



*Proprietary & Confidential*



## Canvas Learning Management System and Studio Video Learning Platform

### SOC 3

Relevant to Security, Availability, Processing Integrity,  
Confidentiality, and Privacy



*Integrated SOC 3 Report Prepared in Accordance with the AICPA Attestation  
Standards and IAASB ISAE No. 3000 (Revised) Standards*

JULY 1, 2022 TO JUNE 30, 2023



# Table of Contents

<b>I. Independent Service Auditor's Report</b>	<b>1</b>
<b>II. Instructure's Assertion</b>	<b>4</b>
<b>III. Instructure's Description of the Boundaries of Its Canvas Learning Management System and Studio Video Learning Platform</b>	<b>5</b>
<b>A. System Overview</b>	<b>5</b>
1. Services Provided	5
2. Infrastructure	6
3. Software	7
4. People	8
5. Data	9
6. Processes and Procedures	9
<b>B. Principal Service Commitments and System Requirements</b>	<b>15</b>
<b>C. Complementary Subservice Organization Controls</b>	<b>16</b>
<b>D. Complementary User Entity Controls</b>	<b>17</b>

## I. Independent Service Auditor's Report

Instructure, Inc.  
6330 South 3000 East #700  
Salt Lake City, UT 84121

To the Management of Instructure:

### Scope

We have examined Instructure's accompanying assertion in Section II titled "Instructure's Assertion" (assertion) that the controls within Instructure's Canvas Learning Management System and Studio Video Learning Platform (system) were effective throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Instructure's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Instructure uses Amazon Web Services for data hosting services and Elevate Data Sync for data processing services (subservice organizations). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Instructure, to achieve Instructure's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Instructure's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Instructure, to achieve Instructure's service commitments and system requirements based on the applicable trust services criteria. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

### Service Organization's Responsibilities

Instructure is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Instructure's service commitments and system requirements were achieved. Instructure has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Instructure is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.



## Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Instructure's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Instructure's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

## Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

## Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.



## Opinion

In our opinion, management's assertion that the controls within Instructure's Canvas Learning Management System and Studio Video Learning Platform were effective throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Instructure's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Salt Lake City, Utah  
September 19, 2023

## II. Instructure's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Instructure's Canvas Learning Management System and Studio Video Learning Platform (system) throughout the period July 1, 2022 to June 30, 2023 to provide reasonable assurance that Instructure's service commitments and system requirements relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy were achieved. Our description of the boundaries of the system is presented in Section III titled "Instructure's Description of the Boundaries of Its Canvas Learning Management System and Studio Video Learning Platform" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Instructure's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Instructure's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III titled "Instructure's Description of the Boundaries of Its Canvas Learning Management System and Studio Video Learning Platform".

Instructure uses Amazon Web Services for data hosting services and Elevate Data Sync for data processing services (subservice organizations). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Instructure, to achieve Instructure's service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Instructure's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Instructure, to achieve Instructure's service commitments and system requirements based on the applicable trust services criteria. The description presents Instructure's complementary user entity controls assumed in the design of Instructure's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Instructure's service commitments and system requirements were achieved based on the applicable trust services criteria.



### III. Instructure's Description of the Boundaries of Its Canvas Learning Management System and Studio Video Learning Platform

#### A. System Overview

##### 1. Services Provided

###### COMPANY OVERVIEW

Instructure is focused on helping institutions improve education through technology. Instructure provides the Canvas Learning Management System (Canvas), a cloud-based education technology platform with advanced learning management system (LMS) functionality; and the Studio Video Learning Platform (Studio), a cloud-based education technology platform with advanced video learning platform functionality. Instructure's comprehensive implementation and hosting services include full system monitoring, automated provisioning, hands-free update and upgrade services, a basic support package, an online standard training package, and a beta environment. The Canvas architecture, inclusive of the Canvas and Studio web applications, is hosted on public cloud infrastructure hosted by Amazon Web Services (AWS). AWS provides the foundation for Instructure's products to be extremely reliable, available, extensible, secure, and scalable cloud-based LMS solutions.

Instructure was incorporated in September 2008, and is headquartered in Salt Lake City, Utah.

###### SYSTEM DESCRIPTION

###### CANVAS LEARNING MANAGEMENT SYSTEM (CANVAS)

Canvas is a course organizer and resource manager and provides student guidance for personalized learning. Canvas is a subscription service and provides a platform to help teachers organize and sequence content, learning activities, and assessments; and streamline the delivery of learning.

Key features, services, and strategies that differentiate Canvas include:

- *Advanced LMS functionality:*
  - legacy content migration tools
  - SpeedGrader <sup>TM</sup>
  - rich-content integration
  - learning outcomes
  - rubrics
  - ePortfolios
  - communication channels
  - robust analytics and reporting toolset
  - canvadocs/document viewer
  - Google Drive/Office365 LTI



- file management system (Inst-FS)
- Android and iOS mobile applications
- outcomes
- assessments and quizzes
- *Robust architecture*-Native cloud implementation, Web 2.0 tools and services integration, open RESTful and GraphQL application programming interfaces (APIs), automated provisioning, horizontal scalability, fully redundant resources, minimal site administration, and exceptional extensibility, reliability, and availability.
- *Usability and quality of the user experience*-Canvas consistently receives high ranks for ease of use and the overall user experience. Native features and apps provide a robust experience for each student using Canvas.
- *Cloud technology*-Being a leading innovator in the LMS market, Instructure is committed to open web and educational technology standards. Canvas features and functionality are included as part of the annual subscription. Supported integrations, updates, and upgrades are also provided. As a native cloud application, Canvas is continuously updated so users always have the latest, up-to-date features.

#### STUDIO VIDEO LEARNING PLATFORM (STUDIO)

Studio is a video-centric, interactive way to approach e-learning. Where video-as-a-learning-tool has typically been one-way and passive, Studio makes learning an active, collaborative, and impactful two-way street.

Key features, services, and strategies that differentiate Studio include:

- *Seamless integration with Canvas*-Allows users of Canvas to integrate Studio to enhance the platform with Studio's video learning management technology. Allows users to use Studio anywhere the Rich Content Editor is used in Canvas.
- *Insightful analytics*-Allows instructors and administrators to quickly and easily analyze which videos people are watching, how long they are watching, and when they stop watching. This information allows instructors to optimize videos to communicate critical information more effectively and monitor learner behavior.
- *Engagement*-Allows learners and instructors to engage with video content by commenting directly on the video timeline in real time. Learners can learn from each other's insights as well as from the instructor's direction and feedback.
- *Two-way video*-Engages users by turning content into conversation, making video a discussion, not a statement.

## 2. Infrastructure

Instructure's production computing, storage, and networking infrastructure is hosted on the AWS public cloud service. The infrastructure is distributed across discrete regions and availability zones within the AWS enterprise. This solution allows for the quick creation/destruction of compute, storage, and network resources based on customer demand with minimal budget impact or lead time. Instructure utilizes the following AWS services to facilitate the operation of its applications:





AWS Service	Function
<b>Elastic Compute Cloud (EC2)</b>	EC2 provides a virtual computing environment that uses web service interfaces to perform the following functions: <ul style="list-style-type: none"> <li>• Launch instances of operating systems.</li> <li>• Create Amazon Machine Images (AMIs) containing applications, libraries, data, and associated configuration settings.</li> <li>• Configure security and network access on the Amazon EC2 instances.</li> </ul>
<b>CloudWatch</b>	CloudWatch provides monitoring for AWS cloud resources and applications. CloudWatch provides visibility into resource utilization, operational performance, and overall demand patterns—including metrics such as central processing unit (CPU) utilization, disk reads and writes, and network traffic. CloudWatch provides the ability to review statistics, view graphs, and set alarms for specified metric data.
<b>CloudTrail</b>	CloudTrail is an AWS service that helps you enable operational and risk auditing, governance, and compliance of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail.
<b>Elastic Block Store (EBS)</b>	EBS provides raw block-level storage that can be attached to EC2 instances and is used by Amazon Relational Database Service.
<b>Relational Database Service (RDS)</b>	RDS is a web service used to operate relational databases in the AWS cloud.
<b>Simple Storage Service (S3)</b>	S3 is virtual storage used in conjunction with EC2 and EBS to store object data.
<b>Virtual Private Cloud (VPC)</b>	VPC is used to provision logically isolated virtual networks in the AWS cloud. VPC is used to manage the virtual networking environment, including selection of Internet Protocol (IP) address ranges, creation of subnets, and configuration of route tables and network gateways.

### 3. Software

Instructure builds and delivers Canvas and Studio as Software as a Service (SaaS) offerings. Each customer has a compartmentalized instance of the application, which is administered and customized by the customer using back-office functionality.

Canvas and Studio are engineered primarily using Ruby within the Rails framework. Application data is stored within enterprise relational databases and key value stores. Canvas and Studio are hosted on virtualized compute infrastructure running Linux.

Instructure leverages Okta as an authentication service, as well as GitHub as a code management tool. Monitoring utilities include Lacework and CloudTrail.



## 4. People

People consist of the personnel involved in the development, operation, and use of a system (including developers, operators, users, and managers). The following outlines the various teams and functions that support Canvas and Studio:

- *Customer Success*-This team is responsible for managing customer accounts and communicating directly with clients.
- *Customer Support*-This team is responsible for responding to and resolution of customer request tickets from end users and administrators at institutions. The Customer Support team is separated into multiple levels, including L1, L2, and L3 support representatives that handle ticket flow. Any ticket unable to be resolved by this team is routed to the Engineering team.
- *Database* – This team is responsible for database management.
- *Engineering*-This team is responsible for building and maintaining Canvas and Studio, including new feature development, maintaining current products, updating code, and fixing bugs.
- *Site Reliability Engineering (SRE)*-This team is responsible for the reliability of system infrastructure. This team maintains administrative access to branch protections.
- *Human Resources (HR)*-This team is responsible for hiring, benefits design and administration, employee relations, personnel growth, and performance evaluations through regular employee check ins, and overall compliance. HR also oversees the office administration and facilities staff.
- *Information Technology (IT)*-This team is responsible for supporting and assisting the maintenance of personal computer systems, databases, firewalls, Active Directory, networks, telephones, copiers, and general computer and network troubleshooting at Instructure.
- *IT Operations*-This team is responsible for designing, automating, and maintaining a large systems environment to support Canvas and Studio. This team's activities include automation, configuration management, writing code, and managing scale while effectively spinning up servers to maintain a highly available application for customers.
- *Legal*-This team is responsible for fielding whistleblower submissions and privacy inquiries.
- *Product*-This team is responsible to steer the features, enhancements, and user experience for Canvas and Studio. The Product team also develops new ideas and features based on industry understanding. This team maintains direct contact with customers, prospects, and market trends.
- *Security*-This team is responsible for the security of each layer of the technology stack supporting Canvas and Studio — including physical, personnel, network, AWS, systems, application, code, and data.
- *Senior Management*-This team is responsible for oversight of company operations. All other teams report up to the Senior Management team.
- *Technology Leadership*-This team is responsible for meeting monthly to discuss technological needs of Instructure products. This team includes leadership from the Security and Engineering teams.



## 5. Data

Canvas/Studio stores the following credential, profile, and transaction data on behalf of institutions and their users:

- Credential data consists of username, password, and multi-factor authentication (MFA) security questions used to protect user transaction data. These credentials are stored in a one-way, salted hash format.
- Profile data consists of user demographic data, including name, email, age, and gender.
- Transaction data consists of data gathered and curated during the course of users utilizing the features and functions of the Canvas and Studio web applications (such as course enrollment, assignment completion, and grades).

## 6. Processes and Procedures

The following is a list of Instructure's policies and a description of the contents contained within each policy:

- *Asset Management Policy*-Instructure maintains policies and procedures to help ensure assets, including servers, workstations, software, network devices, and media containing customer data, are managed from the point of acquisition to the point of decommissioning.
- *Customer Support Policy*-Instructure maintains policies and procedures for the Customer Support team to provide guidance on support protocol, including the appropriate use of client data.
- *Data Classification, Handling, and Encryption Policy*-Instructure maintains policies and procedures to help ensure customer and internal data are properly treated and protected according to their classification. The policy includes access rights, access restrictions, data retention, and data destruction requirements.
- *Disaster Recovery Plan*-Instructure maintains documented procedures to be followed in the event a disaster or other event threatens the availability of Instructure's products.
- *Disaster Recovery Policy*-Instructure maintains policies and procedures for addressing natural disasters, environmental hazards, and other incidents that would impair system functionality or cause accidental data disclosure.
- *End-User IT Security Policy*-Instructure maintains policies and procedures to help ensure devices are accessible only by internal employees and to prevent unauthorized access to company sites and equipment.
- *Enterprise IT Security Policy*-Instructure maintains policies and procedures for general information security which includes roles and responsibilities supporting Instructure's service commitments and system requirements.
- *Logging Policy*-Instructure maintains policies and procedures to govern the logging of system and application events; which include types of events logged, where logs are stored, and for how long.
- *Logical Access Policy*-Instructure maintains policies and procedures to help ensure processes are in place for managing access to systems by identifying users, authenticating users, and appropriately authorizing and provisioning user access to systems.



- *Network Security Policy*-Instructure maintains policies and procedures to help ensure firewalls are configured to limit network traffic to only approved ports, keeping network devices secured and up to date, configuring remote access for secure authentication, configuring wireless networks, and using effective intrusion detection technology.
- *Password Policy*-Instructure maintains policies and procedures to help ensure its personnel manage passwords using secure creation and handling.
- *Prime Directive*-This directive provides guidance to the Customer Support team concerning how to help end users change and access their own personal information.
- *Risk Management Policy*-Instructure maintains policies and procedures that define risk tolerances and include the identification, analysis, communication, and mitigation of risks relating to company operations, information technology, safeguarding of informational assets, product development, and changes in regulatory requirements or business relationships.
- *Security Awareness Policy*-Instructure maintains policies and procedures to provide its personnel with security training as part of onboarding and annually thereafter.
- *Security Incident Response Policy*-Instructure maintains policies and procedures to help ensure its personnel prepare, identify, and contain security, confidentiality, and privacy incidents. The policy also includes definition of responsibilities, escalation procedures, and notification requirements.
- *Software Development and Change Management Policy*-Instructure maintains policies and procedures for changes deployed to production environments, which include code changes, system configuration changes, architecture changes, and any other changes that would impact the security, availability, processing integrity, confidentiality, and privacy of production environments.
- *Third-Party Security Policy*-Instructure maintains policies and procedures to assess and monitor the security compliance of its critical third-party service providers.
- *Vulnerability Management Policy*-Instructure maintains policies and procedures that define how its personnel continuously identify, assess, and mitigate vulnerabilities based on overall risk rating.

## AUTHENTICATION

Employees utilize unique user IDs to authenticate to systems, and policy prohibits users from directly authenticating using service accounts. Access to internal company systems, including source code repository tools, code review tools, and internal ticketing systems, requires network authentication with a valid user ID and password. Access to the internal systems requires a valid username, MFA token, and password to authenticate. In addition, password authentication systems are configured to perform the following:

- prevent the reuse of at least the last 12 passwords
- restrict the use of 3 or more repeating characters
- restrict the use of a password that contains a user's display name or username
- check a user's proposed password against a blacklist of known weak passwords and dictionary words
- limit authentication attempts to 5 times prior to account lockout for 60 minutes



Access to production infrastructure is restricted to users with a valid SSH key. Authentication to the AWS Admin Console requires multiple factors (valid username and password, and one-time passcode). The AWS environment enforces a minimum password length of 12 characters and prevents the reuse of the most recent 24 passwords.

End users can rely on native authentication mechanisms or tie in their existing single sign-on solution. Native authentication to Canvas/Studio requires a minimum password length of eight characters.

## USER ACCESS ADMINISTRATION

Administrative access to production databases is restricted to the Engineering and Operations teams through role-based access.

New and modified access for internal personnel requires documented manager approval prior to these personnel receiving access. Additionally, the Security team performs a quarterly access review to validate ongoing appropriateness of access for internal Instructure employees and contractors within the production systems and databases. The IT and IT Operations teams disable or remove the relevant user accounts within five business days of termination.

Canvas and Studio end users are provisioned accounts through their respective local administrator. Local administrator accounts are provisioned for the user entity when the Canvas or Studio instance is first set up.

## NETWORK SECURITY

Instructure utilizes AWS asset tags to classify infrastructure components. Tags help manage, identify, organize, search for, and filter AWS resources.

Secure communication protocols are utilized to protect information transmitted over the internet. The storage of information, including user authentication information, and the transmission of private or confidential information through Canvas and Studio, is encrypted using Transport Layer Security (TLS) over Hypertext Transfer Protocol Secure (HTTPS) connections. Communications with Instructure systems over public networks are encrypted using TLS 1.2 or higher. Further, Data is encrypted at rest in production and non-production customer environments. Additionally, external connections to internal production systems pass through a firewall, limiting traffic to approved ports in accordance with the Network Security Policy.

Jump hosts point to Lightweight Directory Access Protocol (LDAP) servers to authenticate internal personnel to production systems. Jump hosts ban IP addresses after multiple failed access attempts within a defined period of time.

## VULNERABILITY MANAGEMENT

To validate application layer security, vulnerability scanning occurs monthly to validate that internal and public-facing systems are secure. The Security team engages a third party to either perform a penetration test or conduct researcher-based testing (i.e., a bug bounty program) for Instructure's client-facing services. Critical and high-severity vulnerabilities are tracked to remediation. The Security team logs vulnerabilities from both the scans and the bug bounty program or penetration test and tracks critical and high-severity vulnerabilities to remediation according to priority and risk levels.



## ENDPOINT MANAGEMENT

The Instructure IT team manages the configuration of desktops and laptops used by employees. Laptop and desktop computers are configured with full hard drive encryption and anti-malware software. The IT team centrally manages the anti-malware software to help ensure computers are periodically scanned and have updated signatures.

## SYSTEM MONITORING

System monitoring tools are in place to monitor company systems for capacity and operational processes. When specified thresholds are reached, notifications are sent to the Engineering team. If the team identifies a problem, the issue is documented and tracked to resolution in a ticket tracking system.

The Security team uses intrusion detection software to identify, monitor, and evaluate security threats and unusual system activity. Alerts for these events are tracked to resolution.

Authorization logs are continuously scanned for invalid commands and other invalid authentication events. Notifications are sent to the IT Operations team when monitoring events are triggered. Notable issues are documented and resolved.

Users with administrative access on servers are monitored by the Security team. Within Canvas, specific commands have been whitelisted by the Security team, and server administrators are permitted to run those commands outside of Security team monitoring. When commands that are not whitelisted are run by an administrator, the Security team is notified, and they investigate access appropriateness.

## INCIDENT MANAGEMENT

Management has established a Security Incident Response Policy outlining the process of identifying, prioritizing, communicating, assigning, and tracking incidents through to resolution. Security events and incidents are documented and evaluated in a ticketing system through to resolution in accordance with the Security Incident Response Policy. The Security team communicates incidents internally and externally. Incident details such as analysis, rating, impact, and resolution are documented.

The Security team tests the Incident Response Plan annually, via simulation or retrospective of an actual event. Lessons learned are incorporated into the plan. Instructure provides notification of security breaches to its customers as described in the Instructure Data Processing Addendum, or applicable customer contract.

## CHANGE AND CONFIGURATION MANAGEMENT

Canvas and Studio are continually being updated to meet user needs and to enhance both the functionality and the security of Canvas and Studio. Instructure employs an agile application development methodology. To help ensure changes are made in a controlled manner, Instructure has implemented controls related to the documentation, authorization, testing, and migration of code into the production environment.



Code changes may be initiated via customer request or feedback, or through internal initiatives. Ticketing systems and code review tools are in place to document code changes and any required data changes from identification through the development and deployment processes. Once the requirements are defined, a member of the Engineering team develops new code in a local development environment (Instructure maintains separate development, Quality Assurance (QA), and production environments). A peer developer then reviews the code. Upon review, the new code requires a documented peer approval that serves as authorization to move the change into the staging environment to undergo testing. This authorization is recorded in a custom-developed code review tool. Branch protections enforce peer review on code and configuration changes. Access to modify branch protection settings is restricted to the IT and SRE teams.

The Engineering team performs a QA review by testing application software, including code changes, through automated continuous integration (CI) scripts or manual testing. When a successful CI build has been accomplished, the code is ready to be released into production. The code is released via deploy scripts. Access to deploy changes to production environments is restricted to members of the Engineering and IT Operations teams.

Emergency code changes (hotfixes) follow the standardized code change process, including authorization and testing, but are released to production outside of the established release schedule.

Access to administer the source code management system is limited to members of the Engineering Operations, IT, and Systems Administration teams.

Configuration is managed as code, and as such, the peer approval and testing process applies to configuration changes as well as code changes.

## SYSTEM AVAILABILITY

Instructure has implemented controls and procedures to help ensure the availability of Canvas and Studio. Data backup procedures have been configured within AWS to run a daily full backup snapshot of Canvas and Studio databases. The Database team is alerted when backups fail, and any failures are tracked to resolution. These backups are retained in accordance with a defined retention schedule. Canvas and 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 4 months
- The most recent snapshot

The IT Operations team restores data backups to a non-production environment at least annually to validate their integrity.

As additional institutions and students use Canvas and Studio, Instructure has created a process to help support scalability over time. Application servers are also configured to automatically scale to customer demand. Application servers are configured to automatically scale to meet customer demand. Further, Instructure maintains a formal disaster recovery plan. The plan is tested at least annually through tabletop exercises.





## DATA MANAGEMENT

Instructure is committed to complying with its Data Classification, Handling, and Encryption Policy and the commitments made in the Terms of Service and Privacy Policy. Client data is retained for the duration the customer utilizes Canvas and Studio. Instructure retains and destroys customer data according to the Data Classification, Handling and Encryption Policy. Customers may request for the removal of their data. Requests from individuals or institutions to delete data are tracked via the internal ticketing system until the requested data is securely deleted. If the request is denied, the data subject is informed of the denial and informed of the reason for such denial.

Additionally, data validation checks are in place within Canvas and Studio to validate the completeness, integrity, timeliness, and authorization of the data received into the company environment. Errors from data inputs are returned to the end user to re-enter the data in the correct format.

Additional database layer and application security controls enforce the following access rules that prevent user accounts from viewing data other than their own:

- Unique account IDs and permissions restrict access at the application account level.
- Database shards map to unique schema to isolate database connections (Canvas and Studio).

## PRIVACY

Instructure provides the Instructure Product Privacy Notice publicly on Instructure websites. Instructure's Product Privacy Notice is included in the footer of Instructure's public-facing websites, as well as the Canvas application. The Product Privacy Notice includes provisions related to regional privacy law requirements including the US, European Union, Brazil, and the Australia-Pacific region. Instructure's Product Privacy Notice also includes provisions for:

- Purpose for collecting personal information
- Choice and consent
- Types of personal information
- Methods of collection
- Use, retention, and disposal
- Access
- Disclosure to third parties
- Security for privacy
- Quality, including customer responsibilities for quality
- Monitoring and enforcement

Instructure collects and uses personal information only to the limit allowable as outlined in the Product Privacy Notice by enforcing data elements collected at the application layer and backend database.





Instructure executes contractual commitments with vendors or third parties with access to personal information. These contracts require that vendors or third parties (a) comply with applicable data privacy laws world-wide related to the processing of personal information, (b) maintain appropriate administrative, technical, and operational controls related to the processing of personal information, (c) notify Instructure of any event that impacts the integrity, security, confidentiality, or privacy of personal information, (d) notify Instructure of an unauthorized use or disclosure of personal information, (e) provide Instructure audit rights for privacy and security controls, (f) comply with data subject access requests as required by Instructure, (g) notify Instructure of any third parties that process personal information, (h) only process personal information as described in the applicable services contract or data processing agreement, and (i) not transfer personal data to any unapproved regions.

Access to personal information is recorded in web application logs. Instructure's Customer Support team provides access to a data subject's personal data processed by Instructure and can provide a data extract of such personal data upon request by the data subject with approval by the applicable customer. If Instructure is unable to provide a copy of the requested personal information processing activities, either (a) Instructure's Customer Support team informs a data subject if their access request has been denied, or (b) Privacy team provides notification, or (c) Customer Support team refers the data subject back to their institution. End users are able to access or make corrections to their private data through the application.

Instructure's methods for collecting and processing personal information are reviewed at least annually to ensure those methods of collection are completed lawfully, and fairly. This review is completed by reviewing (a) internal privacy impact assessments, (b) vendor and third-party assessments, and or (c) internal personal data inventories.

Instructure's Vendor Data Processing Agreement requires that vendors or other third parties with access to personal information notify Instructure in the event of actual or suspected unauthorized disclosures of personal information. Incident notifications are sent to Instructure's Chief Information Security and Privacy Officer and evaluated in accordance with Instructure's Incident Response Policy.

The Instructure Legal team notifies customers (institutions) of material changes to the Instructure Product Privacy Notice via email. End users are notified via the "Global Announcements" function in the application.

## **B. Principal Service Commitments and System Requirements**

Instructure designs its processes and procedures to provide a secure environment for customer data. Instructure's security, availability, processing integrity, confidentiality, and privacy commitments and system requirements are documented and communicated to customers in the Terms and Conditions, Master Services Agreement, and at other resources listed below:

- Trust Center (<https://www.instructure.com/trust-center>)
- Instructure's Product Privacy Notice (<https://www.instructure.com/policies/privacy>)

Instructure's service commitments include, but are not limited to, the following:



- Data retention for at least 90 days after client termination
- Security training upon hire and annually thereafter
- Restricted logical access and strong authentication requirements
- Security threat monitoring
- Encryption in transit using TLS 1.2 or higher
- Encryption at rest
- Data replication

Compliance with the EU-US Privacy Shield Framework and Swiss-US Privacy Shield Framework

## C. Complementary Subservice Organization Controls

Instructure's controls related to the Canvas Learning Management System and Studio Video Learning Platform cover only a portion of overall internal control for each user entity of Instructure. It is not feasible for the criteria related to the Canvas Learning Management System and Studio Video Learning Platform to be achieved solely by Instructure. Therefore, each user entity's internal controls must be evaluated in conjunction with Instructure's controls, taking into account the types of controls expected to be implemented by the subservice organization as described below.

Complementary Subservice Organization Controls	
AWS, Elevate	
1	Access to hosted systems requires users to use a secure method to authenticate.
2	User content is segregated and made viewable only to authorized individuals.
3	Network security mechanisms restrict external access to the production environment.
4	New user accounts are approved by appropriate individuals prior to being provisioned.
5	User accounts are removed when access is no longer needed.
6	User accounts are reviewed on a regular basis by appropriate personnel.
7	Access modifications to hosted systems are approved by appropriate individuals prior to being provisioned.
8	Access to physical facilities is restricted to authorized users.
9	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.
10	Encrypted communication is required for connections to the production system.
11	Access to hosted data is restricted to appropriate users.
12	Hosted data is protected during transmission through encryption and secure protocols.
13	Anti-virus or anti-malware solutions are installed to detect or prevent unauthorized or malicious software.



Complementary Subservice Organization Controls	
14	System configurations changes are logged and monitored.
15	Vulnerabilities are identified and tracked to resolution.
16	Security events are monitored and evaluated to determine potential impact per policy.
17	Operations personnel log, monitor and evaluate to incident events identified by monitoring systems.
18	Operations personnel respond, contain and remediate incident events, and update stakeholders, as needed.
19	System changes are documented, tested, and approved prior to migration to production.
20	Access to make system changes is restricted to appropriate personnel.
21	Personnel monitor processing and system capacity on hosted systems.
22	Personnel execute and monitor daily backups. Any identified errors are resolved in a timely manner.
23	Environmental mechanisms provide protection over fire, water, power outages, temperature changes, and natural disasters.
24	Software and recovery infrastructure are implemented over hosted systems.

## D. Complementary User Entity Controls

Instructure's Canvas Learning Management System and Studio Video Learning Platform was designed under the assumption that certain controls would be implemented by the user entities for whom it provides its Canvas Learning Management System and Studio Video Learning Platform. In these situations, the application of specific controls at these user entities is necessary to achieve certain criteria included in this report.

This section describes additional controls that should be in operation at the user entities to complement the controls at Instructure. User auditors should consider whether the following controls have been placed in operation by the user entity.

Each user entity must evaluate its own internal control structure to determine if the identified user entity controls are in place. User entities are responsible for:

Complementary User Entity Controls	
1	For information requiring explicit consent, the user entity communicates with end users regarding the need for such consent and obtains the consent prior to the collection of information from the data subject.
2	Validating the completeness and accuracy of system outputs.

