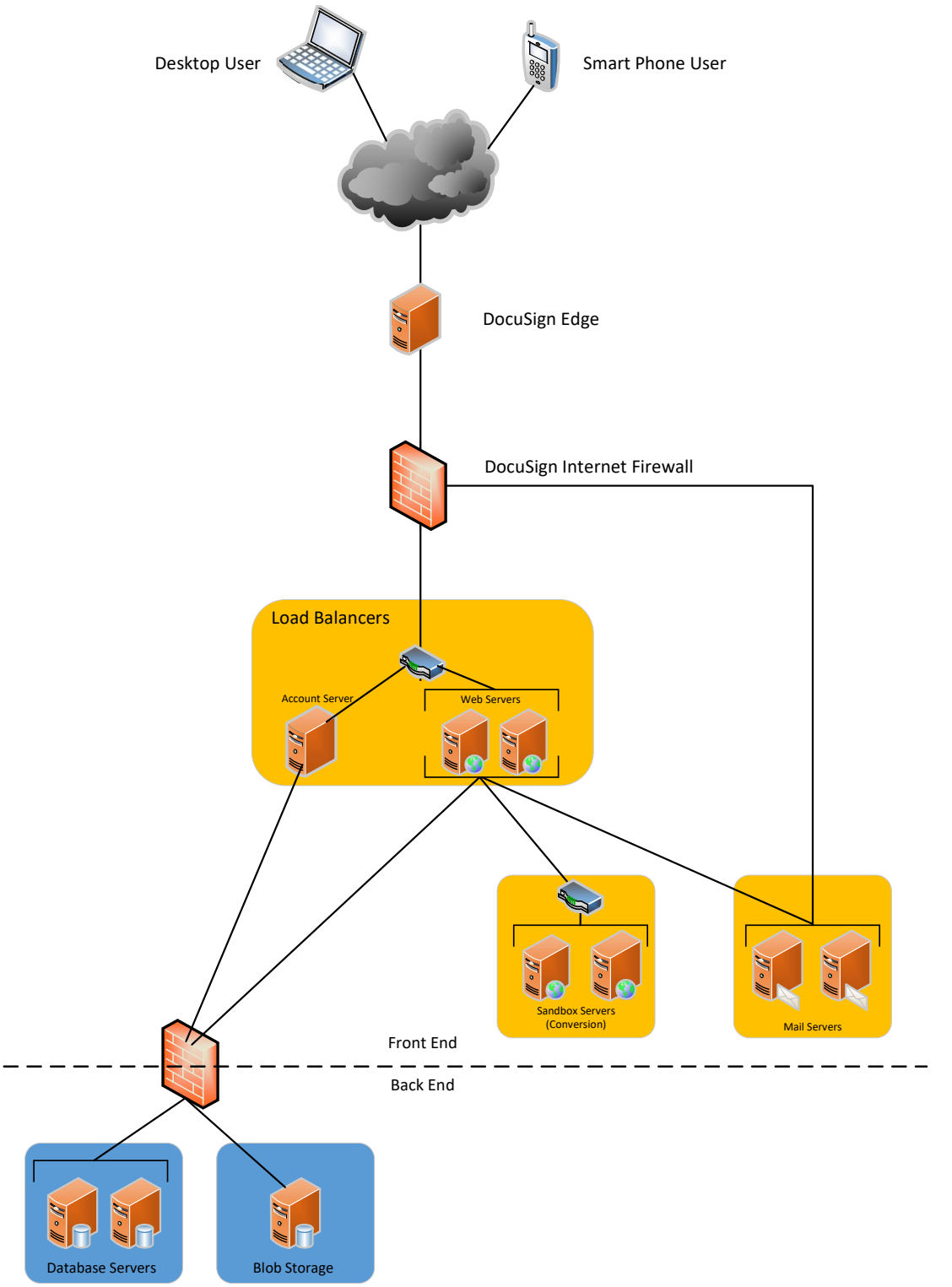
DocuSign®

Reports and Attestations:

Customer Data Flow Diagram

DocuSign

Customer Data Flow Diagram



About DocuSign
DocuSign helps organizations connect and automate how they prepare, sign, act on and manage agreements. As part of the DocuSign Agreement Cloud, DocuSign offers eSignature: the world's #1 way to sign electronically on practically any device, from almost anywhere, at any time. Today, more than 750,000 customers and hundreds of millions of users in over 180 countries use DocuSign to accelerate the process of doing business and to simplify people's lives.

DocuSign, Inc.
221 Main Street, Suite 1000
San Francisco, CA 94105
www.docusign.com

For more information
call +1-877-720-2040

STAP ST050923COMPLNDAGLB