



**ELLUCIAN COMPANY L.P.**

**INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT**

**FOR**

**CLOUD SERVICES**

**FOR THE PERIOD OF APRIL 1, 2022, TO MARCH 31, 2023**

Attestation and Compliance Services



**Proprietary & Confidential**

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

## INDEPENDENT SERVICE AUDITOR'S REPORT

To Ellucian Company L.P.:

### *Scope*

We have examined Ellucian Company L.P.'s ("Ellucian") accompanying assertion titled "Assertion of Ellucian Company L.P. Service Organization Management" ("assertion") that the controls within Ellucian's Cloud Services system ("system") were effective throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that Ellucian's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality, (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Ellucian uses a subservice organization for cloud-based hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Ellucian, to achieve Ellucian's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

### *Service Organization's Responsibilities*

Ellucian 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 Ellucian's service commitments and system requirements were achieved. Ellucian has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Ellucian 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 systems 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. 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 Ellucian's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Ellucian'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.

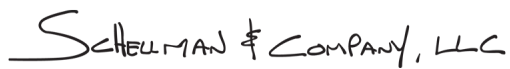
*Inherent Limitations*

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 Ellucian'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 Ellucian's Cloud Services system were effective throughout the period April 1, 2022, through March 31, 2023, to provide reasonable assurance that Ellucian's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

SCHHELLMAN & COMPANY, LLC

Washington, District of Columbia  
April 24, 2023

## ASSERTION OF ELLUCIAN SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Ellucian Company L.P.'s ("Ellucian") system ("system") throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that Ellucian's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented below 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 April 1, 2022, to March 31, 2023, to provide reasonable assurance that Ellucian's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Ellucian's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 April 1, 2022, to March 31, 2023, to provide reasonable assurance that Ellucian's service commitments and systems requirements were achieved based on the applicable trust services criteria.

# DESCRIPTION OF THE BOUNDARIES OF THE CLOUD SERVICES SYSTEM

## Company Background

Ellucian Company L.P. was founded in 1986 and is headquartered in Reston, Virginia with regional offices worldwide. Ellucian is charting the digital future of higher education with a portfolio of cloud-ready technology solutions and services. Serving more than 2,700 institutions in over 50 countries, reaching over 20 million students, Ellucian delivers student information systems (SIS), finance and HR, financial aid, integration, analytics, recruiting, retention, and advancement software solutions. Ellucian also supports the higher education community with a range of professional services that includes application software implementation, management consulting, and grants services.

Ellucian Cloud Services provides the technical infrastructure and support management services for the customer's Ellucian Cloud environment(s).

The Ellucian Cloud deployment options include:

- **Managed Cloud:** a secure and dedicated software instance deployed on cloud infrastructure managed by Ellucian.
- **Software-as-a-Service (SaaS):** a shared software instance on cloud infrastructure fully managed by Ellucian.

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 services. These services include the system and network infrastructure as well as software administration utilized to support the Managed Cloud environment and the multi-tenant SaaS deployments. Software development of the applications is the responsibility of dedicated research and development groups and is not included in the scope of this examination.

## Description of Services Provided

Ellucian provides cloud-based enterprise solutions and services specifically designed to 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. The portfolio of solutions and services includes:

### *Enterprise Resource Planning (ERP) and SIS solutions*

- **Banner:** a higher education ERP solution designed for complex higher education processes.
- **Colleague:** a higher education ERP/SIS solution that is only available in North America.
- **PowerCampus:** a higher education ERP solution designed for small to mid-sized institutions.
- **Quercus:** a SIS designed for higher education institutions.
- **Elevate:** a SaaS solution designed specifically for continuing education and workforce development program administrators.

### *Constituent Relationship Management (CRM) solutions*

- **CRM Recruit:** a comprehensive solution designed to support the higher education institution's entire recruiting and admissions lifecycle.
- **CRM Advise:** a comprehensive solution designed to support the higher education institution's entire advising lifecycle from orientation to commencement.

- CRM Advance: a donor management solution designed to manage the fundraising program for higher education institutions.
- Degree Works: an academic advising, transfer articulation, and degree audit solution designed to help students and their advisors negotiate an institution's curriculum requirements.

#### *Analytic and Integration Solutions*

- Ellucian Ethos: an integration service designed to connect people, processes, and applications across the higher education institution.
- Ellucian Ethos Identity: the identity component of the Ethos framework that provides the default identity management solution (single sign-on and secure authentication) for the platform.
- Ellucian Analytics: a guided business intelligence component of the Ethos platform designed to provide analysis, reporting and metric functionality for the platform.
- Ellucian Intelligent Learning Platform: an integration solution designed to streamline and manage multiple Learning Management Systems (LMS) into a single platform.
- Ellucian Experience Platform: a cloud-based, fully extensible user experience platform that delivers Ellucian solutions across the institution. Other Ellucian solutions are integrated with Ellucian Experience via Ethos integration.
- Ellucian Insights: a unified SaaS data platform that provides reporting, analytics, and extensibility tools within the Experience platform.

#### **System Boundaries**

Ellucian utilizes the cloud-based hosting services provided by Amazon Web Services (AWS). Ellucian's Cloud Services system is designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the control objectives related to Ellucian's Cloud Services system to be solely achieved by Ellucian's control activities. Accordingly, subservice organizations, in conjunction with the Cloud Services system, should establish their own internal controls or procedures to complement those of Ellucian.

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

Ellucian designs its processes and procedures related to the Cloud Services to meet its objectives. Those objectives are based on the service commitments that Ellucian makes to user entities, the laws and regulations that govern the provision of the Cloud Services, and the financial, operational, and compliance requirements that Ellucian has established for the services. The Cloud Services of Ellucian are subject to the security, availability, and confidentiality requirements of the state laws and regulations in the jurisdiction in which Ellucian operates.

The security, availability, and confidentiality commitments to user entities are documented and communicated to internal and external users via policies and procedures, customer contracts, and the Ellucian website. The principal security, availability, and confidentiality commitments are standardized and include the following:

- The use of logical access controls to safeguard the receipt, storage, and internal transfer of client data within the system boundaries.
- The maintenance of the information security program including Ellucian infrastructure, technical controls, processes, policies, and certifications.
- The development, testing, and maintenance of business continuity plans for critical functions.
- The retention and destruction of confidential data in accordance with defined Ellucian policies.

Ellucian has also established system requirements that support the achievement of the principal service commitments. These requirements include the following:

- The use of encryption technologies to protect system user data both at rest and in transit;
- Role-based access control with the principal of least privilege;
- Database management processes to ensure databases and supporting tables are loaded, maintained, and monitored for completion and performance;
- Change management procedures to support the requisite authorization, documentation, testing, and approval of changes; and
- A data deletion process run by the management team to ensure confidential data is removed after retention periods are met.

Such requirements are communicated in Ellucian system policies and procedures, system description documentation, data classification and handling policies and procedures, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Cloud Services.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

## **Infrastructure and Software**

Ellucian SaaS offerings utilize a single instance of products and services, and its supporting infrastructure serves multiple customers.

Ellucian Managed Cloud offerings are protected inside dedicated Amazon Virtual Private Cloud (VPC) infrastructure provided by AWS that are separate and unique from each other. Each VPC consists of dedicated service systems that support the products and services provided to the customer.

Ellucian utilizes a combination of Linux/Unix, Windows, Oracle, PostgreSQL, Unidata DB, and SQL Server systems to deliver its services. Due to the customization offered, the operating system and database environments for each application vary from customer to customer.

Production systems are located within AWS data centers. These data centers are strategically located in multiple availability zones around the world to provide resilient cloud computing services to Ellucian. The production systems are managed and monitored remotely by Ellucian personnel except for the physical and environmental security of the hardware devices, which is the responsibility of AWS.

## **People**

Management has developed and communicated to users, procedures related to the security, availability, and confidentiality of the Cloud Service system. Review of these procedures is performed periodically and any changes necessary are authorized by management prior to being implemented.

The procedures used to maintain the security posture of the system cover the following key areas:

- Executive Management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Global Information Security – responsible for the strategic direction, implementation, and continuous improvement of the overall information security program. This organization is comprised of the Security

Risk and Compliance; Security Architecture and Engineering; and Threat and Security Incident Management functions.

- Cloud – responsible for overseeing the Infrastructure Engineering and Operations, Database Engineering, and Cloud Application Assurance functions.
- Operations and Programs – responsible for overseeing the Cloud Service Design, Cloud Service Operations, Project Management, Service Report and Analysis, Site Reliability, and Cloud Customer Enablement functions.
- Global Support – responsible for overseeing the Action Line, Call Center Service, Incident Command Center, and Customer Experience Center functions.
- Human Resources (HR) – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).

## **Procedures**

### *Employee Hiring / Onboarding*

Candidates for employment including third-party contractors undergo a pre-employment screening process that includes resume screening, multiple rounds of interviews, and reference/background check, as applicable by law depending on the region. These background verification checks may include Social Security number, national identification number, employment history verification, criminal record, and educational background verification.

Upon hire, employees participate in new hire orientation and complete mandatory compliance training which includes Information Security training. As part of the new hire on-boarding process, employees receive a copy of Ellucian's Code of Conduct, which includes the Alert Hotline number for employees to report instances of fraudulent, unethical, or non-compliant behavior or activity. Employees are required to affirm acceptance of the Code of Conduct upon hire and on an annual basis.

Ellucian employees are trained regularly on security awareness and data protection requirements. Employees are required to acknowledge their understanding of and adherence to Ellucian's Code of Conduct, Information Security and Data Privacy policies upon hire and on an annual basis.

### *Employee Termination*

The HR department sends out employee termination notices to Corporate IT personnel in charge of terminations. Corporate IT personnel in charge of terminations receive this information via e-mail and create a termination ticket in the Ellucian tracking system on the day of and/or prior to the noted termination date.

Prior to the employee's termination date, HR sends an e-mail requesting that termination packets be sent to the appropriate management team members. These teams usually comprise the employee's immediate manager, the area/department's general manager, and the area/department's senior manager. If the employee is in possession of Ellucian owned equipment (mobile phone, laptop, desktop, or other computer equipment), a notification is sent to the employee's manager with a list of equipment assigned to the user in Ellucian's asset management tool. If the employee works remotely, Corporate IT requests that the mailroom send an empty box, including packing material and a preprinted return label, to the employee for the return of Ellucian-provided equipment.

Upon termination of employment, Corporate IT disables all access for the specified employee according to policy unless otherwise specified by HR or the employee's management team. This includes disabling the employee's network and security access.



### *Access Authentication and Authorization*

Ellucian has defined and documented security policies and procedures, including guidelines governing information security standards, password parameters, VPN access, and user administration. The policy is reviewed by management annually.

The Cloud organization has implemented operational policies and practices to help ensure Ellucian's assets are safeguarded and access to the company systems, application, databases, networks, resources, and data is secured. Documented operational policies and procedures are available to personnel on an internal web page accessible from the corporate intranet. Policies address access to Ellucian production systems, databases, and applications, including privileged user access, periodic access review, and access revocation upon termination or job transfer.

Ellucian uses Windows Active Directory (AD) technology to restrict access to the company's network through Lightweight Directory Access Protocol (LDAP). The cloud Active Directory domains are used to control access through AD group privileges to Ellucian resources, including supporting infrastructures and applications.

Ellucian users and customer accounts in a support role are required to authenticate to the Ellucian cloud environment using their cloud Active Directory user ID and password, as well as enter valid credentials to a VPN, before being granted access to their application or server.

Microsoft AD password settings are in place to control access to the operating system and hosting environment. The Ellucian password policy enforces the following settings:

- A minimum password length
- Password history
- Maximum password age
- Password complexity
- Account lockout after a predetermined number of failed attempts

Remote users are required to use a secure sockets layer virtual private network (SSL VPN) to connect to the Ellucian Cloud hosting environment. The VPN connection is restricted to authorized personnel and requires an Ellucian username / password enforced via multi-factor.

Access to privileged IT functions at the network, infrastructure, and application layers is restricted to appropriate members of the Ellucian cloud team.

### *Access Requests*

The cloud access authorization policy establishes standard criteria to provision, deprovision and recertify access to Ellucian's cloud Active Directory production environments. The policy is reviewed by management on an annual basis.

All regional domains are synchronized with the corporate Active Directory system. When a new employee is hired, the cloud Active Directory account and access privileges are automatically activated if the individual is a member of a team that is designated as needing access to the Ellucian cloud as part of their job role.

When an existing employee requires a cloud Active Directory user account and is not in a designated job role, a request is submitted within the IT Service Management (ITSM) system to be processed. Once approved by the appropriate manager or supervisor, the ticket is assigned to a cloud engineer to create the account and grant access.

### *Access Revocation*

All regional cloud domains are synchronized with the corporate HR system. The cloud Active Directory account and access privileges for terminated employees are automatically deactivated by a feed received from the corporate HR system.

When a cloud Active Directory user account needs to be manually deactivated, the requestor submits a request within the ITSM system to be processed. Once the ticket is approved by the appropriate manager or supervisor, it is assigned to a cloud engineer to disable access and close the ticket.

For customer accounts, a request for the removal of access is submitted to their designated Cloud Service Delivery Manager (CSDM). The CSDM creates a ticket in the ITSM system and assigns it to a Cloud Engineer to disable access and close the ticket. Each user identified in the review as having an expired password is e-mailed notifying them of the password status of their account. Ellucian Cloud management performs a review of inactive logins to identify customer accounts with passwords that have been expired for 90 days or more. Upon expiration, the account is disabled.

#### *Access Review*

Ellucian Cloud management performs a user access review of Ellucian cloud domain administrator accounts on a monthly basis to reconfirm whether access is appropriate. Access listings are generated and assigned to the manager of Cloud engineering within the ITSM system. The manager reviews the listings, indicates the required changes, and routes the ticket to the Cloud Engineer for processing. Upon completion the ticket is routed to the Senior Director of Cloud Engineering for approval.

On a semi-annual basis, cloud management performs a review of role-based assignments and service accounts to reconfirm whether access is appropriate. Access listings are generated and assigned to the appropriate manager or supervisor using the ITSM system. The manager, supervisor, or sponsor reviews their listings, indicates the required changes, and routes the ticket back to the cloud engineer to process the required changes and close the ticket.

#### *Change Management*

Ellucian Cloud has established a formal change enablement practice within Ellucian Cloud with clearly defined roles and responsibilities for creating, implementing, and maintaining an ITIL best-practice framework for change enablement.

The Ellucian Cloud Change Approval Board (CAB) will oversee and execute the change enablement practice as it applies to the products and services supported by the Cloud business unit. The CAB is composed of cross functional members of the Cloud business unit.

The Cloud Change Management Policy, which establishes standard criteria to identify, document and approve changes being made to the Ellucian cloud production environment has been established and is reviewed by management on an annual basis.

Changes to the infrastructure, environments and data centers which support the Ellucian service are managed through the cloud change management process. Changes are documented in an internal ITSM ticketing tool and the change documentation must include, but not limited to the following:

- How the change will be implemented
- Success criteria for the change
- Rollback procedures to return to the prior known good state
- Estimated duration of implementation
- Dependencies of the change, if applicable

Customers may request work through work planning efforts with their Ellucian contact directly through the Customer Center web portal which interfaces with the ITSM system, or they may call or e-mail their Ellucian contact. Customer work is planned through projects. Customer approval, for specific maintenance, is provided through project tasks. Once the planning and customer approval is completed, the ITSM request for change details is automatically created from the project task.

Change requests are assigned a change type of Normal, Standard, or Emergency, based on the risk and impact on the production environment, in accordance with the change management policy and procedures.

Normal changes are requests that are not standard or emergency changes and need to be scheduled, assessed, and authorized via the CAB. Normal changes must undergo a risk assessment and peer review where the team analyzes the change within the scope of the assignment and assesses its viability. Upon completion of the peer review, a manager or CAB member reviews the change and adds approval to the ITSM ticket, validating that the change is appropriately authorized, developed, tested and ready to migrate.

Standard changes are pre-defined, low-risk, low impact changes that are added to the Standard Change catalog upon approval by the CAB.

Emergency changes do not follow the complete life cycle of a normal change due to the speed with which they must be authorized by the change authority.

All production changes require authorization before being implemented except for Emergency changes which can be approved by the Assignment Group Manager after the fact when associated with an unplanned outage event.

After the appropriate change authorization is obtained, the change is migrated to the customer's production environment by an appropriate administrator. Administrative access required to implement system changes into the production environment is restricted to authorized individuals who require such access to perform job responsibilities.

### *Data Transmission and Encryption*

Ellucian has defined and documented policies relating to transmitting data between Ellucian, customer organizations, and any applicable third parties. The policy is reviewed by management on an annual basis.

Customers receiving Cloud Managed Services are set up with a secure encryption tunnel between their organizations and Ellucian's cloud hosting environment end point and/or using peering connections that are managed by AWS security groups. Ellucian and its customers use an extranet-based, site-to-site VPN connection to provide a secure and reliable private connection and/or peering that is managed by AWS security groups between Ellucian's cloud hosting environment end point and each entity's computer network. The security routers function as a bidirectional tunnel endpoint, allowing for the encryption and decryption of data, as necessary, to send and receive data through the established encryption tunnel between Ellucian and its customer.

When a new customer is being set up, Ellucian will send the customer a template, including a diagram of the site-to-site connection, instructions on how to configure customer firewall ports/protocols, and a request for specific router configuration information and resource networks. The customer is responsible for providing accurate and complete information to Ellucian to establish the appropriate connections.

Network requirements (including permitted network rules, ports, and protocols) are documented within the customer's Server Network Build (SNB) and for newer customers the customer configuration is managed in code defined deployments. Changes are documented and follow the cloud operations change management process. For a standard configuration modification, a request is assigned to cloud operations to review and approve prior to the change being implemented. For a new configuration or non-standard configuration modification, an ITSM ticket is assigned to the appropriate infrastructure/architecture team to review, approve, and update the customer's SNB or appropriate source control prior to the change being implemented by the cloud engineering team.

Once data passes through to the internal Ellucian network, the data is routed to the appropriate customer server, based on the settings configured in the firewalls and routers. Customer data is segregated internally by Ellucian to allow only customers to view and access their own data.

Customer data transmissions and connections are monitored in real time by the Ellucian network group via the monitoring application. If an issue is noted, a ticket is automatically created within the ITSM system, where it is worked through to resolution.

Ellucian cloud solutions use strong encryption when data is being transmitted from the hosted environment end point to the customer site-to-site router. These standards are continuously evaluated to ensure that any changes to their effectiveness or security are addressed and quickly remediated in the environments. Advanced application data encryption is also an option for customers. This enables customers to encrypt sensitive application data on storage media completely transparent to the application.

### *Data Backup and Disaster Recovery*

Ellucian has defined and documented policies relating to backup and storage of database and application data, which are reviewed by management on an annual basis.

Ellucian leverages multiple backup tools and strategies designed to fit the needs of each application and service offering. Backups are configured based on server role and run on a schedule in accordance with corporate policy and individual customer contractual requirements.

Server level backups are performed through volume snapshot and image generation. The creation and retention of the volume snapshots and images correspond to the established contractual data retention policies.

In the unlikely event that a backup fails, the software is configured to automatically rerun the job and generate an automated alert to the cloud teams with details on the failure and action taken by the system. The issue is then worked through to resolution by a member of the cloud team, who documents the resolution in an ITSM ticket. However, in the event that an AWS Elastic Container Service (ECS) instance is in use in the production environment, Ellucian employs an infrastructure-as-code approach to address the availability of the resource such that in the event of a failure, the instance can be decommissioned and redeployed seamlessly via an automated tool.

Policies and procedures are in place to guide personnel in the areas of business continuity and disaster recovery. Test plans are formally documented, and include an outline of the requirements for testing, as well as the responsibilities of the various personnel involved in the tests. The test plans themselves are reviewed, and updated if required, on an annual basis. Additionally, disaster recovery tests are performed on an annual basis, in line with the test plans described above. Test results are documented and communicated to management, along with formal recommendations based on the results of testing.

### *Incident Response*

Ellucian has defined and documented policies relating to incident management and monitoring. The policy is reviewed by management on an annual basis.

Ellucian maintains communication channels for customers to report any issue which disrupts or could disrupt an existing service or has the potential to cause an information security incident. Customers can notify Ellucian of any suspected incident or suspicious activity by contacting the action line, their Customer Success Manager (CSM), Cloud Service Delivery Manager (CSDM) or other Ellucian point of contact.

If the customer reports an information security related issue, the Ellucian point of contact will escalate the issue by contacting the information security incident hotline which triggers Ellucian's incident response process.

Customer applications and servers are monitored in real time by members of the cloud delivery team for performance and availability issues through the automated monitoring software programs. The applications monitor service availability, including the network availability, CPU/disk utilization, application statistics, log files, and URL sequence checks. Ellucian defines thresholds per device type to trigger alerts, which are then configured by Ellucian within the application. Requests to define or change thresholds are documented in an ITSM ticket.

If an issue is detected by the monitoring system, the system is configured to automatically create an ITSM ticket assigned to a member of the cloud delivery team who verifies that there is an issue and assigns the ticket to an appropriate technician to be resolved. The assigned technician then appropriately resolves the incident and sets the ticket status to resolved.

If the customer reports a Priority 1 (critical) outage, the Ellucian point of contact will escalate the issue which triggers Ellucian's incident response process. Once a resolution has been reached and the ticket is updated, the customer is sent an e-mail notification of the resolution. A customer who is not satisfied with the resolution may click on a link in the e-mail to write a comment and request to reopen the ticket for further resolution. If the resolved ticket is not reopened within seven days, the ticket is automatically set to closed.

Ellucian's cloud incident management team will open an ITSM problem ticket as a means to track problem resolution for Priority 1 (critical) ITSM incident tickets categorized as customer outage in accordance with the cloud problem

management process guide. If required, a postmortem report will be generated for those problem records that are identified as requiring further root cause analysis.

### *Application Security*

Ellucian applications are created following a Secure Software Development Life Cycle (SDLC) that integrates the Open Web Application Security Project (OWASP) for software development. Ellucian has established a Secure Software Development Standard, which provides requirements for security controls and practices related to software development and maintenance activities at Ellucian. Through the use of this Secure SDLC, potential software application flaws or defects are addressed during application development and maintenance. Coupled with functionality and security-based testing, Ellucian ensures that security and performance are delivered with each solution.

The Application Security team has established an application security testing policy and framework that is comprised of security testing tools and/or techniques that are integrated into Ellucian's software development lifecycle. Automated static and dynamic application security testing tools are embedded into the DevOps pipeline. Vulnerabilities identified from the automated security tools, bug bounty program, and compliance penetration tests are imported and managed in a software vulnerability aggregation and management solution.

The Application Security team utilizes this solution to classify, review, monitor and resolve critical vulnerabilities in accordance with Ellucian's Vulnerability Management Standard. Ellucian has implemented the Cloud Readiness and Acceptance Criteria Checklist which establishes the DevOps, CloudOps, and Global Information Security teams minimum set of acceptance criteria that must be completed by the relevant team for every product being released to production. A completed copy of the checklist is attached to the ITSM change request and follows the standardized change management process described above. The Cloud Release Deployment team is responsible for validating that relevant checklist items (includes valid Golden Amazon Machine Images (AMI), security testing and vulnerability remediation) have been completed before deploying any update into a production environment.

Ellucian segments production and non-production environments. For Cloud Managed Service customers, each environment (dev, test, stage, prod) is designated by separate AWS accounts that are comprised of separate URL and login. Each account is used for a separate purpose in accordance with Ellucian's Operations Security Standard. Ellucian teams with appropriate access utilize Ellucian's SSO portal to gain access to specific customer accounts and environments within AWS. Ellucian requires the use of anonymized data within the system test environments for system and performance testing.

### *Perimeter Security*

Ellucian practices defense-in-depth with host-based and network-based technology to protect customer systems and data. Through use of AWS security group rules, host-based configuration, and account segmentation, Ellucian provides protection from unauthorized access of customer hosted systems and data.

### *Endpoint Security*

Ellucian systems are protected by an enterprise level antivirus/antimalware solution that provide continuous, up-to-date signature and behavior-based protection for relevant system platforms. Ellucian has implemented a continuous vulnerability identification and remediation process to address the newest emerging threats to systems and software are addressed efficiently. Through the use of enterprise level vulnerability tools to support this process, Ellucian can quickly identify and remediate vulnerabilities found in software and configurations.

Ellucian utilizes Golden AMIs to deploy secure configurations and the required tools for endpoint protection and asset management. Established procedures are in place for building and deploying the Golden AMI baseline images. Changes to the Golden AMIs are managed through the change management process described above.

Coupled with Ellucian's Vulnerability Management program, patch management utilizes an enterprise level patching solution for all layers of the system from OS to database to application. The solution is used for standard operational patching or for immediate zero-day threats.

Ellucian Global Information Security globally employs a Security Information and Event Management (SIEM) solution that captures, indexes, and correlates real-time data to identify potential threats and security events in the Ellucian environments.

## Data

Ellucian defines customer data as the electronic data or information submitted by the customer to the Ellucian system. Customer data is classified as restricted information. Established policies and procedures are in place for labeling, handling, and the security of customer information. Access to handling of restricted information is strictly managed through the use of physical and logical access.

The following table describes the information used and supported by the system.

Classification Type	Risk from Disclosure	Description	Examples
Public	None	Information which is in the public domain.	<ul style="list-style-type: none"> <li>Public websites / portal login pages</li> <li>Information approved for public release</li> </ul>
Confidential	Medium	Information that does not qualify as Restricted and that has not been approved for public disclosure.	<ul style="list-style-type: none"> <li>Application architectures</li> <li>System configurations</li> <li>Software version, license keys</li> <li>Source code</li> </ul>
Restricted	High	Information protected from general access, governed by applicable statutes, regulations, or contractual language.	<ul style="list-style-type: none"> <li>Personal data or Personal Identifiable Information (PII)</li> <li>Student records</li> <li>Access credentials</li> <li>Authentication secrets</li> </ul>

## Subservice Organizations

The cloud-based hosting services provided by AWS were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, alone or in combination with controls at Ellucian, and the types of controls expected to be implemented at AWS to meet those criteria.

Control Activities Expected to be Implemented by AWS	Applicable Trust Services Criteria
AWS is responsible for ensuring operational procedures are in place within the hosting and data center facilities over physical assets to prevent processing errors and/or unexpected interruptions and support the complete, accurate, and timely processing of operations.	CC6.1
AWS is responsible for ensuring physical access to computer and other resources to confirm it is restricted to authorized and appropriate personnel.	CC6.4
AWS is responsible for ensuring infrastructure changes are authorized, tested, and approved prior to implementation.	CC8.1
AWS is responsible for ensuring data backup processes and recovery infrastructure are designed, developed, and implemented, including automated backup systems are in place to perform scheduled backups and alerting notifications.	A1.2

## **Complementary Controls at User Entities**

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

## **Complementary Control Responsibilities at User Entities**

Ellucian's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

However, in order for user entities to benefit from the Cloud Services system and its controls, the following responsibilities should be considered by user entities:

- 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 submitting change requests to Ellucian to opt-out/decline planned maintenance window for Managed Cloud environment.
- 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 providing accurate and complete data to Ellucian to configure a file transfer method, including secure FTP (SFTP), SSH, or FTP, over an SSL connection.

## **Trust Services Criteria Not Applicable to the In-Scope System**

All criteria within the security, availability, and confidentiality categories are applicable to the Cloud Services system.