WHITE PAPER

Adobe Business Continuity and Disaster Recovery Program

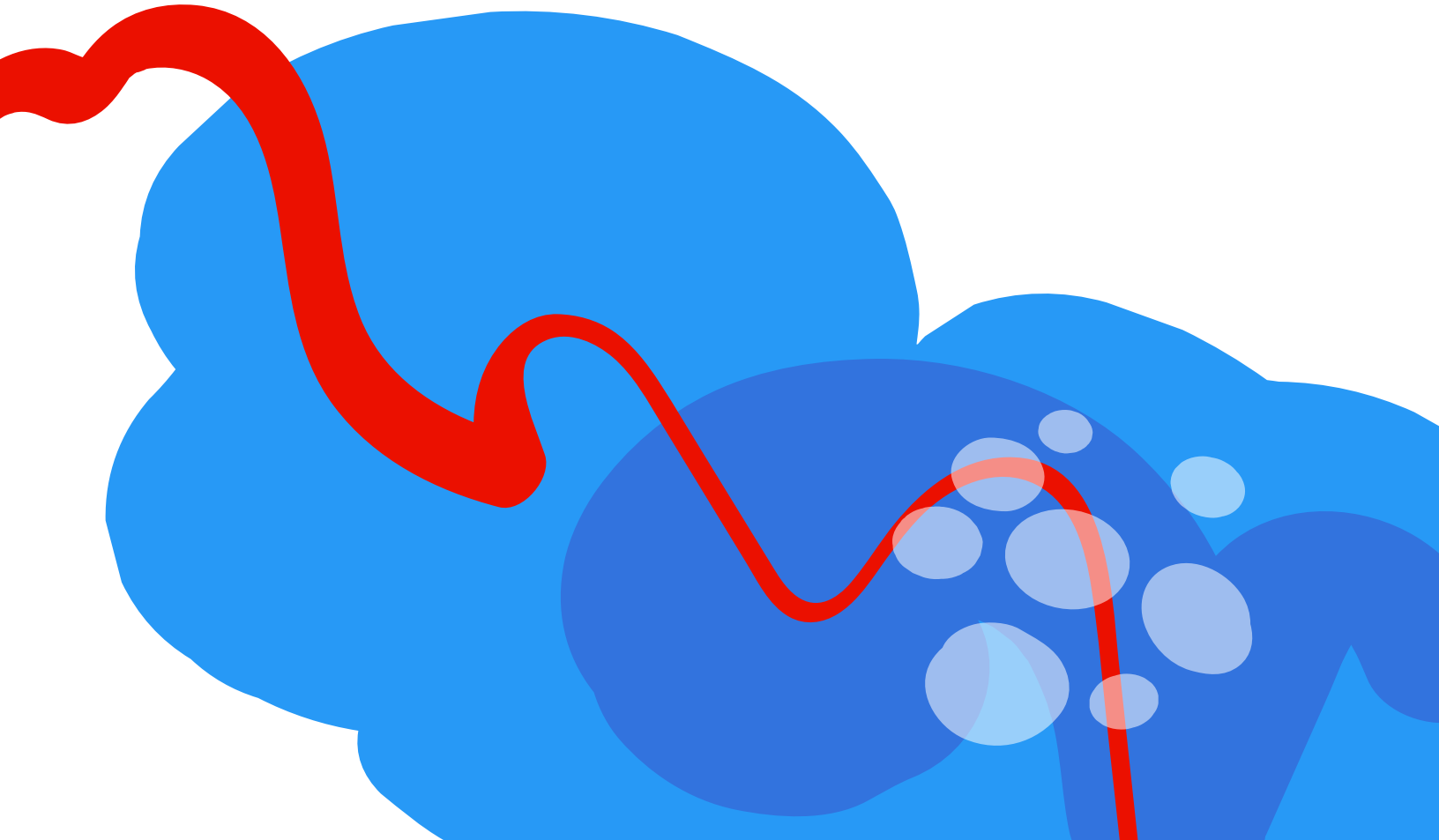
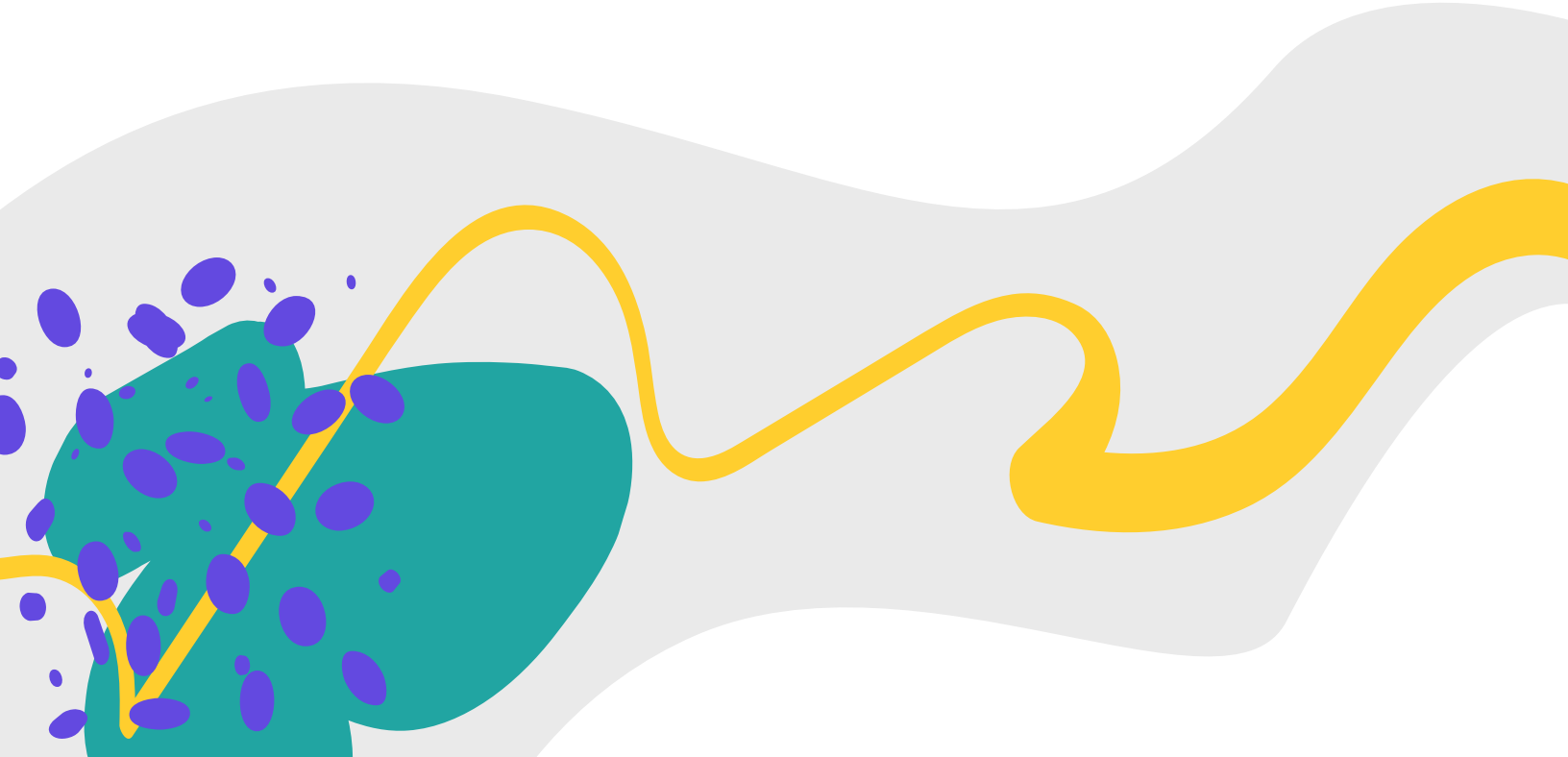


Table of Contents



Introduction

Adobe is committed to helping ensure the continued availability and delivery of our products and services for our customers. To that end, Adobe deploys and supports a comprehensive, ISO 22301-certified business continuity and disaster recovery (BCDR) program that enhances our ability to respond to, mitigate, and recover from the impacts of unexpected disruptions.

Using our open-source Common Controls Framework (CCF) to guide decisions, Adobe drives resilience requirements across the organization and enables the continued certification of our products and services against international standards (e.g., ISO 22301, SOC 2, ISO 27001).

The Adobe BCDR Program is composed of the Adobe Corporate Business Continuity Plan (BCP) and product-specific Disaster Recovery (DR) Plans, both of which are detailed below.

Adobe Corporate Business Continuity Plan

The Adobe Corporate Business Continuity Plan provides a framework to help enable response, stabilization, and recovery from catastrophic events that disrupt operations of the company's critical business processes and technologies. This plan includes all Adobe products and services. In the event of a disruption to personnel or facilities, a core evaluation and response team convenes to discuss business impact and determine next steps. If required, Adobe activates the BCP and uses well-defined and tested recovery strategies to help mitigate the disruption and to recover within timeframes that support our recovery objectives and service-level agreements.

Any member of the core evaluation and response team may activate the BCP. Once activated, the office of the CSO communicates the activation to leadership, management, and relevant product and service teams and begins the required documentation and event monitoring efforts. In the event of a business interruption or disaster, the CSO's office is also responsible for ensuring the safety of personnel, stabilizing the situation, reducing the impact to the Adobe business and customers, and overseeing emergency response and recovery activities.

The Adobe BCP is tested on an annual basis, with the most recent test completed on August 31, 2021. The test met all BCP objectives and identified no plan deficiencies. The annual BCP test includes training for key staff in the BCP processes.

Adobe Crisis Management Program

Adobe has a proven, scalable, and consistent Crisis Management Program (CMP), which covers overall management of any crisis faced by the company, whether large or small. Including an effective and responsive global and regional crisis management and risk mitigation process that protects employees, information, critical infrastructure, and business functions, the Adobe CMP was most recently exercised in March 2020 in response to the COVID-19 pandemic.

Disaster Recovery and Resilience Plans

Adobe designs and builds its cloud-based offerings with a focus on high-availability and resilience, using an always-on, redundant architecture. Delivering services this way allows Adobe to establish our SLAs for uptime, which is the relevant measure for providing modern software services. The recovery time objectives (RTO) and recovery point objectives (RPO) identified in our disaster recovery plans do not holistically represent the end-to-end resilience built into our products. For example, a disaster recovery plan may focus on rebuilding an impacted resource while the high-availability architecture would quickly shift traffic to unimpacted resources and reduce the likelihood of impact to the customer. To learn more about Adobe SLAs, please visit: https://www.adobe.com/legal/service-commitments.html

The two core processes involved in maintaining a recoverable operational environment are backup and redundancy. Adobe product and service teams are responsible for evaluating their specific technical architecture and processing capabilities to determine the appropriate strategy in order to meet the requirements of the Adobe BCDR Program.

This process includes conducting a comprehensive Business Impact Analysis (BIA) that identifies the Critical Business Functions (CBFs) for the product or service that must be covered by the DR plan.

Each Adobe product- or service-specific disaster recovery plan includes:

- Critical Business Functions requiring restoration
- Procedures for recovering the critical business functions
- Recovery time and recovery point objectives (RTO and RPO)
- Dependencies
- Key personnel required

- External services required to support the critical business function
- Established priorities for restoring critical business functions and data in accordance with recovery objectives
- Access and availability to vital records

Disaster recovery plans are updated at least annually or as required by changes in the operating environment. For security reasons, Adobe does not share our DR plans externally.

Annual Testing Procedure

In addition to updating the DR plans, each product and service team at Adobe performs an annual disaster recovery and data restoration test. These tests exercise the documented steps in their DR plan, determine whether the plan meets RTO and RPO expectations, and help ensure personnel knowledge of the recovery process.

When performing the annual DR testing, teams must execute the test without causing any material impact to the Adobe production environment or customer experience. The test must conduct a recovery against a clean, newly provisioned asset, making sure the test performs all steps in the associated DR plan. At the conclusion of each test, teams must document the test's outcome, indicate whether the test met RTO and RPO goals, and outline applicable DRP updates. All completed test results are documented, reviewed and approved by the product or service team and retained as records in a central repository.

If the test did not meet RTO or RPO expectations, the product or service team is responsible for investigating the root cause and implementing a resolution.

Continuity Event Process

Adobe product and service teams coordinate with the Adobe Global Operations Center (GOC) to monitor the availability of their production systems. If a critical business function becomes unavailable, the GOC declares an outage and sends a notification to the appropriate incident response team members to assist with the investigation and validate the scope. The product or service team works with the GOC and other response teams and vendors as required to remediate the issue.

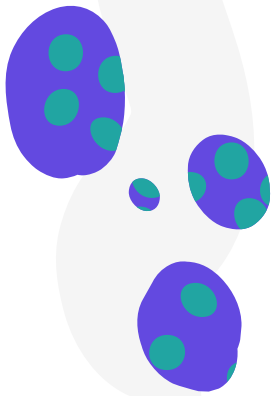
In the event of a customer-impacting problem or continuity event, Adobe notifies affected customers of the outage and provides updates on status.adobe.com. If necessary, the proper authorities (e.g., fire, police, medical) are also notified.

Third-party Products and Services

Third-party products or services deployed in the Adobe infrastructure that process (i.e., collect, transmit, or store) Adobe or its customers' data are reviewed through the Adobe Vendor Security Review Program. Adobe reviews vendors against our baseline security requirements for encryption, user authentication, administrative access, vulnerability resolution, patch management, logging and monitoring, backup and recovery, breach notifications, data center security, network security, endpoint security, application security, and service provider management. You can find more information in the Adobe Vendor Security Review Program white paper.

Conclusion

Adobe is committed to the availability and resilience of our infrastructure and our product and service offerings, as demonstrated by our ISO 22301-certified BCDR program, which helps enable us to respond to, mitigate, and recover from the impact of unexpected disruptions. For more information about the Adobe BCDR Program, or for specific information about an Adobe product or service, please contact your Adobe account manager or visit the Adobe Trust Center.



Information in this document is subject to change without notice. For more information on Adobe solutions and controls, please contact your Adobe sales representative.

www.adobe.com

Adobe