



System and Organization Controls 3 (SOC 3) Report

**Description of Ellucian's  
Cloud Services System**

For the period April 1, 2020 to March 31, 2021

# Ellucian

## Service Organization Controls 3 Report Description of Ellucian's Cloud Hosting System

For the Period April 1, 2020 to March 31, 2021

### Table of Contents

<b>Management's Report of its Assertion on the Effectiveness of Its Controls over the Ellucian Cloud Services System Based on the Trust Services Criteria for Security, Availability, and Confidentiality .....</b>	<b>1</b>
<b>Report of Independent Accountants .....</b>	<b>2</b>
<b>Description of Ellucian's Cloud Services System throughout the period from April 1, 2020 to March 31, 2021 .....</b>	<b>4</b>
Company Overview .....	4
Customers .....	4
Boundaries of the System .....	4
Cloud-based Enterprise Applications .....	5
Complementary User Entity Controls .....	7



## **Management's Report of its Assertion on the Effectiveness of Its Controls over the Ellucian Cloud Services System Based on the Trust Services Criteria for Security, Availability, and Confidentiality**

May 12, 2021

We, as management of, Ellucian are responsible for:

- Identifying the Cloud Services (System) and describing the boundaries of the System, which are presented in Description of Ellucian's Cloud Services System throughout the period from April 1, 2020 to March 31, 2021
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in Description of Ellucian's Cloud Services System throughout the period from April 1, 2020 to March 31, 2021
- Identifying, designing, implementing, operating, and monitoring effective controls over the Application Hosting and Application Management System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion

Ellucian (Ellucian) uses Amazon Web Services (AWS) to provide physical safeguards and environmental safeguards. The Description includes only the controls of Ellucian and excludes controls of AWS, however it does present the types of controls Ellucian assumes have been implemented, suitably designed, and operating effectively at AWS. The Description also indicates that certain trust services criteria specified therein can be met only if controls AWS assumed in the design of Ellucian's controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of AWS.

However, we perform annual due diligence procedures for third-party sub-service providers and based on the procedures performed, nothing has been identified that prevents Ellucian from achieving its specified service commitments.

We assert that the controls over the system were effective throughout the period April 1, 2020 to March 31, 2021, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.



Ernst & Young LLP  
1775 Tysons Blvd  
Tysons, VA 22102

Tel: +1 703 747 1000  
Fax: +1 703 747 0100  
ey.com

## Report of Independent Accountants

To the Management of Ellucian

### *Scope:*

We have examined management's assertion, contained within the accompanying Management's Report of its Assertion on the Effectiveness of Its Controls over the Ellucian Cloud Services System Based on the Trust Services Criteria for Security, Availability, and Confidentiality (Assertion), that Ellucian's controls over the Cloud Services System (System) were effective throughout the period April 1, 2020 to March 31, 2021, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

### *Management's responsibilities*

Ellucian's management is responsible for its assertion, selecting the trust services categories and associated criteria on which the its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Ellucian Cloud Services System and describing the boundaries of the System
- Identifying our principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement

### *Our responsibilities*

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Ellucian's relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.



Our examination was not conducted for the purpose of evaluating Ellucian’s cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Ellucian uses Amazon Web Services (AWS) (subservice organization) to provide physical safeguards and environmental safeguards. The Description of Ellucian’s Cloud Services System throughout the period from April 1, 2020 to March 31, 2021 indicates that Ellucian’s controls can provide reasonable assurance that certain service commitments and system requirements, based on the applicable trust services criteria, can be achieved only if controls at AWS, assumed in the design of Ellucian’s controls, are suitably designed and operating effectively along with related controls at the service organization. The Description presents Ellucian’s system and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS. Our examination did not extend to the services provided by AWS and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period April 1, 2020 to March 31, 2021.

*Inherent limitations*

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Ellucian’s principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

*Opinion*

In our opinion, Ellucian’s controls over the system were effective throughout the period April 1, 2020 to March 31, 2021, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria, if the subservice organization applied the controls assumed in the design of Ellucian’s controls throughout the period April 1, 2020 to March 31, 2021.

*Ernst + Young LLP*

May 12, 2021  
Tysons, Virginia

## **Description of Ellucian's Cloud Services System throughout the period from April 1, 2020 to March 31, 2021**

### **Company Overview**

Ellucian (Ellucian or the Company) is a global company that develops software and services that higher education institutions use to deliver a modern, integrated experience in the cloud. Ellucian's cloud-based deployment models include Managed Cloud and Software-as-a-Service (SaaS).

The deployment of Ellucian Managed Cloud provides a secure and dedicated software instance on cloud infrastructure managed by Ellucian. With a SaaS deployment, Ellucian provides a fully managed shared software instance on cloud infrastructure. Both deployment options provide access to a high-quality data center, high performance internet connectivity, hardware and operating system support, security administration, and operational monitoring, including management of the database, operating system, and administrative applications.

The scope of this report includes only services related to Managed Cloud and SaaS and does not extend to other available Ellucian services. There have been no significant changes made or additional applications added to the scope of Cloud-based Enterprise Applications included within this report since the prior reporting period.

Ellucian, Inc. was founded in 1986 and is headquartered in Reston, Virginia with regional offices worldwide.

### **Customers**

Ellucian customers represent a range of educational institutions worldwide. More than 2,700 institutions in over 60 countries have selected Ellucian to improve operations and enhance the user experience for their faculties, staff, and over 20 million students.

### **Boundaries of the System**

This report provides a description of Ellucian's Cloud Services System relevant to Security, Availability and Confidentiality throughout the period from April 1, 2020 to March 31, 2021, (Description) based on the criteria for a description of a service organization's system set forth in the AICPA's TSP Section 100, 2017 *Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (description criteria).

The Description is intended to provide users with information about Ellucian's Cloud Services System (System), particularly system controls intended to meet the criteria for the security, availability and confidentiality criteria set forth in the AICPA's TSP Section 100, 2017, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Ellucian's System boundaries are defined as the processes supporting the deployment, administration, security, availability and confidentiality of the Cloud-based Enterprise Applications listed above and their supporting infrastructure.

## Cloud-based Enterprise Applications

Ellucian provides Cloud-based Enterprise Applications designed to specifically meet the needs of higher education and helps students, staff and faculty achieve their goals for student success, constituent experience, operational experience and institutional growth:

<b><i>Ellucian Banner</i></b>	Ellucian Banner is a higher education Enterprise Resource Planning (ERP) solution designed for complex higher education processes.
<b><i>Ellucian Colleague</i></b>	Ellucian Colleague is a higher education ERP solution that is only available in North America.
<b><i>Ellucian PowerCampus</i></b>	Ellucian PowerCampus is a higher education ERP solution designed for smaller institutions.
<b><i>Ellucian Elevate</i></b>	Ellucian Elevate is a SaaS solution designed to manage the continuing education and workforce development program for higher education institutions.
<b><i>Ellucian Quercus</i></b>	Ellucian Quercus is a student information system (SIS) designed for higher education institutions.
<b><i>Ellucian CRM Recruit</i></b>	Ellucian CRM Recruit is a student engagement solution designed to manage the recruiting and admission processes for higher education institutions.
<b><i>Ellucian CRM Advise</i></b>	Ellucian CRM Advise is a student engagement solution designed to manage the student intervention and retention program for higher education institutions.
<b><i>Ellucian CRM Advance</i></b>	Ellucian CRM Advance is a donor management solution designed to manage the fundraising program for higher education institutions.
<b><i>Ellucian Degree Works</i></b>	Ellucian Degree Works is an academic advising solution designed to manage the student planning, academic advising, degree audit and transfer equivalency processes for higher education institutions.
<b><i>Ellucian Intelligent Learning Platform</i></b>	Ellucian Intelligent Learning Platform (ILP) is an integration solution designed to streamline and manage multiple learning management systems (LMS) into a single platform.
<b><i>Ellucian Ethos Integration</i></b>	Ellucian Ethos Integration is an integration service designed to connect people, processes, and applications across the higher education institution.
<b><i>Ethos Analytics</i></b>	Ellucian Analytics is the business intelligence component of the Ethos platform designed to provide analysis, reporting and metric functionality for the platform.

<b><i>Ethos Identity</i></b>	Ellucian Identity component of the Ethos framework that provides the default identity management solution (single sign-on and secure authentication) for the platform.
<b><i>Ethos Data Access</i></b>	Ellucian Data Access is a component the Ethos framework that provides the central data store and APIs to store current and changed event history.

These applications are supported by a combination of Linux, Windows, Oracle, and SQL Server environments. Due to the customization offered, the operating system and database environments for each application vary from customer to customer.

### Sub-Service Organization

Ellucian uses Amazon Web Services (AWS) to provide cloud-based hosting services that support the Cloud Services System. The scope of the examination and the description include only the controls performed by Ellucian relevant to the achievement of the specified criteria and do not include controls of the third-party subservice organizations. The services provided by the subservice organizations relate to the Security and Availability principles and the following specific criteria that are intended to be met by the controls at the subservice organizations, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

<b>Criteria</b>	<b>Complementary Subservice Organization Controls at AWS</b>
<b>CC6.1:</b> The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	<p>IT access above "least privileged", including administrator access, is approved by appropriate personnel prior to access provisioning.</p> <p>IT access privileges are reviewed regularly by appropriate personnel.</p> <p>User access to systems is revoked timely upon termination.</p>
<b>CC6.4:</b> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	<p>Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware, is restricted to authorized individuals through a badge access system or equivalent and monitored by video surveillance.</p> <p>Requests for physical access privileges require management approval.</p> <p>Documented procedures exist for the identification and escalation of potential physical security breaches.</p> <p>Visitors must be signed in by an authorized workforce member before gaining entry and must be escorted at all times.</p>



Criteria	Complementary Subservice Organization Controls at AWS
<p><b>CC8.1:</b> The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.</p>	<p>Changes are authorized, tested, and approved prior to implementation.</p>
<p><b>A1.1:</b> The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.</p>	<p>Backups are appropriately scheduled, and completion status is being periodically monitored. Any failures are tracked, researched, and resolved timely.</p>
<p><b>A1.2:</b> The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.</p>	<p>Environmental protections have been installed including the following:</p> <ul style="list-style-type: none"> <li>• Cooling systems</li> <li>• Battery and generator backups</li> <li>• Smoke detection</li> <li>• Dry pipe sprinklers</li> </ul> <p>Environmental protection equipment receive maintenance on at least an annual basis.</p>

Management has a control over the annual review of the AWS SOC report which is evaluated as part of the SOC2 procedures.

### Complementary User Entity Controls

The complementary user entity (customer) control considerations listed below were developed based on the assumption that internal controls would be implemented by customer organizations. The application of such internal controls by customer organizations is necessary to meet certain applicable trust services criteria identified in this report. There may be additional criteria and related controls that would be appropriate for the processing of customer transactions that are not identified in this report.

Below is a description of certain controls that the customer organizations should consider to achieve the applicable trust services criteria identified in this report. The customer control considerations presented should not be regarded as a comprehensive list of all the controls that should be employed by customer organizations.

- Customers are responsible for designating a point of contact, whose role is to provide requisite customer resources and cooperation.
- Customers are responsible for testing system software changes applied to their environments and providing final written sign off on the requested changes to Ellucian.

- Customers are responsible for selecting a time frame for their weekly maintenance interval, during which time noncritical patches and other updates will be applied to hosted systems.
- Customers are responsible for the day-to-day user administration of the various software applications hosted. This includes designation of users' rights and privileges, determination of password policies, access to specific modules installed, and the timely removal of expired accounts and services.
- Customers are responsible for the management, periodic review, and timely notification of any access changes needed to customer accounts with access to their supporting infrastructure environments.
- Customers are responsible for requesting Ellucian to perform changes to thresholds per device type to trigger alerts for monitoring of the customers hosting environments.
- Customers are responsible for notifying Ellucian of any suspected incident or suspicious activity.
- Customers are responsible for providing accurate and complete data to Ellucian to configure a file transfer method, including secure FTP (SFTP), SSH, or FTP, over an SSL connection.