Dropbox Service Organization Controls (SOC) 3 Report

Management's Report of its Assertions on the Effectiveness of Its Controls over the Dropbox Sign System Based on the Trust Services Criteria for Security, Availability, and Confidentiality

Period: October 1, 2022 to September 30, 2023

Ernst & Young LLP
Suite 1600
560 Mission Street
San Francisco, CA 94105-2907

Tel: +1 415 894 8000
Fax: +1 415 894 8099
ey.com

Report of Independent Accountants

Management of Dropbox, Inc.

Scope:
We have examined management's assertion, contained within the accompanying Management's Report of its Assertions on the Effectiveness of Its Controls over the Dropbox Sign System (Assertion), that Dropbox, Inc.'s controls over the Dropbox Standard, Dropbox Advanced, Dropbox Enterprise and Dropbox Education System (System) were effective throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Dropbox, Inc.'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 (With Revised Points of Focus – 2022)*.

Dropbox, Inc. uses Amazon Web Services (AWS) (Subservice Organization) to provide physical safeguards, environmental safeguards, infrastructure support and management, and storage services. The description of the boundaries of the system presented in the Dropbox Sign System Description Overview indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with related controls at Dropbox, Inc., to provide reasonable assurance that Dropbox, Inc.'s service commitments and system requirements are achieved based on the applicable trust service criteria. The description of the boundaries of the system presents the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS. Our procedures did not extend to the services provided by AWS and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period October 1, 2022 to September 30, 2023.

Management's responsibilities
Dropbox, Inc.'s management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that Dropbox, Inc.'s service commitments and system requirements were achieved. Dropbox, Inc. management is also responsible for providing the accompanying assertion about the effectiveness of controls within the system, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of the System.

Building a better working world

Our responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Dropbox, Inc.'s relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we consider necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Dropbox, Inc.'s cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

We are required to be independent of Dropbox, Inc. and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Inherent limitations:

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Dropbox, Inc.'s service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the System or controls, or the failure to make needed changes to the System or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion:

In our opinion, Dropbox, Inc.'s controls over the System were effective throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst & Young LLP

November 22, 2023

Management's Report of its Assertion on the Effectiveness of Its Controls Over the Dropbox Sign System Based on the Trust Services Criteria for Security, Availability, and Confidentiality

We, as management of Dropbox, Inc., are responsible for:

- Identifying the Dropbox Sign System (System) and describing the boundaries of the System, which are presented in the Dropbox Sign System Description Overview
- Identifying our principal service commitments and system requirements which are presented in the Dropbox Sign System Description Overview
- Identifying the risks that would threaten the achievement of our principal service commitments and service requirements that are the objectives of our System
- Identifying, designing, implementing, operating, and monitoring effective controls over the Dropbox Sign System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories and associated criteria that are the basis of our assertion

Dropbox, Inc. uses Amazon Web Services (AWS) to provide physical safeguards, environmental safeguards, infrastructure support and management, and storage services. The description of the boundaries of the system presented in the Dropbox Sign System Description Overview indicates that complementary controls at AWS that are suitably designed and operating effectively are necessary, along with controls at Dropbox, Inc. to achieve the service commitments and system requirements. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Dropbox, Inc.'s controls. It does not disclose the actual controls at AWS.

We confirm to the best of our knowledge and belief that the controls over the System were effective throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus – 2022*).

Dropbox Sign System Description Overview

Company Background

Since 2008, Dropbox, Inc. (“Dropbox” or “the Company”) has helped users store their files (such as documents, photos, and videos), access them from anywhere, and share them easily. In 2019, Dropbox acquired HelloSign, now called Dropbox Sign, which offers e-signature and electronic fax solutions for businesses through a cloud-based digital workflow platform with customizable application program interface (API) features for simplified integration. The Company is based in San Francisco, California, United States.

Description of Services

The following Dropbox Sign services are included in standard and premium plans, which offer specific feature packages tailored to different organizational needs:

Dropbox Sign and API

Dropbox Sign is the flagship offering that gives users the ability to sign documents electronically, eliminating the need for paper-based signatures. The Dropbox Sign API gives customers the ability to integrate the product into their own products and workflows. The Dropbox Sign API enables features such as signature capture; custom workflows and fields; text tags; and a white label offering for self-branding.

Dropbox Fax and API

Dropbox Fax is a paperless fax product that enables businesses to customize their faxing experience without the need for a physical fax machine. The Dropbox Fax API allows for integration into users’ custom solutions. It offers the same functionality as the web version, such as forwarding faxes to e-mail and sending documents to fax numbers without utilizing the web interface.

Dropbox Forms and API

Dropbox Forms is a mobile-first platform that uses an intuitive interface that guides customers through agreements and forms without ever needing to see the underlying document they are completing. With drag-and-drop functionality, users can build multi-form workflows that include data validation and conditional logic in a matter of minutes. The Dropbox Forms API allows for integration into users’ backend systems.

Principal Service Commitments

Commitments are declarations made by management to customers regarding the performance of the Dropbox Sign System. Commitments are communicated in policies and procedures, system design documentation, and contracts with customers.

System requirements are specifications regarding how the Dropbox Sign System should function to meet Dropbox Sign’s principal commitments to user entities. System requirements are specified in the Company’s policies and procedures, which are available to all employees.

Dropbox Sign's principal service commitments related to the Dropbox Sign, Dropbox Fax, and Dropbox Forms Applications system include the following:

- System access is granted to authorized personnel only
- Data is protected at rest and in transit
- Regular security assessments
- Regular system updates
- Protection of customer and user data and security of the information system from unauthorized access, use, modification, disclosure, destruction, threats, or hazards
- Development, implementation, and maintenance of an information security program designed to protect the security of the system and its information
- Risk assessments are performed for both internal and external threats to the system and its information
- Ability to recover and restore customer data
- Timely, reliable, and continuous access to and use of information and systems to support operations
- Maintain customer data as confidential and not to disclose information to any unauthorized parties without written consent
- Data is retained for the life of the user's account, or until a customer request for data deletion.

In accordance with Dropbox Sign's assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Components of the System Used to Provide the Service

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

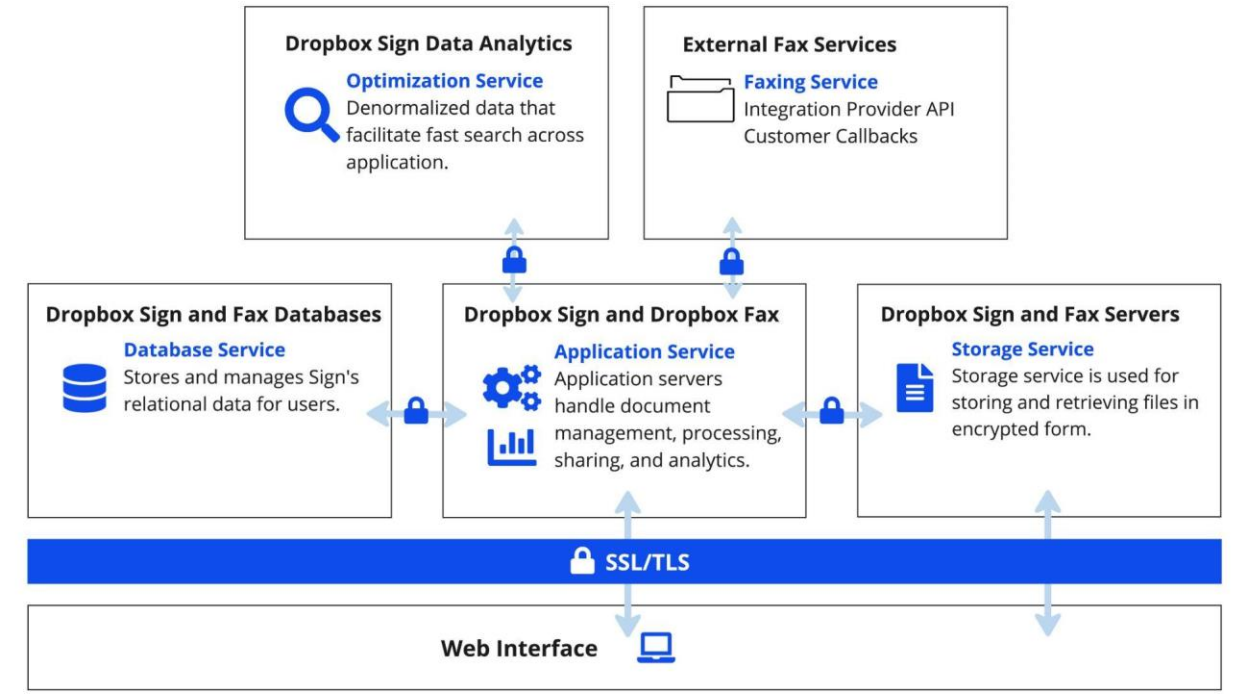
Dropbox Sign leverages Amazon Web Services (AWS) as its Infrastructure as a Service (IaaS) provider. Dropbox Sign does not host the in-scope applications in co-located data centers.

Operating Environments

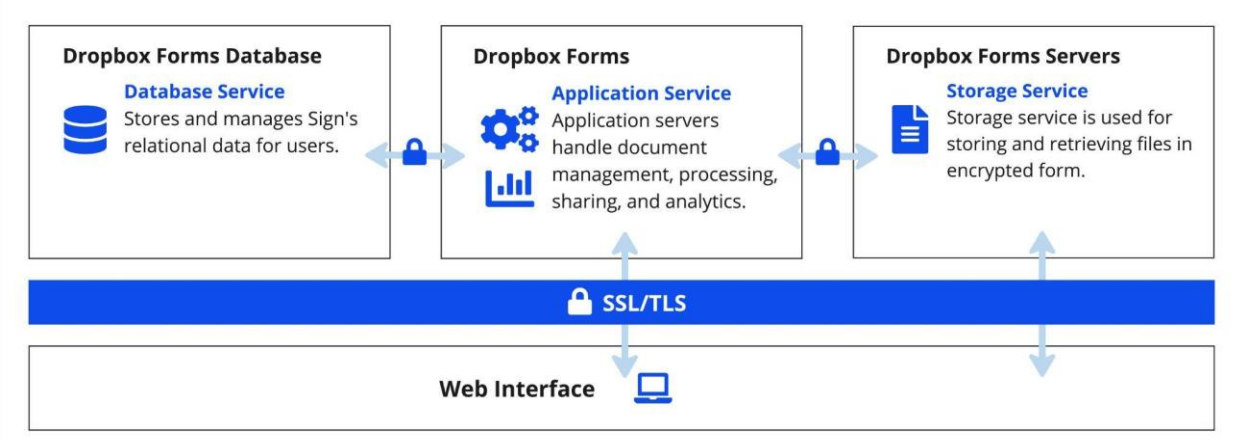
Dropbox Sign has separate AWS accounts for production and non-production (staging and quality assurance) environments, which helps ensure logical separation. Development efforts are handled locally on developer machines.

Dropbox Sign's infrastructure details for the in-scope applications are detailed in the following diagrams:

Dropbox Sign and Dropbox Fax



Dropbox Forms



Infrastructure and Software

The system is designed to restrict logical access to information assets. The system makes use of dedicated AWS accounts and virtual private clouds (VPCs) to help ensure that the organization's infrastructure and data does not overflow or interact with any other AWS tenant. Within each VPC, the system is segregated into logical security groups to help ensure internal processes can only interact as intended. The system is designed with logical controls in place where customer data is segregated from others. As a result, one customer cannot view the data of another customer to protect against unintended information disclosure.

The organization uses separate environments for testing, staging, and production to help ensure customer data is not compromised. Access to the production environment and customer data is restricted via access control policies. Dropbox Sign employees access these environments via bastion host or application user interface (UI).

The system utilizes AWS EC2 security groups to configure inbound and outbound firewall traffic to allow access only to required services and deny all others. The traffic may be restricted by any combination of protocol, port, and source (individual IP, classless inter-domain routing (CIDR) subnet, or other customer-defined security group).

As a feature of the AWS cloud hosting model, the switching, routing, and security nodes in the system infrastructure are designed by AWS. The organization's Engineering Team manages the configuration of the infrastructure and practices the principle of least privilege to help ensure communication between services inside and outside the boundary is kept to the bare minimum. The information security and Engineering teams review the security groups quarterly to help ensure communication between services is appropriate and kept to a minimum.

The in-scope infrastructure consists of multiple applications, operating system platforms, and databases, as shown in the table below:

Primary Infrastructure

Production System/ Application	Business Function Description	Platform	Physical Location
Dropbox Sign and Dropbox Fax Queuing Service	Queueing service for asynchronous request queuing.	Dropbox Sign Proprietary	AWS (us-east-1, us-east-2)
Dropbox Sign and Dropbox Fax Search	Distributed, multitenant capable, full-text search engine.	Dropbox Sign Proprietary	AWS (us-east-1, us-east-2)
Dropbox Forms Portable Document Format (PDF) Mapping	Mechanism for users to indicate where fields filled in by a workflow participant should appear on an underlying PDF.	Dropbox Sign Proprietary	AWS (us-east-1, us-east-2)
Bastion Hosts	Deployed by Engineering Team for administrative access to production systems.	Linux	AWS (us-east-1, us-east-2)
AWS Relational Database Service (RDS)	Database solution for storage of operational data.	MySQL	AWS (us-east-1, us-east-2)

Production System/ Application	Business Function Description	Platform	Physical Location
Amazon EC2	Virtual instances that provide secure, resizable compute capacity in the cloud that allow for the scaling of resources based on the requirements of target workloads.	Amazon Proprietary	AWS (us-east-1, us-east-2)
Amazon Simple Storage Service (S3)	Encrypted object storage service utilized to store and protect user documents across multiple availability zones.	Amazon Proprietary	AWS (us-east-1, us-west-2)

Secondary Infrastructure and Supporting Software

The following secondary infrastructure and supporting software is utilized in support of the delivery of the services:

- Puppet – automated configuration management tool to distribute Amazon Machine Images (AMI) and the latest software and security updates.
- AWS Shield Advanced – provides 24X7 access to the AWS Shield Response Team (SRT), who proactively apply any mitigations necessary for sophisticated infrastructure layer (Layer 3 or 4) attacks using additional techniques like traffic engineering.
- AWS web application firewall (WAF) – WAF that helps protect the web applications and APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources.
- CloudWatch – monitoring and management service that collects monitoring and operational data in the form of logs, metrics, and events for AWS resources.
- Logstash – open-source data collection engine with real-time pipelining capabilities.
- Threat Stack – cloud security management and compliance solution that provides risk identification and real-time threat detection across cloud workloads.
- PagerDuty – incident management platform used to provide notifications, automatic escalations, and other functionality to help teams detect and fix infrastructure issues.
- Jira – work management tool used for workflow mapping and issue tracking.
- Okta – identity and access management software used to help manage and secure user authentication.
- LastPass – password management tool used to keep passwords safe and secure.
- YubiKey – security key hardware solution utilized to enforce multi-factor authentication when accessing certain production resources.

Control Environment

The control environment at Dropbox Sign is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the Dropbox board of directors.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of the Company's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of the Company's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. The Company's Trust Management Team is responsible for developing, maintaining, reviewing, and approving internal security, availability, and confidentiality policies related to Dropbox Sign, Dropbox Fax, and Dropbox Forms applications as well as reviewing, updating, approving the policies at least annually, and retaining a summary of revisions or historical copies of each policy.

Dropbox is responsible for implementing controls for new employee hiring policies and procedures; employment candidate screening and onboarding procedures; evaluating the competency of existing personnel; maintaining training policies and procedures, the employee handbook, and the code of conduct; defining job descriptions; and other HR functions that may relate to the stated criterion.

Dropbox Board of Directors Oversight

Dropbox is responsible for implementing controls that ensures the board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Organizational Structure and Assignment of Authority and Responsibility

The Company's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. The Company maintains a personnel directory to delineate reporting lines and organizational structure, including an information security function. The Company's personnel directory is available to internal personnel (employees and contractors) via the Company's intranet.

Dropbox is responsible for implementing controls for defining job descriptions and other HR functions that establish authorities and responsibilities of personnel Commitment to Competence

Dropbox is responsible for implementing controls for new employee hiring policies and procedures; employment candidate screening and onboarding procedures; evaluating the competency of existing personnel; maintaining training policies and procedures, the employee handbook, and the code of conduct; defining job descriptions; and other HR functions that may relate to the stated criterion.

Commitment to Competence

Dropbox is responsible for implementing controls for new employee hiring policies and procedures; employment candidate screening and onboarding procedures; evaluating the competency of existing personnel; maintaining training policies and procedures, the employee handbook, and the code of conduct; defining job descriptions; and other HR functions that may relate to the stated criterion.

Accountability

The Company's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward information processing, accounting functions, and personnel. The Company maintains a personnel directory to delineate reporting lines and organizational structure, including an information security function. The Company's personnel directory is available to internal personnel (employees and contractors) via the Company's intranet.

The Company's Trust Management Team performs a review of the Dropbox Sign trust program at least annually. An internal audit of the Dropbox Sign trust program is performed at least annually or when deemed necessary due to significant changes in the environment. The Company's Governance, Risk, and Compliance team documents and tracks findings until resolution.

The Company contracts a third-party provider to perform external independent audits of Dropbox Sign's security, availability, and confidentiality controls at least annually. The Company documents and tracks the resulting findings until resolved. The Company makes independent external audit reports available to potential and current Dropbox Sign customers.

Dropbox is responsible for implementing controls for new employee hiring policies and procedures; employment candidate screening and onboarding procedures; evaluating the competency of existing personnel; maintaining training policies and procedures, the employee handbook, and the code of conduct; defining job descriptions; and other HR functions that may relate to the stated criterion.

People

Dropbox Sign personnel are the employees and contractors responsible for managing and operating Dropbox Sign systems and services. The following personnel are involved in the governance, operation, and use of the system:

The Dropbox Trust Management Team

The Dropbox Trust Management team plays a key role in the Dropbox Sign Trust Program and regularly reviews and updates security policies, provides security training, performs application and network security testing, monitors compliance with security policies, and conducts internal and external assessments of the control environment. Such reviews occur at least annually and on an as-needed basis. The Trust Management Team also performs an annual review of the overall effectiveness of the Dropbox Sign Trust Program to ensure continual improvement of the security, availability, and confidentiality controls.

The Dropbox Trust Management Team presents the Dropbox Sign Trust Program's top risks and roadmap on an annual basis to members of the Board of Directors. These members approve the Dropbox Sign Trust Program and provide feedback on the results of the Trust Program's top risks.

The Engineering Team

Responsible for creating and implementing systems and software and improving the existing infrastructure. The engineering team is also tasked with adhering to the change management policies and procedures when developing, testing, and deploying changes to production. Furthermore, Engineering personnel are responsible for tracking/patching vulnerabilities.

Dropbox Legal

Responsible for reviewing communications with customers from a legal perspective. The legal team fields and responds to incidents of unauthorized use and disclosure.

The Security Team

Responsible for security monitoring; periodic vulnerability scanning; network and application layer penetration testing; security awareness training; incident response; security architecture; compliance oversight; and the development of security policies.

The Information Technology (IT) Team

Responsible for providing technical assistance across the organization including access provisioning, access removal, and tracking/patching vulnerabilities.

Dropbox Board of Directors

Dropbox maintains responsibility for ensuring that the board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Dropbox Human Resources

Dropbox maintains ownership of the Human Resources functions supporting Dropbox Sign's environment, which include responsibility for new employee hiring policies and procedures; employment candidate screening and onboarding procedures; evaluating the competency of existing personnel; maintaining training policies and procedures and the code of conduct; and defining job descriptions.

Policies

Dropbox Sign maintains the formal policies and procedures concerning various security, availability, and confidentiality matters. The policies and procedures allow employees to perform their job responsibilities in accordance with established goals and objectives and to sustain an effective control environment.

The information security policies are developed in relation to the Company's security, availability, processing integrity, confidentiality, and privacy commitments. The policies are reviewed at least annually, or as needed, by the Dropbox Trust Management Team, which consists of representative individuals from Teams within the organization, including the Security, Engineering, Operations, and Legal Teams.

Dropbox has established the following policies intended for employees and contractors:

- Dropbox Sign Trust Program
- Information Security
- Physical Security

- User Data Privacy
- Data Classification
- Incident Response
- Mobile Device Security
- Unauthorized Copyright Materials
- Vulnerability Management
- Baseline Security Configuration
- Travel Security
- Privacy Program
- Payments Environment Security

Dropbox has established the following policies intended for employees and contractors with responsibilities for organizational resilience and safety:

- Business Continuity

Dropbox has established the following policies intended for employees and contractors with access to Dropbox systems:

- Logical Access Control
- Change Management
- Production Physical Access
- Sales and Customer Experience Security

Dropbox Engineering Teams maintain a series of operating procedures which provide guidance to its members on the day-to-day performance of their roles. The operating procedures are updated on an annual basis (e.g. for significant changes related to engineering operations).

The policies and supporting operating procedures are made available within the corporate network and provide employees with direction for corporate and production environment security, physical and environmental safety, logical access management, change management, incident management, compliance, monitoring, and risk management. New employees must acknowledge the Information Security Policy as a component of the onboarding process. The Trust Management Team reviews and updates the policies based on technological, regulatory, contractual, and environmental changes to the Dropbox systems, and communicates significant changes to Dropbox personnel via email and the corporate intranet. As deemed necessary by the Trust Management Team, communications are sent to internal users via email to notify them of changes to their security obligations or to provide recommendations on how to best protect themselves from current security threats.

Additionally, the Dropbox Legal Team maintains a Worldwide Code of Conduct which is reviewed at least annually. The Code of Conduct is designed to deter wrongdoing and promote employee integrity, honesty and ethics, compliance with local laws and regulations, and fiscal responsibility. Dropbox requires employees and contractors with access to systems to read and acknowledge the Code of Conduct as part of the onboarding process and at least annually thereafter.

Internal Communications

Effective communication and exchange of information is an integral component of Dropbox's internal control system. Dropbox ensures that information is identified, processed, and reported by various systems in a form and time frame necessary to manage operations.

Dropbox has developed various methods of internal communication to ensure employees understand their individual roles and responsibilities. These methods include:

- Employee onboarding orientation and required ongoing security awareness and role based training programs.
- Technical learning events hosted by members of engineering, product, and design.
- Meetings with respective Teams and management.
- Periodic communication regarding changes to information security policies and current security threats.
- The existence and communication of a security intranet page available to all Dropbox personnel, and includes information security policies, the design and operation of the system, how to report suspected security, availability, processing integrity, confidentiality, or privacy incidents or breaches, best practices, industry news updates, etc.

The Dropbox Security Team is responsible for maintaining knowledge of current security news, issues, and threat intelligence. The Team is also responsible for communicating security practices to employees and communicating specialized information on threat intelligence to teams on a need-to-know basis.

External Communications

Customers and external users are provided a description of the system made available via Dropbox Sign's website. The description includes system boundaries and describes relevant system components and how the system components address Dropbox Sign's ability to meet its security, availability, and confidentiality commitments. System changes that could potentially impact the system's commitments are communicated to external users via the status page of the company website. Customer responsibilities and procedures for reporting operational failures, incidents, problems, concerns, and complaints are also described and made available to customer and external users via Dropbox Sign's website. The Company further requires third-party providers and business associates with access to confidential information and/or customer data sign a contractual agreement that includes confidential provisions. further requires individual users to provide express agreement to the terms of service and acceptable use policy before the provision of services. Changes to the Dropbox Sign terms of service are posted on their dedicated webpages. The Dropbox Sign terms of service and acceptable use policy provide notice of the following terms:

- The use of trusted third parties in the provision, improvement, protection, and promotion of the services

- The obligations of users and Dropbox Sign commitments to those users

- The effect of termination on user data accessibility and/or transportability

Dropbox Sign customer administrators or representatives must agree to the standard or custom business agreement before provision of the services. These individuals also agree they have authority to bind their organization to the business agreement. Standard or custom versions of the Dropbox Sign terms of service provide notice of the following terms:

- The obligations of business and education customers and the Company's commitments to those customers (unless prohibited by applicable law)

- Any dispute brought by the customer related to the terms may be reported through an established dispute resolution process or through the courts. Reported disputes are reviewed by the legal team and resolved in a timely manner following a dispute resolution process

The Company further publishes whitepapers and other information about the Dropbox Sign system, its boundaries, and the services provided on the company website. These publications include information about:

- The manner in which customers may request confidential information, such as detailed policies, procedures, audits, and assessments under non-disclosure agreement (NDA)

- The cryptographic controls Dropbox Sign uses to protect customer data and information that may assist customers in adding additional security controls

- The controls used to protect customer secret authentication data and the procedures for user authentication

- The scope, schedule, and methods used for replication and/or backup and recovery of customer data

- The ability of the customer administrators to manage users' roles and access controls

- The ability of the user view and download the documents they have signed.

- The ability of administrators to manage user access to their team's templates and signed documents

- The ability for users to request the secure destruction of their customer data

Risk Management

The Company maintains a risk management framework to regularly analyze and manage risks to an acceptable level for the system environment and effectiveness of controls. The risk management framework is part of the Dropbox Sign Trust Program and is in conformity with the ISO/IEC 27001:2013 and ISO/IEC 27018:2019 standards.

The Company's Governance, Risk and Compliance Team assesses risks that may affect the control environment or the systems at least annually. This includes evaluating dynamic technical and environmental risks, threats from users and third parties, potential impacts to business continuity, and assessing relevant laws, regulations, and contractual requirements. The Governance, Risk and Compliance Team then analyzes those risks in consideration of their associated existing controls, likelihood of occurrence, and impact to the security, availability, and confidentiality of the system.

The Company's Insurance Team transfers risk by obtaining and maintaining cybersecurity insurance as a way to mitigate financial impact risk and renews the insurance on an annual basis. If the risks are still at an unacceptable level, the Team documents additional mitigation tasks, and then predicts the likelihood and impact of the risks after the implementation of the mitigation plan.

The risk and business impact analyses and resulting conclusions are documented and retained for future reference. The Company has developed a risk and business impact analysis process to ensure all applicable risks are identified, addressed, and monitored to ensure protection of information assets.

The Company's Security Team identifies individuals who are accountable and responsible for monitoring the effectiveness of controls during the risk and business impact analysis procedures.

Monitoring and System Operations

The system utilizes various automated and manual systems such as traffic analysis systems; performance and health systems; and security event monitoring systems to monitor the security and availability service commitments and system requirements, as well as general performance of the system. The system and supporting infrastructure are monitored for security events/incidents, system availability, and other metrics. The organization utilizes a security event response platform to ensure that operational and security alerts, which are categorized by priority or when certain predefined thresholds are exceeded, are routed to appropriate individuals.

The Dropbox IT Team uses malware protection software to protect Dropbox laptops and desktops with Mac and Windows operating systems from malware. The team configures the malware protection software to automatically receive updates to identify and stop malicious software. The malware protection software is installed on machines assigned to Dropbox personnel during the initial machine configuration process. Those machines are configured with a baseline image, which includes malware protection software. As defined in Dropbox's documented information security policies, the removal or bypass of system security features (which applies to malware) is not allowed. All machines are configured to either block uninstallation of the malware protection software (PC) or automatically reinstall the malware protection software if an uninstallation is detected (Mac).

Multiple monitoring and reporting mechanisms are in place. The Engineering and Security teams use various enterprise monitoring applications to provide monitoring and alerting functionality of the production environment. Availability and capacity are also continuously monitored through tools provided by AWS, as well as proprietary solutions. Event notifications are configured to notify Engineering personnel when predefined thresholds are exceeded.

As part of its security program, the organization monitors its systems for potential malicious activity. Monthly vulnerability scans are performed on the system environment for potential vulnerabilities and high priority findings are documented and tracked to resolution.

The organization also contracts with an independent third-party provider to perform a penetration test of the system at least annually. The Security Team reviews the results of the penetration test and prioritizes tracking high priority findings to resolution.

Incident Management

Dropbox provides a mechanism for reporting suspected or observed security, availability, processing integrity, confidentiality, or privacy incidents or weaknesses for its employees and contractors. Employees and contractors are required to report security and confidentiality incidents per their acceptance of the Information Security Policy. Dropbox has established incident response procedures. These procedures are followed when a security, availability, processing integrity, confidentiality, or privacy incident is reported and determined to be valid. The Dropbox Engineering Team receives alerts about large scale events, such as service outages or data integrity issues, from its managed services provider. The team acknowledges these alerts in a timely manner and responds to them as necessary. The Dropbox Engineering Team or Security Team (depending on the type of incident) assigns a severity level to the incident based on pre- defined criteria and initiates the procedures with an email announcement and ticket assigned to the impacted Team. An on-call Incident Manager and Technical Lead coordinate the response procedures. Escalation procedures are in-place in the event such an escalation is required. Dropbox Security Team performs an exercise to test the effectiveness of the incident response process on an annual basis. A ticket is filed to the Offensive Security Team to conduct a penetration exercise without the knowledge of the Detection and Response Team. The Detection and Response Team responds to the intrusion accordingly and documents and tracks relevant findings identified until resolution.

A post-mortem review of each significant severity incident is completed to review the root cause and other contributing factors, and to determine steps (including system changes, as necessary) to prevent, detect, and minimize the risk of future incidents.

The Dropbox Legal Team maintains appropriate contacts with relevant authorities (e.g., regulators, law enforcement, government officials) and evaluates that list on a regular basis. Dropbox may contact the relevant authorities in the event of certain types of incidents, as deemed necessary by the Legal Team and the Trust Management Team.

Additionally, Dropbox maintains a whistleblower hotline for employees and contractors with access to systems to communicate concerns and violations of the Dropbox Worldwide Code of Conduct or any other ethical concerns. Any violations to the Dropbox Worldwide Code of Conduct are appropriately handled, which may include disciplinary action, up to and including termination of employment or any other working relationship with Dropbox.

Confidentiality

Dropbox Sign, Dropbox Fax, and Dropbox Forms are designed to maintain confidentiality of the customer data stored and shared using the services. Customer data is only accessible to individuals whom the owner (end-user) designates and the team's Dropbox Sign, Dropbox Fax, or Dropbox Forms administrator. Access to customer data can be restricted by limited access to members of the team the user belongs to or by limiting access to users who have been explicitly invited to the workflow containing the customer data, as well as their Dropbox Sign, Dropbox Fax, or Dropbox Forms administrators.

The Company has established a User Data Privacy Policy specifically addressing the limited conditions and access procedures internal personnel must follow prior to accessing customer data.

The Company requires employees and contractors with access to systems to sign a confidentiality agreement and acknowledge Dropbox security policies as part of the onboarding process. Security policies (and changes therein) are available on the corporate Intranet.

The Company security, confidentiality, and privacy requirements and commitments are communicated to third parties through the initial contractual agreement, amendments, and renewals, when appropriate. The Company also requires a confidentiality agreement be put in-place before it shares confidential information with third parties which receive customer data.

Availability

System infrastructure is designed for resiliency to reduce the impact of an outage. The production databases run on the MySQL database engine and are configured to replicate to a different availability zone within the same region. Data related to the system is backed up daily and the Engineering Team is notified in the event of backup failure. Engineering personnel resolve data backup issues as needed. Application servers running within a region are distributed over multiple availability zones to provide redundancy. Customer data is stored in AWS S3 buckets which are located in the AWS us-east-1 region and replicate to the AWS us-west-2 region for backup and recovery purposes.

The organization has established a Disaster Recovery plan to help ensure system availability and recovery. Disaster Recovery plans are followed when an incident has been assessed and declared a disaster by the head of Dropbox Sign Engineering or designee. Communication procedures in the event of a disaster are outlined in relevant Disaster Recovery policies and procedures. The Disaster Recovery plan is reviewed and tested annually by the Security Team. The results of these tests, including lessons learned and action items, are documented and the team follows up to fix any issues found and update the plan, as needed. The Engineering Team performs backup restoration tests as part of the annual Disaster Recovery testing process.

An external website maintained by Dropbox Sign communicates the current status of the Dropbox Sign, Dropbox Fax, and Dropbox Forms services to users and provides a record of past service disruptions and maintenance at https://status.hellosign.com/.

Disaster Recovery

Dropbox Sign has established a Disaster Recovery plan to help ensure system availability and recovery. Disaster Recovery plans are followed when an incident has been assessed and declared a disaster by the head of Dropbox Sign Engineering or designee. Communication procedures in the event of a disaster are outlined in relevant Disaster Recovery policies and procedures. The Disaster Recovery plan is reviewed and tested annually by the Security Team. The results of these tests, including lessons learned and action items, are documented and the team follows up to fix any issues found and update the plan, as needed. The Engineering Team performs backup restoration tests as part of the annual Disaster Recovery testing process.

Business Continuity

As part of the Dropbox Trust Program, Dropbox maintains a Business Continuity Program and Business Continuity & Emergency Management Policy based on the ISO 22301:2019 international business continuity standard. The Business Continuity Program and Business Continuity & Emergency Management Policy define the purpose, scope, commitment to satisfy applicable requirements, and commitment to continual improvement.

The program and policies assign ownership, roles and responsibilities, and lines of communication, detail the recovery procedures and work-arounds, and describe the method for business continuity plan invocation. The Business Continuity & Emergency Management Policy also outlines processes for handling extraordinary events that may disrupt operations or threaten strategic objectives.

Dropbox conducts a business impact analysis (BIA) for business processes at least once a year or if there are any major changes, such as the addition of a new significant business process or new critical location, to the business environment. The BIA analyzes processes that are critical to Dropbox and the effect a business disruption might have upon them, sets time frames for recovery, and finds key dependencies, partners, and suppliers.

Dropbox maintains Business Continuity Plans for each team associated with business-critical functions. Business Continuity Teams review these plans at least annually. The business continuity plans establish an incident command structure, orders of succession, response and recovery of critical processes, workaround procedures, devolution, and reconstitution planning. Teams with critical processes test their BCPs at least annually and the relevant findings are documented in a post mortem with an associated improvement plan that is tracked until resolution. In addition, Dropbox conducts evaluations of the business continuity capabilities of its business-critical suppliers at least once a year.

Data

The following table describes the information used and supported by the system:

Data Used and Supported by the System

Data Description	Data Reporting
Customer Data	The customer defines and controls the data they load and store in the system. This data is loaded into the environment and accessed remotely from customer systems through the Internet.
Files	The system accepts multiple file types and converts them to PDF as a part of the signing process. As a final result of the signing process a PDF is produced. This PDF is made available via the UI, API, and e-mail delivery mechanisms.
Customer Credentials	The system also stores credentials, which are used to authenticate system users.

Complementary Controls at User Entities

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

Complementary Subservice Organization Control (CSOC) Considerations

Components of the production system are hosted in a third party managed service provider (Amazon Web Services (AWS)).

AWS owns and operates Logical Security, Change Management, and Physical Security controls required to maintain the environments hosting the Dropbox services. Controls at AWS are not included in the scope of this report.

The affected criteria are included below along with the expected minimum controls in place.

Criteria	Controls expected to be in place at third party (AWS)
CC6.2: 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.	IT access above least privileged, including administrator access, is approved by appropriate personnel prior to access provisioning. IT access privileges are reviewed on a quarterly basis by appropriate personnel. User access to systems is revoked in a timely manner upon termination.
CC6.4: 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.	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware such as firewalls and routers, is restricted to authorized individuals through a badge access system or equivalent, and is monitored by video surveillance. Requests for physical access privileges to the entity's computer facilities require management approval. Documented procedures exist for the identification and escalation of potential physical security breaches. Visitors must be signed in by an authorized workforce member before gaining entry and must be escorted at all times.
CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Changes are authorized, tested, and approved prior to implementation.
A1.1**:** 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.	Processing capacity is monitoring and maintained on an ongoing basis.
A1.2: 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.	Environmental protections have been installed including the following: • Cooling systems • Battery and generator backups • Fire detection and suppression mechanisms • Environmental protection equipment receive maintenance on at least an annual basis.