INSTRUCTURE

BUSINESS CONTINUITY & DISASTER RECOVERY

Engineering, Security, and Operations

April 2023

Table of Contents

INSTRUCTURE

Introduction

Business Continuity

Every organization is subjected to a variety of risks while conducting business. These risks can take shape in the form of serious external threats such as cyber-terrorism or political upheaval to the less serious (yet still important) risks of retaining key personnel or even having to face an angry panda. But whatever the perceived risk, it is critical that an organization identifies, assesses and maintains a Business Continuity Plan (BCP) to prevent and recover from potential or real threats to its most valued assets. At Instructure, our robust risk management processes allow us to identify, assess, and treat these risks on an ongoing basis. To help strengthen our Business Continuity Plan, our Enterprise Risk Steering Committee, comprised of key leaders throughout Instructure, meets regularly and continually identifies and mitigates risks that might impact Instructure, its mission, and its most prized assets.

Naturally, at the heart of every business continuity program is a robust incident response plan—a plan that helps effectively guide an organization through incidents that may arise from time to time. At Instructure, we have a detailed, considered, and operational incident response plan which includes preparing for, detecting, assessing, escalating, responding to, communicating the impacts of, and learning from security, availability, privacy, human resources, finance, and other unforeseen incidents (read: angry panda). The incident response plan is the starting point for all incidents, and can easily escalate—depending on the type and severity of the incident—into a variety of other Instructure plans, including disaster recovery plans, business continuity plans, crisis management plans, evacuation plans, pandemic plans, and other strategic plans to help aid in the effective and efficient recovery of our business operations.

One of the risks that impacts all organizations is the ability to keep business operations in-flight by identifying, assessing, and mitigating the threats that might impact business operations. This was clearly evident in 2021, a time which tested us like no other we had seen before. The COVID-19 global pandemic clearly showed us—and everyone—just how crucial a business continuity plan is in uncertain times. The change and upheaval we saw beginning in 2020 will likely echo for many years to come, both in terms of educational trends and changes to the way we view work and perhaps where we work from. The purpose of this paper is to set forth how we approach business continuity here at Instructure as part of our ongoing risk management program as we continue our mission to be the industry-leading learning management platform.

Disaster Recovery

Also included as part of our Business Continuity plan are our Disaster Recovery plans and procedures. No business wants a disaster, whether it's the catastrophic loss of a datacenter or a crazy panda running around the office pulling out cables. But if or when the time comes, having a robust disaster recovery plan in place allows us to restore our services as quickly as possible and minimize loss or disruption to both our customers and our internal operations.

Included in this document is an overview of the disaster recovery plan and procedures Instructure has established to recover from disasters affecting its production operations. We describe how our Software as a Service (SaaS) product offerings have been architected to recover from disaster scenarios, the steps we will take if a disaster is declared, our policies, communication strategies and customer notification procedures, and several example scenarios and impact assessments.

Business Continuity

Building in Resilience and Maintaining Plans to Effectively Recover

Instructure's approach to business continuity is building resilience into its processes, technology and people. This document describes the different practices Instructure uses to ensure business resilience through the core business functions by ensuring synchronization between the use of technology and applications, infrastructure and cloud service providers, and personnel. This approach is based on industry best practices for SaaS for mitigating downtime caused by common disruption of service vectors for SaaS companies including, but not limited to cyber attacks, physical security breaches, vendor dependencies, fraud and civil disturbances, pandemics, and natural or man-made disasters.

The practices adopted by Instructure increase the ability to recover from a disruption in service and protect its customers' data, as well as its personnel. These practices involve processes for both preventative and recovery practices that aim to meet the following objectives:

- Provide continued service to customers
- Reduce risk to core business operations
- Maintain clear communication with customers and employees

Processes

Instructure has designed and operates the following key processes to support Instructure's ongoing (and effective recovery of incidents impacting) business operations:

Incident response plans - Instructure has developed, maintains, and operates comprehensive incident response plans. These plans include definitions of incident preparation, detection, assessment of incident criticality, escalation, containment actions to take based on the criticality of the incident, communication methods, testing, and playbooks—or examples of what to do given certain incidents, and improvement.

Backup and recovery plans - Instructure has developed, maintains, and operates robust backup and disaster recovery plans. These plans include taking daily snapshots (backups) and near-real-time replicating data to a separate, geographically isolated location within the customer's region. Because Instructure uses the world leader in Infrastructure as a Service (IaaS), Amazon Web Services (AWS) to host data in the customer's geographical region, each region has multiple, isolated locations known as

Availability Zones where customer data is replicated for disaster recovery purposes. The use of multiple AWS Availability Zones is to ensure that if there is a failure in one physical location, the data is readily available in another geographically separate location. Backups and customer-uploaded objects are stored in Amazon S3, which boasts 99.999999999% uptime and reliability over a given year. Backups are checked for integrity and tested at least once a month.

Vendor Assessments - Instructure operates a robust third party security risk management program. These practices include managing an accurate inventory of vendors, conducting vendor risk assessments, and reviewing critical vendors' security and availability practices. These reviews include ensuring that the vendors have robust practices for backup, disaster recovery, and business continuity plans. Additionally, Instructure also ensures Service Level Agreements with vendors contain a description of services provided and contain information regarding promised network availability.

Cyber Insurance - Instructure ensures it protects its business from major expenses, business losses, and regulatory fines and penalties should a data breach occur by having cyber insurance coverage.

Annual Recovery testing - Instructure tests recovery plans at least once annually using both live scenario tests and tabletop tests. Scenarios include events where service disruptions occur and personnel included in the tabletop testing are responsible for determining actions used to recover services.

Risk Management - Instructure recognizes risk management as a critical component of its operations that helps to verify customer assets are properly protected and incorporates risk management throughout its processes.

Strategic Planning - Instructure has an overall strategic plan that is presented to the board of directors. This plan is separated into specific segment plans designed to 'operationalize' what is expected of the segments in order to support Instructure's overall objectives.

Communication Channels - Instructure has processes in place to respond to incidents and inform all of its personnel in case of a service disruption or event that needs to be communicated to its personnel. In general, customers will be notified primarily by their respective Customer Success Manager (CSM), who is the main point of contact with all customers. CSMs will use the preferred method(s) of communication identified by the customer. In the event of a widely impacting outage, notifications will also be provided using a more widely available public website with the latest details. For internal communications, Instructure has identified both a primary and a secondary means for communication during an impactful event in order to keep the recovery efforts effective during an incident.

Crisis Training - Instructure has a crisis response team that consists of its Human Resources, Communication, Legal, and Security teams to respond to crisis situations at Instructure office locations. Additionally, Instructure engages in crisis training and exercises, that include, for example, fire drills and emergency evacuations.

Ownership

Instructure's Chief Information Security Officer (CISO) is responsible for overseeing business continuity in coordination with the Senior Vice President (SVP) of Engineering. We also have a defined disaster recovery team with ultimate escalation to the SVP of Engineering. On the commercial side, all potential disasters are escalated immediately to the Chief Financial Officer, who is ultimately responsible for assessing the event and directing notifications.

Alternate Recovery Site

All Instructure personnel have the capability to work from home (WFH) in case of a disruption that affects the ability to work from one of the Instructure office locations. To ensure this practice is effective, Instructure ensures there are remote working policies in place and communicated to all personnel, security practices are in place for accessing corporate networks, and mass communication notification services in place. Multiple providers are used to supply Instructure's offices with connectivity—allowing for quickly resumption of connectivity if one provider is found unable to provide the level of service required to sustain consistent, continual connectivity. As part of Instructure's annual business continuity tabletop testing, use cases can include events that affect remote employees, Instructure offices, and communication procedures.

Training

Instructure has a crisis response team that consists of its Human Resources, Communication, Legal, and Security teams to respond to crisis situations at Instructure office locations. Additionally, Instructure engages in crisis training and exercises including fire drills and emergency evacuations.

Open Source Code

Instructure's commitment to commercial open source provides another layer of reassurance to clients in terms of business continuity. The Canvas Learning Management System is available as open-source, which means the Canvas LMS code is free, public, and completely open at all times*. Anyone can use the Canvas LMS code without additional cost. Instructure updates the Canvas LMS code on a regular basis, and the code is maintained on GitHub: https://github.com/instructure/canvas-lms/wiki.

In the unlikely event of any material changes to Instructure's normal business operations, our customers have access to the Canvas LMS open-source code to allow for business continuity. This

would allow institutions to host, operate, and support the Canvas LMS open-source code on their own servers in the case that Instructure was no longer able to do so. In addition to our open source code, Canvas LMS also provides content export, open RESTful API access, and Canvas Data. This means our customers will always have access to their course content and data.

*excludes some plugins and extensions that are currently not open source

Disaster Recovery

Key Terms and Assumptions

In the Software as a Service (SaaS) space, there are some key terms in relation to Disaster Recovery.

1) In the context of a disaster recovery scenario, two terms are commonly used to describe how a recovery process may be affected: **Recovery Time Objective (RTO)** and **Recovery Point Objective (RPO)**. The RTO represents how long it will take to restore access to data, and the RPO how much data is at risk of being lost. For example, if it takes 8 hours for a service to be recovered, the RTO is 8 hours. If the last 4 hours of data will potentially be lost due to a disaster, the RPO is 4 hours.

2) While '**Disaster Recovery**' and '**High Availability**' are shared concepts in relation to business continuity, they impact disaster recovery planning differently. Disaster Recovery essentially infers there will be some form of downtime involved, measured in hours or days. High Availability, however, is about ensuring ongoing continuity of operations in a disaster recovery scenario, especially through the design of architectural redundancies such as automated failover of components.

Our services are architected to achieve both exceptionally low RPO and RTO in the most common scenarios and High Availability for our customers due to the distributed and resilient nature of our infrastructure. For the vast majority of failure scenarios, the need to failover to another Availability Zone (AZ) is obviated and the impacts to our services will be minimal.

The primary assumption of our disaster recovery plan is that it only addresses events that would affect an entire data center or our architecture as a whole. Failures of individual components will be recovered through robust architectural redundancies and failover mechanisms.

Disaster Recovery in a SaaS World

Instructure's educational software (and associated data) is hosted in the cloud by Instructure and delivered over the internet through the world's most trusted public cloud provider, Amazon Web Services (AWS). This Software as a Service (SaaS) delivery model means that our customers don't have to worry about maintaining server hardware or software, patches, service packs, or, in the context of this document, disaster recovery.

Not only do we maintain our own robust disaster recovery plans and procedures, but we also benefit from using AWS, an Infrastructure as a Service (IaaS) world-leader that bakes redundancy into its services by providing numerous regions, availability zones, and data centers that allow us to recovery quickly in the event of an unforeseen disaster.

Given the nature of the SaaS delivery model, Instructure is responsible for providing disaster recovery in relation to our software and associated data. Naturally, best practice also dictates that our customers develop and maintain their own disaster recovery plans and procedures.

Definition of a Disaster

A disaster is defined as any disruptive event that has potentially long-term adverse effects on Instructure's services. In general, potential disaster events will be addressed with the highest priority at all levels at Instructure. Such events can be intentional or unintentional, as follows:

- **Natural disasters**: Tornado, earthquake, hurricane, fire, landslide, flood, electrical storm, and tsunami.
- **Supply systems**: Utility failures such as severed gas or water lines, communication line failures, electrical power outages/surges, and energy shortage.
- **Human-made/political**: Terrorism, theft, disgruntled worker, arson, labor strike, sabotage, riots, war, vandalism, virus, and hacker attacks.

Disaster Recovery Procedures

Disaster Monitoring Phase

Instructure monitors the performance of our services around-the-clock using external performance monitoring tools and internal, open- and closed-source monitoring tools. These tools are configured to send real-time alerts to our personnel when certain events occur that would warrant investigation into a potential looming disaster scenario.

Activation Phase

All potential disasters are escalated immediately to both the Executive Leadership Team and the Senior Director of Production Engineering (or a designated officer) who are responsible for assessing the event and confirming the disaster. Once confirmed, the Incident Commander is authorized to declare a disaster and begin activation of the Disaster Recovery Team (DRT). Because disasters can vary in terms of severity and disruption, and can also happen with or without notice, the DRT will assess and analyze the impact of the disaster and act quickly to mitigate any further damage.

Once a disaster has been officially declared, the Incident Commander is responsible for directing the DRT recovery efforts and ongoing notifications.

Execution Phase

Recovery operations commence once the disaster has been declared, the disaster recovery plan activated, the relevant staff notified, and the Disaster Recovery Team (DRT) prepped to perform the recovery activities as outlined in *Backup and Recovery Practices, Performing Recovery*.

Key Organizational Resources

Incident Commander

Jon Fletcher, Senior Director of Production Engineering

Disaster Recovery Team

The Disaster Recovery Team (DRT) is made up of key engineers and operations employees across all areas of our business. The responsibilities of the DRT include:

- Establish communication between the individuals necessary to execute recovery
- Determine steps necessary to recover completely from the disaster
- Execute the recovery steps
- Verify that recovery is complete
- Inform the Incident Commander of completion

Communication Strategy

Notifying Internal Stakeholders

The Incident Commander is responsible for making sure the DRT and any other necessary staff are notified of an emergency or disaster and mobilized.

The DRT (and other key operational staff) have a scheduled on-call roster and are contactable 24x7 in an emergency or disaster. We use a paging platform that specializes in SaaS incident response which allows us to page key staff to commence activation at a moment's notice.

Notifying Customers

- **Disaster Declaration**: Impacted customers and business partners will be notified immediately if a disaster is declared. The notification will include a description of the event, the effect to the service, and any potential impact to data.

- **Updates throughout Execution Phase**: Impacted customers and business partners will be kept up to date throughout the disaster recovery process via phone, messaging, and/or email. We will also post official status updates on status.instructure.com.

- **Completion of Recovery:** Once recovery is complete and services have resumed, our customer notifications will include general information about the steps taken to recovery, and any data that may have been impacted. If the recovery is partial and the service is still in a degraded state, notifications will include an estimate of how long the degradation will continue.

If the primary contact(s) for disaster recovery (nominated by the customer) is unavailable, we will notify the alternative contact (also nominated by the customer). If, for any reason, we are unable to contact the customer's primary and alternative contacts, we will endeavor to make contact with other representatives of the customer's organization.

Disaster Resilience

Operating Infrastructure

Instructure's services are based on a multi-tier cloud-based architecture. Each component is redundant with active monitoring for failure detection and automated failover. The different tiers are:

Load Balancers

All web traffic to our services is served by load balancers in active/passive configurations. The load balancers are responsible for directing traffic to the next tier.

App Servers

App servers process incoming client requests from the load balancers. App servers implement all the business logic, but do not persist any important data. Asynchronous jobs also run on the app servers. The number of app servers varies based on demand but will always be at least two in active/active configurations.

Caching

To improve performance, Instructure's software aggressively caches data in a caching layer. The data stored in the caching layer is strictly a performance cache. Any data loss resulting from the loss of any of these servers would be limited to a small number of page view statistics that may not have been flushed to persistent storage. The number of cache servers is variable, and the cache data will be partitioned among all servers.

Databases

Most structured data—courses, user information, and assignments, for example—is stored in a database. This data is typically sharded between instances based on account and on demand. Each shard has a primary and a secondary database, located in geographically separate sites. The data from each primary is replicated asynchronously in near real-time to its corresponding secondary. Each primary is also backed up completely every 24 hours, and the backup is stored in a third geographically separate site. The infrastructure also includes an internal database proxy layer for the relational databases that enables the Operations Team to perform maintenance on the relational database servers with minimal downtime.

Third-Party Object Store

Content—such as documents, PDFs, audio, and video—is stored in a third-party scalable object store.

Data Centers

Data centers are built in clusters in various global regions where we operate. All data centers are online and continually serving our customers; no data center is “cold.”

In the case of failure, automated processes move customer data traffic away from the affected area. Our core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. N in this context simply refers to the amount of capacity needed to run a service at full load. N+1 indicates an additional, duplicate layer has been added to support primary service failure and therefore provide failover and redundancy at equivalent capacity.

As the world leader in Infrastructure as a Service (IaaS), Amazon Web Services (AWS) provides us with the flexibility to place instances and store data within multiple geographic regions as well as across multiple availability zones within each region.

Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by region).

In addition to utilizing discrete uninterruptible power supply (UPS) and onsite backup generators, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability Zones are all redundantly connected to the AWS Global Backbone, a carrier-class backbone built to standards of the largest ISPs in the world (known as Tier 1 transit providers).

Data Sovereignty

We architect our AWS usage to take advantage of multiple regions and Availability Zones (AZ). Distributing applications across multiple availability zones provides the ability to remain resilient in the face of most failure scenarios, including natural disasters or system failures. For location-dependent privacy and compliance with data sovereignty requirements, such as the EU Data Privacy Directive, data is not replicated between regions. However, in the unlikely event of a disaster that affects a customer's entire region, our services can be relocated to numerous active regions within the AWS infrastructure that Instructure uses.

Backup and Recovery Practices

Customer data is backed-up automatically both in real-time and on a 24-hour schedule to multiple geographic locations in the customer's region, ensuring the security and reliability of data in the event of a disaster or outage of any scale. Database is backed up from one live database to another, with no additional load on our systems. Static files are stored in secure, geographically redundant storage systems. Recovery backups are encrypted using the AES-GCM 256-bit algorithm and stored within a highly secured separate location. The IT Operations team is alerted when backups fail and any failures are tracked to resolution. These backups are retained in accordance with a defined retention schedule according to product. *See Backup Retention.*

As an example, our Canvas LMS backup and recovery procedures are outlined below:

Canvas Production Databases

Performing Backup	**Data is replicated asynchronously in near real-time to remote site (monitored, etc.).** **Nightly backups of every database are stored at a remote site.**
	When secondary database is up to date (common case): Promote secondary database to primary, following replication docs Provision new database using provisioning tools Establish new database as new secondary, following replication docs
Performing Recovery	When secondary is > 24 hours behind (unlikely): Copy last nightly backup to secondary database Load secondary database with nightly backup Provision new database using provisioning tools Establish new database as new secondary, following replication docs

Static assets such as documents and other content files

Performing Backup	**Files are stored on a scalable, encrypted, geographically redundant storage (Amazon S3)**
Performing Recovery	Recovery in case of failures is built into the scalable storage system

Web applications

Performing Backup	**Web application source code is stored in versioned source control and backed up to multiple locations** **There is no state stored on the application servers that would need to be backed up**
Performing Recovery	Not applicable

Backup Retention

Canvas

Canvas LMS

In addition to real-time replication to multiple geographic locations in the customer's region ensuring an incredibly low RPO, Instructure retains full database backups (also known as "snapshots") for Canvas customers, totalling **12 months** of rolling backup data. Specifically, we retain:

- **7 x daily** snapshots
- **4 x weekly** snapshots
- and, **12 x monthly** snapshots.

This allows us to conduct Point-In-Time-Recovery (PITR) for up to **4 months** of aged data, and perform monthly restores for **5-12 months** of aged data.

Object data such as files, documents, and uploaded media, etc., are recoverable in the event of a deletion or modification for a period of **1 year**.

Canvas Credentials

Canvas Credentials databases and media (badges) are backed up with Point in Time (PIT) snapshots with a 5-minute granularity.

The following backup retention rules apply to pertinent Canvas Credentials information:

- Daily incremental backups are saved for **1 week**
- Weekly backups are stored for the previous **4 weeks**
- Monthly backups are stored for the previous **13 months**
- Full backups are saved for **13 months**.

Canvas Catalog

Canvas Catalog is backed up daily and backups are retained as follows:

- Last **60 daily** backups retained
- Last **60 monthly** backups retained

Canvas Studio

Canvas Studio backups are configured to be retained as follows:

- One snapshot for each of the past **7 days**
- One snapshot for each of the prior **4 weeks**
- One snapshot for each of the prior **12 months**
- The most recent snapshot

Student Pathways / Student ePortfolios

Student Pathways / Student ePortfolios are configured to be retained for **35 days**.

Mastery Connect

Data backup procedures have been configured within AWS to run a daily full backup snapshot of Mastery Connect databases. Mastery Connect backups are configured to be retained as follows:

- Point In Time (PIT) snapshots for **35 days**
- Daily snapshots for **35 days**
- Monthly backups for **1 year**
- Yearly backups for **10 years**

Impact

While Impact does not store or process customer data, backup procedures have been configured within AWS to run a daily full backup snapshot of Impact system databases and configuration. Impact backups are configured to be retained as follows:

- Daily snapshots for **7 days**

Elevate

Elevate K-12 Analytics

Customer data is ingested by Elevate K-12 Analytics for analysis and therefore Elevate K-12 Analytics is not considered a source of truth for customer data. However, we use AWS Backup to create backups of EC2 instances (user configuration, dashboards, and settings, etc.) as follows:

- AWS daily backups for **15 days**
- AWS monthly backups for **1 year**

Elevate Data Quality

Customer data is ingested by Elevate Data Quality for analysis and therefore Elevate Data Quality is not considered a source of truth for customer data. However, we use AWS Backup to create backups of EC2 instances (user configuration, dashboards, and settings, etc.) as follows:

- AWS monthly backups (currently we do not delete backups; **indefinite retention**)

Elevate Data Hub

- Weekly Long-Term Retention Backups for **6 months**
- Monthly Long-Term Retention Backups for **1 year**
- Yearly Long-Term Retention Backups; Keep week 52 for **3 years.**

Disaster Recovery Plan Testing

A Disaster Recovery Plan is only useful insofar as it is tested regularly.

The Incident Commander is responsible for ensuring our Disaster Recovery Plan is reviewed at least annually and in part whenever major components of our architecture are changed. We conduct annual table-top exercises which discuss simulated emergency situations and allow the DRT to discuss our processes and plans to manage both an incident and the aftermath of a natural or human-made disaster. Typically, for our tabletop testing we focus on the more extreme scenarios, such as the loss of an Availability Zone and/or hosting region. Any changes or revisions of a DR response are then captured and updated in our formal Disaster Recovery Plan.

Our tabletop DR tests are conducted annually, and a letter of attestation is available on request.

We also frequently test our ability to restore from backup as part of our regular release cycle, as non-production sites are populated from production backups. For example, Canvas LMS non-production (beta) instance(s) are restored each week from production backup data, thus testing our ability to recover from data loss each and every week (verifiable in a client's own instance).

Functional Testing

Instructure has a crisis response team that consists of its Human Resources, Communication, Legal, and Security teams to respond to crisis situations and/or disaster scenarios at Instructure office locations. On an ongoing basis, we engage in crisis training and exercises, that include, for example, fire drills and other disaster scenarios.

Sample Disaster Scenarios

We have outlined below several possible disaster scenarios, the services affected, recovery strategies, and the Recovery Point Objective (RPO) / Recovery Time Objective (RTO), services affected, and recovery overview. Note that these are intended only to convey magnitude of impact and recovery efforts required under different situations. *Likelihood* is an estimated chance of the scenario occurring but does not guarantee occurrence - its presence is intended not to convey probability, but rather, to merely indicate chance and describe the unlikeliness of some of the most extreme scenarios. *Last Incident* refers to the last time we encountered this disaster recovery scenario in a live environment.

Complete Loss of a Primary Database

Services Affected	Most accounts hosted on the affected database
Recovery Overview	When the secondary database is up-to-date (common case): The secondary database is promoted to be the new primary database according to the steps described above When the secondary database is inconsistent: The secondary database is populated with the latest nightly snapshot and brought online as the new primary database.
RPO	5 minutes (consistent secondary, common case), 24 hours (inconsistent secondary)
RTO	1 hour (consistent secondary, common case), 6 hours (inconsistent secondary)
Likelihood	Unlikely (Once every 5+ years)
Last Incident	Never

Simultaneous Complete Loss of Primary and Secondary Databases

Services Affected	Most accounts hosted on the affected database.
Recovery Overview	New primary and secondary databases are brought online in separate locations The primary database is populated with data from the remote backup App servers are pointed to the new primary database Replication re-established with the new secondary database
RPO	24 hours
RTO	6 hours
Likelihood	Rare (Once every 20 years; the primary and secondary databases are hosted in geographically separate locations, which makes simultaneous failure unlikely)
Last Incident	Never

Database Destruction by Security Breach

Services Affected	Most accounts hosted on the affected database.
Recovery Overview	The primary database is restored from the most recent complete backup Replication is re-established with the secondary database
RPO	24 hours
RTO	6 hours
Likelihood	Highly Unlikely (Once every 10+ years)
Last Incident	Never

Complete Loss of Primary Hosting Facility

Services Affected	Platform for most accounts
Recovery Overview	New load balancers and app servers are brought up in the secondary site with the secondary database The old secondary database is promoted to primary database. A new secondary database is brought up at a third site and replication re-established DNS is pointed to the new load balancers at the recovery site and services are restored
RPO	4 hours
RTO	Commercially Reasonable
Likelihood	Extremely Unlikely (Once every 100+ years)
Last Incident	Never

Conclusion

We live in an unpredictable world. Disasters are in many ways, inevitable, and we recognize, despite architecting our products for high availability and failover, that it would be unwise to assume our business was immune to disaster. As the leading educational Software as a Service (SaaS) provider, we recognize that your most precious non-human asset you entrust with us is data. This is why we have taken careful planning and preparation to create robust business continuity and disaster recovery plans and procedures as outlined in this document, which we hope instills trust and assurance that, in the unexpected event we do encounter disaster, we are prepared, capable, and ready to launch recovery efforts to restore our services as quickly as possible and minimize loss or disruption to our customers.

Our approach to business continuity planning is that it is a living, breathing part of our organization that evolves as we change and grow with our customers. We've learned from the COVID-19 global pandemic that business continuity is not that of fiction or merely a required document to checkbox in the course of doing business but, on the contrary, is vital to surviving (and thriving) through disasters, threats and challenges. During the last two years of the pandemic, not only did our employees have to adapt to working from home and live a new normal for many months of disruption to business as usual, but at the same time, were required to work as a united team like never before and provide monumental efforts to keep our services running as normal when thousands upon thousands of students were forced to migrate to online learning. Thanks to our business continuity planning, when our customers needed our services more than ever to provide high availability and performance throughout the global pandemic and stressful times, we delivered.

At Instructure, we proactively approach business continuity by building resilience in our key processes, use of technology, and hiring and retaining key personnel. When unforeseen incidents impact or disrupt our business, know that we are ready to act, with robust plans to quickly recover and ensure the continuation of both our business and yours during and following any critical incident that results in disruption to our normal operational capability.