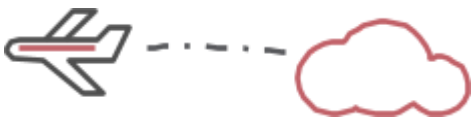
Business Continuity Plan

Last revision date: 08/30/2023



Confidentiality

This document contains confidential Zuora information. This document is intended solely for use by internal Zuora personnel, Zuora business partners, Zuora customers, and Zuora prospective customers that have completed a non-disclosure agreement with Zuora.

Unauthorized use, reproduction, or distributions of this document, in whole or in part, is strictly prohibited.

Disclaimer

The information contained herein is believed to be accurate at the time of issue; no liability can be accepted for any inaccuracies. The reader is reminded that changes may have taken place since the issue.

ZUORA BUSINESS CONTINUITY PLAN

LAST REVIEW AND OR UPDATE DATE: 06/30/2022

TABLE OF CONTENTS

1. Overview

Zuora is responsible for the management and maintenance of business continuity services and associated resources to provide for restoration of services, processes, and technology used to provide the Zuora Platform to customers within the timeframe specified in Zuora's service level agreement (SLA). Zuora's SLA is consistent with SLAs of other SaaS providers engaged in business similar to Zuora's business. The process described below is applicable to all Zuora services, unless otherwise noted.

Zuora provides planning and implementation of contingency and disaster recovery processes to meet our organizational and customer's requirements for business continuity. These plans include, but are not limited to, identification of mission-critical applications, risk assessment, emergency procedures, restoration of facilities, and contingency procedures and operations. These plans are consistent with other Zuora policies and procedures.

Zuora will work with Third-Party Suppliers providing materially related services, processes, and technology that Zuora deems mission critical to provide Services to Zuora customers. These services include application services, data center services, and network management services.

Zuora will conduct periodic business continuity tests with respect to the services, processes, and technology used to provide services to Zuora's customers. Zuora plans include data back-up frequency and disaster simulations with commitments to retest within 90 days if any disaster simulation fails to achieve expected results. Zuora will document the results of all business continuity testing. Additionally, Zuora will make updates to the business continuity plan on an as needed basis and will review the plan at least annually.

Zuora's responsibilities to provide business continuity services to customers include the following:

1. With respect to the Services located at Zuora's primary data center, Zuora shall maintain backup databases replicated to a remote site at all times.
2. Zuora's backup facility shall maintain equivalent physical security controls as Zuora's primary data center.
3. Zuora will monitor backup databases using equivalent monitoring controls as the primary databases to verify that such backups are operating effectively.
4. In the event of a disaster, Zuora will perform restoration activities to restore the services, processes, and technology so that customers can continue to use the Services in a manner consistent with how they used the Services prior to the disaster.
5. Determine what business continuity resources to deploy in the event of a disaster, and conduct, supervise, and administer the operation and implementation of such resources.
6. Provide additional resources as necessary to maintain the provision of services, processes and technology used to provide the Services.
7. Adjust the business continuity program as necessary, to accommodate changes in Zuora's business volumes, application enhancements, business and operational needs, or new functions.

Zuora will provide crisis management including, but not limited to, declaration of crisis, crisis monitoring, escalation, and conducting post-mortem. Zuora is responsible for ensuring that all business continuity program documentation is updated pursuant to any modification of policy, procedure, software, or hardware infrastructure, or supporting components or

services by Zuora insofar as such modification relates to the services, processes or technology used to provide the Services to Zuora's customers.

Zuora's corporate systems are exclusively software-as-a-service (SaaS) applications and do not reside in any of Zuora's offices. This allows personnel to perform their job function from any location they desire and operate "around the clock" (24x7x365). Due to the nature of Zuora's SaaS application strategy, the primary risk to the organization is not the ability to access systems in the event of an interruption at a Zuora office, but instead coordinating with employees during an event and ensuring that the applications in use at Zuora will be available during such an event.

This plan was developed to meet or exceed the specified HIPAA performance criteria for recovering data from emergency or disastrous events.

2. Objectives

This plan is designed to meet the following objectives:

- Serves as a guide for the Zuora's recovery teams.
- References and points to the location of critical data.
- Provides procedures and resources needed to assist in recovery.
- Identifies vendors and customers that must be notified in the event of a disaster.
- Assists in avoiding confusion experienced during a crisis by documenting, testing, and reviewing recovery procedures.
- Identifies alternate sources for supplies, resources, and locations.
- Documents storage, safeguarding and retrieval procedures for vital records.
- Address the risks to the organization in the event that a disaster (earthquake, fire, power outage, pandemic, etc.) would impact the ability of the organization to service existing customers.

3. Recovery strategies

Each team should take into consideration the tasks that must be performed to recover their business unit to normal or acceptable operations after an event. Each team should consider what the team will do in case of:

- An event affecting IT systems and/or telecommunication service; and/or
- An event affecting access to the work area; and/or,
- A sudden reduction in employee availability.

Recovery strategies will be based on the type of event and available resources:

- Short-term interruption: Temporary interruption with little or no damage to the business unit's work area, IT environment, or the business unit's staff levels; or,
- Long-term interruption: Physical damage to critical equipment, property, and/or a significant impact on the business unit's workforce

3.1 Short Term Strategies

Short term strategies will likely identify manual processing procedures that may be implemented following a short-term telecommunications or computer service outage.

These strategies may also be used to reduce business impacts following a crisis event, until more time-consuming recovery strategies can be implemented. Non-essential or non-critical functions may be suspended. Procedures may consist of manually logging client/customer requests, and use of home offices, as available. Critical functions may be completed using alternate means.

3.2 Long Term Strategies

Long term strategies and procedures are based upon a crisis scenario, such as total destruction or loss of the facility and/or workforce, resulting in an extended business interruption. These strategies address business recovery at an alternate site utilizing resources and/or securing third party vendors to help perform critical functions.

4. Procedures to Maintain Operational Continuity

4.1 Personnel Measures in Place

Zuora's respective business areas have established chains of command in place for assigning responsibilities regarding tasks for the Business Continuity Plan and for the escalation of items as needed. Additionally, personnel receive training of others' responsibilities in order to perform tasks associated with Business Continuity Plan in case certain employees are unavailable for any reason. In the case where certain skills and/or knowledge is lost, outside resources will be acquired to assist until full time personnel are trained or hired in those areas.

4.2 Technical Operations Measures in Place

Zuora's Technical Operations team is geographically dispersed with the majority of personnel located in Redwood City, California; Beijing, China; Chennai, India; and San Jose, Costa Rica. Technical Operations on-call personnel provide coverage 24 hours a day, 7 days a week, and 365 days a year. In the event that a disaster at any location was to occur, and personnel cannot respond to system events, the other operations team would be automatically notified with existing system monitoring tools to respond to the event. Each operation team is capable of covering the operations of Zuora for an indefinite period of time if required to, due to a disaster.

In the event that a disaster occurs Technical Operations management has a call tree with phone numbers and email addresses and will instruct personnel on where to work. Operations personnel have laptops and cell phones that allow them to work from any location that has an Internet connection.

In addition to remote teams, Zuora has virtual meeting or war rooms that are available using Slack to meet and respond to events regardless of geographic location. Slack is a SaaS application and can be accessed from anywhere. If there is an issue that arises with Slack, Zuora's backup communication tool is gchat (Google chat).

The general recovery strategies that will be implemented is to resume Technical Operations processing for Zuora is as follows:

Strategy	Technical Operations

Immediate	Immediate strategies address tasks that should be performed as soon as possible following an event, in order to reduce possible impacts. In some instances, this may include initial external communications to customers.
Short Term	• Wherever possible, suspend non-essential activity requiring IT systems. • Make work schedule adjustments, as needed. • Prioritize essential departmental activities. • Work remotely from home, as appropriate. • If unable to gain access remotely, begin manual processing; retain all documentation and enter when IT systems are available. • When access to systems is restored, update records to reflect any manual or alternative activities.
Long Term	• If unable to gain access remotely, continue manual processing; retain all documentation and enter when IT systems are available. • When access to systems is restored, resume activities according to priorities schedule. • Once system access is available, relocate to recovery location and resume activities according to priorities schedule. • Refine and prioritize actions to sustain critical business processes in the face of reduced staffing levels. • When the workforce is back to full capacity, re-evaluate status of each project and re-prioritize, as needed. • Ensure employees have the necessary equipment in place to work remotely (laptops, printers, VPN access, etc.). • Update records to reflect any manual or alternative activities.

4.3 Support Measures in Place

Zuora's Support team is geographically dispersed with personnel located in Redwood City, California; London, England; Chennai, India; and Beijing, China. Support personnel work around the clock in shifts and provide coverage 24 hours a day, 7 days a week, and 365 days a year. In the event that a disaster at any location was to occur and personnel cannot respond to customer support requests, the other support teams would be notified to respond to support requests. Remaining locations have the resources, tools, and training in place to meet documented service level agreements provided to Zuora customers.

In the event that a disaster occurs, Support management has a call tree with phone numbers and email addresses and will instruct personnel on where to work. A remote office facility is in place for Support personnel to meet and perform their job should Zuora's offices be inaccessible. Support personnel have laptops that allow them to work from any location that has an internet connection.

In addition to remote teams, Zuora has virtual meeting or war rooms that are available using Slack to meet and respond to events regardless of geographic location. Slack is a SaaS application and can be accessed from anywhere.

The general recovery strategies that will be implemented is to resume support processing for Zuora is as follows:

Strategy	ational
Immediate	Immediate strategies address tasks that should be performed as soon as possible following an event, in order to reduce possible impacts. In some instances, this may include initial external communications to customers.
Short Term	• Determine work in progress and prioritize activities based on impending deadlines/ commitments. • Work remotely from home, as appropriate. • Defer non-essential activities, as needed. • Make work schedule adjustments, as needed. • Prioritize essential departmental activities. • Defer non-essential activities.
Long Term	• Determine work in progress and prioritize activities based on impending deadlines. • Leverage internal resources to assist in essential business processes, as needed. • Implement voluntary staffing changes, including enhanced workloads and alternative schedules. • Refine and prioritize actions to sustain critical business processes in the face of reduced staffing levels. • When the workforce is back to full capacity, re-evaluate status of each project and re-prioritize, as needed. • Ensure employees have the necessary equipment in place to work remotely (laptops, printers, VPN access, etc.). • Once system access is available, relocate to recovery location and resume activities according to priorities schedule.

4.4 Applications Business Impact Analysis

The purpose of the business impact analysis (BIA) is to identify which applications are essential to the survival of Zuora across all critical business areas. The BIA will identify how quickly essential applications have to return to full operation following a disaster situation. The BIA will also identify the resources required to resume business operations.

Business impacts are identified based on the worst-case Scenario that assumes that the physical infrastructure supporting each respective business unit has been destroyed and all records, equipment, etc. are not accessible for 30 days. Please note that the BIA will not address recovery solutions.

The objectives of the BIA are as follows:

- Impact Criteria: Zuora evaluated the impact in the following areas:
    - System Security (Confidentiality & Integrity)
    - Business Interruption (Availability)
    - Financial
    - Reputation & Image

- People
- Likelihood: The likelihood criteria allowed Zuora to evaluate the likelihood of the situation to occur.

Business Impact Analysis Scores

The following number scores have been established to provide firm tangible and intangible exposure categories for cross-company comparison. For the final Risk Rating, impact and likelihood scores were determined and combined for the final risk rating of that application.

Impact Scoring System

	Impact Criteria
5	Catastrophic
4	Major
3	Moderate
2	Minor
1	Insignificant

Likelihood Scoring System

	Likelihood Criteria
5	Almost Certain
4	Likely
3	Possible
2	Unlikely
1	Rare

Note: For additional details regarding the impact and likelihood scoring scale, refer to Zuora's Risk Assessment.

Application	Location	Risk Rating
ADManager	Cloud	Low
Adobe Apps	Cloud and Local Workstations	Low
ADP	Cloud	Medium
AlertLogic	Cloud	High
Ansible	Cloud (AWS)	High
Cisco AnyConnect (Production)	Cloud	High

Application	Location	Risk Rating
Authentication Servers Corporate	Redundant Infrastructure in and Singapore, San Jose Palo Alto, Paris	High
Authentication Servers Production	Redundant Infrastructure in AWS	High
Autonomous Digital Expression Manager - ADEM	Cloud	Low
Avalara	Cloud	High
AWS – Corporate & Production	Cloud (AWS – Multiple Availability Zones/Regions)	High
Axonius	Cloud	High
Box	Cloud (Box Data Center)	Low
BitSight	Cloud	Medium
Cloudforge	Cloud	High
Concur	Cloud (Concur Data Center)	Low
Confluence	Cloud (AWS - Oregon)	Low
Coupa	Cloud	Low
Digital Guardian	Cloud	Medium
DocuSign	Cloud	Low
Power BI	Cloud	Medium
ElasticSearch, Logstash, Kibana (ELK)	Cloud	High
E*Trade	Cloud	Low
Evernote	Cloud	Low
Fidelity	Cloud	Low
Thales/Gemalto (Safenet)	Cloud (AWS)	High
GitHub Enterprise	Cloud (AWS) and Github Cloud	High
GitLab	Cloud	High
Google Apps	Cloud (Google data center)	High
Grafana	Cloud	High
Greenhouse	Cloud	Low
ISE (Cisco)	On Prem	High
JAMF	Cloud (AWS)	Medium
Jenkins	Cloud	High
JetBrains	Individual	Medium
JIRA (Zuora)	Atlassian Cloud	Low

Application	Location	Risk Rating
Kaseya	Cloud	Medium
Achievers (KudoZ)	Cloud	Low
Kubernetes	Cloud	High
Lacework	Cloud	High
LucidCharts	Cloud	Medium
Lynda	Cloud	Low
Marketo	Cloud	Medium
Microsoft 365	Cloud	High
Mindtouch	Cloud (Mindtouch Data Center)	Medium
Navex	Cloud	Low
NetSuite	Cloud (NetSuite Data Center)	High
Okta	Cloud (Okta Data Center)	High
OpenDNS	Cloud	High
OSSEC	Local	High
Outreach	Cloud	Medium
Palo Alto Firewall	Cloud	High
PagerDuty (GS)	Cloud	Medium
PagerDuty (Engineering)	Cloud	Medium
Pingdom	Cloud	High
PlanSource	Cloud	Medium
PolicyTech	Cloud	Low
Prisma (PaloAlto Global Protect VPN)	Cloud	High
Production Hosting Services	AWS West, East, EU; Azure (West)	High
Puppet	Cloud	High
PurelyHR (Time Off Manager)	Cloud	Low
Rapid7	Cloud	High
LogicMonitor	AWS	High
Route53 (Production and Corp.)	Cloud (AWS)	High
Salesforce	Cloud (Salesforce DC)	High
Jira Service Management (JSM)	Cloud (Salesforce DC)	High
Saleshood	Cloud	Medium
SaltStack	Cloud (AWS)	High
SANS	Cloud	Low

Application	Location	Risk Rating
Shareworks (Soleum)	Cloud	Low
Slack	Cloud (Slack Data Center)	Medium
Slideshare	Cloud	Medium
SmartSheets	Cloud	Low
Spacewalk	Cloud	High
tCell	Cloud	High
Terraform	Cloud	High
ValiMail	Cloud	Low
Valtix	Cloud	High
Vidyard	Cloud	Low
Whitehat	Cloud	High
Wordpress	Cloud (AWS) and On Prem	High
Workday	Cloud	High
Xactly	Cloud	Medium
Zendesk (Support)	Cloud (Zendesk Data Center)	Medium
Zoom	Cloud	High
Zuora	Cloud (AWS US West, US East, & EU Central)	High

4.5 Key Contacts

In the event that the Business Continuity Plan is enacted, the below are key contacts for each critical department. These internal contacts can be contacted via the various methods supported by Zuora (including but not limited to: Slack, Google chat, email, and telephone).

Department	Primary	Surrogate(s)
Finance	Todd McElhatton	Matt Dobson
Security	Jayson Franklin (CISO)	Anu Veluri
Technical Operations	Venkat Venkataraman (VP Technical Operations)	Karunakaran Duraikannu
Engineering	Pete Hirsch (Chief Product & Engineering Officer)	Mu Yang
Legal	Andy Cohen (General Counsel)	Sylvia Lexington
IT	Karthik Chakkarapani (Chief Information Officer)	Mark Gill, Piyoush Sharma
Product	Pete Hirsch (Chief Product & Engineering Officer)	Karthik Ramamoorthy, Kyle Kolich, Shakir Karim

External contacts that support critical business application services and infrastructure services for Zuora are maintained and known by the respective departments that own the respective service. In the event that the Business Continuity Plan is enacted, the respective departments will reach out to these contacts if the particular service is impacted.

5. Testing and Validation

Testing is performed to ensure the business continuity plan is up to date and to ensure that Zuora and Zuora services can continue to operate as expected during the time when the business continuity plan is enacted. Zuora leverages lessons learned from testing the business continuity plan to update these policies and procedures so that continuity objectives can be met. Included within the annual test procedures, Zuora will perform the following:

1. On an annual basis, Zuora will have a member from the following teams work remotely for one day to ensure that they can still support the services of the organization:
    a. Technical Operations
    b. Security
    c. Engineering
    d. IT
    e. Global Support
    f. Global Services
    g. HR
    h. Finance
    i. Marketing
    j. Sales
2. Confirm with all individuals that they are able to perform their job functions to continue the operations of the organization.

Documentation will include an overview of the individuals who participated in the annual exercise, date of the exercise, and description of the findings.

6. Future Plans

Zuora is actively refining the Business Continuity Plan on an ongoing process by regularly reviewing, making updates to, and expanding it. The Business Continuity Plan will include formal training of employees on the continuity plan, mock exercises, and additional vendor scrutiny to evaluate the operation of critical applications in the event of a disaster.