INSTRUCTURE

Instructure Business Continuity

Instructure Security, Engineering, and Operations

June 2020

CANVAS PORTFOLIUM BRIDGE

Table of Contents

Overview

Every organization is subjected to a variety of risks. At Instructure, we have a robust risk management process where we identify, assess, and treat risks on an ongoing basis. We have an Enterprise Risk Steering Committee comprised of key leaders throughout Instructure, who meet regularly, and continually--collectively--identify and mitigate risks that might impact Instructure and its important mission.

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 pop up over time. At Instructure, we have an effectively designed and operating 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 incidents. 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, efficient recovery of 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. The purpose of this whitepaper is to expound on how we approach business continuity as part of our risk management program.

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 cyberattacks, physical security breaches, vendor dependencies, fraud and civil disturbances, pandemics, and natural or manmade 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 viable backup and disaster recovery plans. These plans include taking daily snapshots (backups) and near-real-time replicating data to a separate, geographically isolated region. Instructure uses Amazon Web Services (AWS) regions that are separated geographically and each region has multiple, isolated locations known as Availability Zones. The use of multiple regions is to ensure that if there is a failure in one region, the data is also located in another AWS region. Backups and customer-uploaded objects are stored in Amazon S3, which

boasts 99.999999999% 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 responses to active shooters and fire drills.

Technology

Instructure uses the following proven technology to support Instructure's ongoing (and effective recovery of incidents impacting) business operations:

Amazon Web Services

Instructure hosts all customer-facing web applications and supporting infrastructure on AWS. The AWS infrastructure is highly stable, fault-tolerant, and secure. AWS publishes an insightful security whitepaper that describes how AWS implemented physical security and environmental protection mechanisms to protect AWS data centers throughout the world. Instructure relies on AWS's ability to design and operate these critical mechanisms and controls to protect physical access to data and availability of Instructure's services.

AWS data centers utilize state-of-the-art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards and access is authorized strictly on a least-privileged basis. Environmental systems are designed to minimize the impact of disruptions to operations. Multiple geographic regions and Availability Zones provide resilience in the face of most failure modes including natural disasters or system failures.

AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure for critical and essential loads in the facility. Generators provide backup power for the data centers of the entire facility.

Instructure uses AWS in such a way to take advantage of all of these benefits described in the paragraphs above. Using AWS' technology--which is built with resilience as a core component to its services--has helped provide Instructure with a differentiating advantage in providing available and resilient applications for customers.

Teleworking Capabilities

Instructure personnel have the capability to work from home 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 teleworking 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.

Remote Offices and Workers

Instructure includes its worldwide office locations and remote workers in its business continuity practices. Additionally, as part of Instructure's annual business continuity tabletop testing, use cases can include events that affect remote employees, Instructure offices, and communication procedures.

Third Party Technology

Instructure relies on several third party software solutions as part of operating key business functions. As part of selecting these third parties to provide these services to Instructure, Instructure's enterprise services team performs a thorough vet of the technology provided by these third parties to help ensure the third party has adequate technology in place to support Instructure to the level of service required by Instructure.

People

Instructure employs (and aims to retain) amazing personnel to support Instructure's ongoing (and effective recovery of incidents impacting) business operations. The following describe some key personnel functions and how Instructure aims to keep these functioning effectively.

Roles and Responsibilities

For all of the plans listed above, Instructure has defined roles and associated responsibilities to individuals to help most effectively respond to these incidents. In general, roles have identified and defined for an Incident Leader and an Incident Response Team (inclusive of roles for managing communication, customer support, public relations, legal, security, human resources, and other critical functions that contribute to an effective response to incidents).

Customer Support - Instructure has customer support teams that are responsible for responding to and resolving customer-reported inquiries, complaints, disputes, and operational requirements regarding

Instructure products. These teams include multiple levels of representatives that can handle ranges of technical support to customers.

Personnel Shortage Plans

Instructure has procedures in place to protect itself against any risk of personnel shortages, which includes the use of cross-trained personnel and hiring reputable and experienced contractors, when necessary. Succession plans are also in place to help ensure key roles have skilled personnel in place to maintain operations.

Retaining Key Personnel

Instructure ensures there are programs, benefits, and training in place to retain key personnel. These include monitoring job satisfaction by surveys and regularly scheduled meetings with managers, providing personnel with compensation packages that include medical and health benefits, and providing a work environment that promotes training and flexibility to learn about other opportunities at work.

Conclusion

In summary, Instructure proactively approaches business continuity by building resilience in to its key processes, use of technology, and hiring and retaining key personnel, and has robust plans to recover business operations for when incidents impact or disrupt these elements.