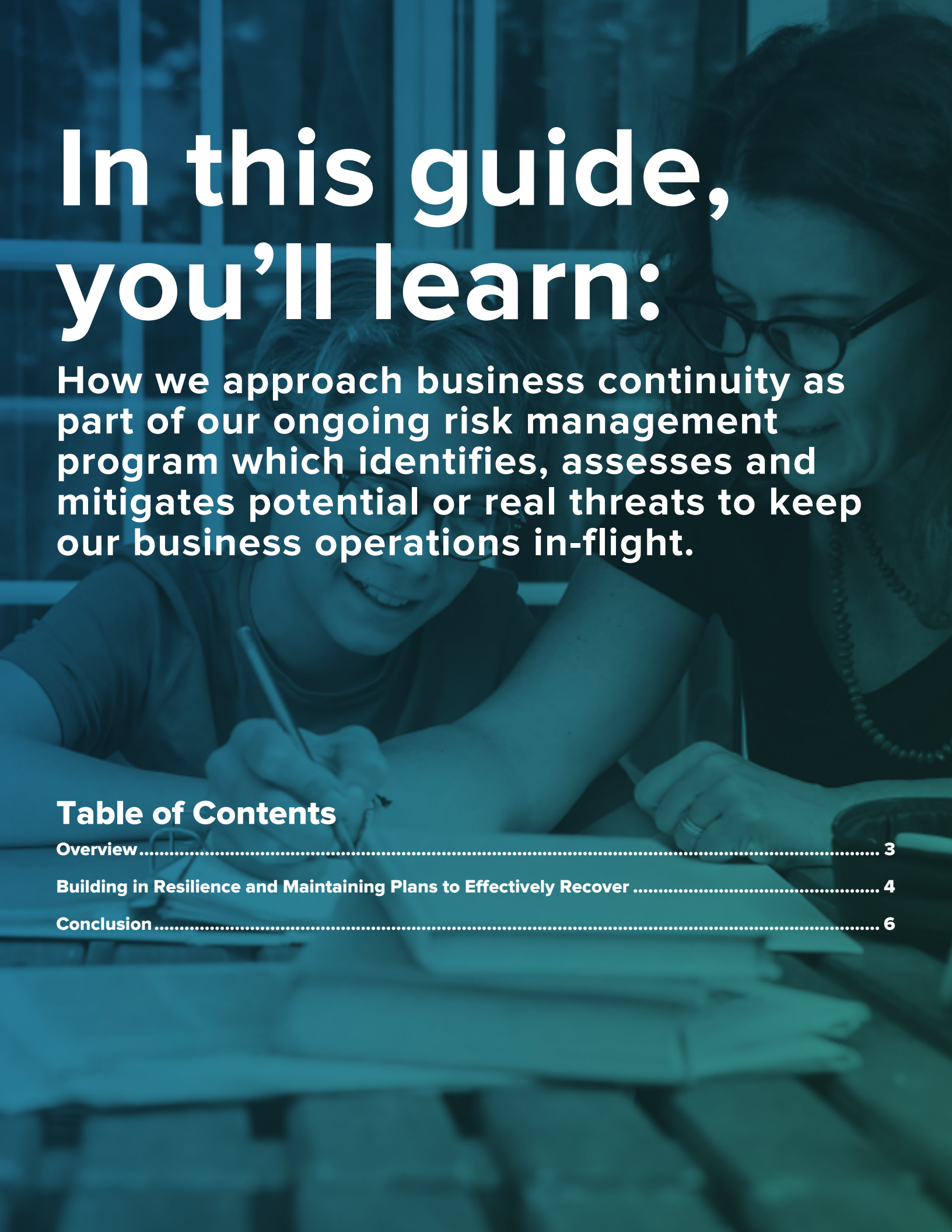
INSTRUCTURE

Business Continuity

Engineering, Security, and Operations

January 2021



In this guide, you'll learn:

How we approach business continuity as part of our ongoing risk management program which identifies, assesses and mitigates potential or real threats to keep our business operations in-flight.

Table of Contents

Overview

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 2020, a year 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 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.

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, responses to active shooters and fire drills.

CONCLUSION

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 2020, 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.