WHITE PAPER

Adobe Vendor Security Review Program

April 2025

Adobe

Table of contents

Overview

The Adobe Vendor Security Review (VSR) program evaluates third-party vendors' compliance to Adobe's established Vendor Information Security Standard and provides a risk-based review of each vendor's security practices, enabling Adobe business owners to make fact-based and risk-informed decisions about selecting a vendor. Managed by the Adobe Security team, the VSR program includes a set of requirements to which third-party vendors must adhere if they collect, store, process, transmit, access, or dispose of Adobe data or otherwise engage with Adobe's network and systems.

The VSR program is a logical extension of Adobe's belief that every action or interaction with the company's products, data, and ecosystem should be conducted with a lens of security, which is one of the key controls within the Adobe Common Controls Framework (CCF). Through the VSR program, Adobe extends its culture of security to any vendor with which the company does business.

All vendor engagements must be reviewed and approved by Adobe's procurement, information security, and legal teams prior to allowing any third party to interact with Adobe's data, products, and environment.

Adobe Vendor Security Review Program Process

When a business owner wishes to engage a third-party vendor, they initiate the vendor onboarding process, which triggers a VSR request. The first step in this process requires the business owner to identify the information handled by each vendor. Any Adobe business owner who wants to onboard a new third-party vendor must also clarify the specific use case for which Adobe is engaging the vendor and how the vendor will interact with the Adobe ecosystem. This clarification includes specifying the data that the vendor will process, store, or engage with on Adobe's behalf.

Vendor Security Review

Based on the information provided by the business owner, Adobe sends a detailed questionnaire to the vendor's main point of contact, which includes questions from each security control area (see the VSR Security Controls Assessment section below). After the vendor completes and returns the questionnaire, Adobe Security analysts review the information and, based on the vendor's responses, evaluate the risk to Adobe in engaging with the vendor. During a vendor security review, Adobe considers the following factors:

- **Inherent risk:** Based on the vendor's use case, the classification of Adobe data with which the vendor engages and how they engage with it (e.g., collect, store, process, transmit, access, or dispose), Adobe determines a baseline risk level.

- **Vendor security posture:** Based on the service being procured, Adobe evaluates the vendor's applicable security controls against Adobe security standards as well as industry best practices, which helps determine if the vendor is equipped to securely provide the required services.

- **Residual risk:** Finally, Adobe assigns a risk level — low, medium, or high — to the vendor based on the inherent risk and the vendor's security controls.

Vendors assessed as low risk proceed through the remainder of the vendor onboarding process. If Adobe conducts the review as part of a vendor reassessment, the vendor remains on the approved vendor list.

If Adobe finds any deviations from Adobe security standards, a risk analyst discusses the gaps and suggests potential remediations and/or mitigations to the business owner. The analyst then documents the recommendations as well as to whom they are assigned: the vendor or the business owner.

Adobe requires vendors assessed as medium or high risk by the VSR process to remediate or mitigate the identified risks. Once Adobe management agrees to the residual risk level, the vendor can proceed with the onboarding process. However, if the residual risk level is beyond Adobe's acceptable threshold, Adobe Security can disapprove procurement of or continuation with the vendor's products or services.

Vendor Security Monitoring

The VSR program monitors vendors for any security risks throughout the vendor's relationship with Adobe, which includes:

- **Periodic reviews:** Based on their inherent and residual risk scores, Adobe periodically reassesses vendors every one to three years. This reassessment includes reviewing the types of data that vendors may engage with, applicable security controls, changes to infrastructure or application(s) since the last review, and gaps identified and/or remediations required in the last review. If there are material changes to the types of data the vendor engages with, or the activities they conduct on Adobe's behalf, or questions arise regarding how the vendor manages Adobe's data prior to the required review cadence (e.g., product change, audit, or other inquiry), Adobe may also conduct a VSR review at that time on an as-needed basis.

- **Threat intelligence loop:** Adobe monitors third-party vendors for real-time security threats and risks to their external landscape using a third-party security intelligence platform. Such continuous monitoring provides Adobe Security more visibility into a vendor's risk profile and enables the vendor to address those risks between review cycles.

Vendor Security Controls Assessment

Adobe expects vendors to comply with Adobe security and privacy standards to help protect the security of Adobe's data and network. The Vendor Security Review program assesses the following security controls, as applicable, when conducting vendor reviews and reassessments:

- **Security certifications and attestations**, including SOC 2 Type II, ISO 27001, and PCI DSS
- **Information security policies and program**, including internal security policies and standards or evidence of a security program
- **User authentication and access control**, such as password policies, access control processes, and support for multi-factor authentication (MFA)
- **Logging and auditing**, including system, application, and network logs and retention periods
- **Data center security**, including the physical security controls for locations in which the vendor hosts Adobe data
- **Vulnerability and patch management**, including the cadence of external and internal vulnerability assessments and penetration tests, as well as timelines for vulnerability remediation
- **Device posture and endpoint security**, including policies that cover device and endpoint security
- **Data encryption**, including data at rest and in transit
- **Data backup and recovery**, including the frequency of backups, encryption algorithms, and review of disaster recovery (DR) plans
- **Breach notification**, including compliance with Adobe's breach notification requirement
- **Service provider access**, including policies that address the security of the vendor's third-party providers, such as data center and cloud service providers
- **Application security**, including secure coding practices, avoidance of the OWASP Top 10 vulnerabilities, and implementation of employee security training
- **Artificial intelligence**, including implementation of AI/ML and generative AI security best practices and threat considerations, if applicable
- **Network security**, including security controls in the network layer, such as network segmentation and firewalls

- **Service decommissioning**, including data destruction after service termination
- **PCI compliance**, including how and where the vendor processes credit card information, if applicable
- **User-generated content**, including storage location and virus and malware scanning of uploaded content

Adobe Vendor Policies, Standards, and Assessments

Vendor Risk Management Policy

Third-party risks at Adobe are managed by the Adobe Vendor Risk Management Organization (VRMO). The VRMO partners with various groups within Adobe, including but not limited to procurement, legal, business resilience, information security, privacy, ethics, and compliance, to implement a global and effective enterprise-wide vendor risk management ecosystem.

Vendor Information Security Standard

The Adobe Vendor Information Security Standard establishes the responsibilities and security requirements regarding vendor engagements and applies to all vendors that interact with Adobe employee or customer data, Adobe products, and the wider Adobe ecosystem. In addition to clarifying the process of vendor compliance with Adobe's information security requirements, ethe standard also elucidates expectations and requirements applicable to vendors that engage with more sensitive types of data for which Adobe has unique obligations, such as cardholder data or electronic protected health information (ePHI).

Privacy Assessment

Adobe requires a privacy assessment as part of the vendor onboarding process. If a vendor will be processing any form of personal information on behalf of Adobe, they must complete the VSR questionnaire and a privacy questionnaire.

The Adobe Privacy Office and Cybersecurity Legal team reviews the privacy questionnaire and other applicable materials and responses to determine if privacy issues exist with the vendor and what privacy and security terms (described in the following section) are required for inclusion in the vendor contract.

Vendor Legal Obligations

To ensure ongoing compliance with the Adobe Vendor Information Security Standard, all third-party vendors must sign a security addendum as part of the contract negotiations during the onboarding process. Adobe reviews these terms annually at contract renewal.

Vendor Data Processing and Transfer Agreement

Adobe requires any vendor that engages with Adobe data to sign a vendor data processing and transfer agreement (VDPTA), which is a written contract between Adobe and the vendor that documents:

- **Processing:** Both parties' obligations with respect to accessing, collecting, processing, transmitting, sharing, and storing personal information.
- **Transferring:** Cross-border data transfer requirements, where applicable, within the scope of services as described in the vendor's master agreement with Adobe.
- **Securing:** Technical and organizational controls to be implemented and maintained by the vendor.

Upon signing the VDPTA or a similar contract document detailing applicable privacy and security obligations, the vendor must adhere to all requirements stated in that document, including:

- **Security:** Contains provisions that describe the minimum security requirements with which a vendor must comply when handling Adobe information, including when and how a vendor must notify Adobe of a security incident involving access controls, security assessments, logging requirements, and processing data subject requests.
- **Privacy:** Documents both parties' obligations under applicable data protection laws, including GDPR. More specifically:
    - **Processing:** A vendor may only process or store personal information necessary to perform its obligations under the vendor's Master Agreement, as per written instructions from Adobe and in compliance with all applicable laws.
    - **Transferring:** A vendor accessing or storing any personal information from outside the originating country (i.e., cross-border transfer) may be required to have a data transfer mechanism, depending on the country of origin.
- **Ethical Behavior:** Provides guidelines by which vendors must adhere to Adobe's business code of conduct, helping ensure strong anti-corruption and anti-bribery best practices. Vendors' codes of conduct are reviewed as part of the onboarding process to help ensure they meet Adobe's published code of conduct standards.

Questions?

For more information about Adobe's operational, application, and enterprise security processes, compliance certifications, incident response program, security training and awareness program, and business continuity and disaster recovery program, please see the Adobe Trust Center.