Higher Education Cloud Vendor Assessment Tool

Version 1.06

HEISC Shared Assessments Working Group

DATE-01	**Date**	□□

General Information

In order to protect the Institution and its systems, vendors whose products and/or services will access and/or host institutional data must complete the Higher Education Cloud Vendor Assessment Tool (HECVAT). Throughout this tool, anywhere where the term data is used, this is an all-encompassing term including at least data and metadata. Answers will be reviewed by Institution security analysts upon submittal. This process will assist the institution in preventing breaches of protected information and comply with Institution policy, state, and federal law. This is intended for use by vendors participating in a Third Party Security Assessment and should be completed by a vendor. Review the *Instructions* tab for further guidance.

GNRL-01 through GNRL-06; populated by Institution		
GNRL-01	Institution Department	*Institution Department Name*
GNRL-02	Institution Department Primary Campus	*Primary Campus*
GNRL-03	Institution Department Code	*Institution Department Code*
GNRL-04	Institution Department Contact Name	*Institution Department Contact Name*
GNRL-05	Institution Department Contact Email	*Institution Department Contact Email*
GNRL-06	Institution Department Contact Phone Number	*555-555-5555*
GNRL-07 through GNRL-14; populated by Vendor		
GNRL-07	Vendor Name	*CollegeSource Inc.*
GNRL-08	Product Name	*uAchieve Cloud*
GNRL-09	Product Description	*Degree audit, batch audit processing, academic planning*
GNRL-10	Web Link to Product Privacy Notice	www.collegesource.com
GNRL-11	Vendor Contact Name	*Ayman Rabi*
GNRL-12	Vendor Contact Title	*Vice President, Services & Support*
GNRL-13	Vendor Contact Email	*Ayman@CollegeSource.com*
GNRL-14	Vendor Contact Phone Number	*513-834-8770*
GNRL-15 and GNRL-16; populated by Institution Security Office		
GNRL-15	Institution Security Analyst/Engineer	*Institution Security Analyst/Engineer Name*
GNRL-16	Assessment Contact	*ticket#@yourdomain.edu*

Higher Education Shared Assessments Confirmation		Vendor Answers	Additional Information	Guidance
By completing the Higher Education Cloud Vendor Assessment Tool, cloud service providers understand that the completed assessment may be shared among higher education institutions. **Answers to the following statements will determine how this assessment may be shared within the Higher Education community**. Shared assessment sharing details can be found on the "Sharing Read Me" tab.				
HESA-01	I understand the goal of Higher Education Shared Assessments and that the completed Higher Education Cloud Vendor Assessment Tool may be shared with other higher education institutions, based on the following selections.	Yes		
HESA-02	Add this completed assessment to a list of Higher Education assessed service providers, with contact information for service providers. No answers are shared; it is a list stating vendor, product, version, and service provider contact information.	Yes; OK to List	Scope: Higher Education Institutions Only	

HESA-03	This completed Vendor Assessment Tool (with vendor answers intact) can be shared within Higher Education institutions through the Cloud Broker Index, https://www.ren-isac.net/hecvat/cbi.html.	No; Sharing Disallowed	Scope: Higher Education Institutions Only	
HESA-04	The security report created by this Higher Education institution, after evaluating this assessment, can be shared within Higher Education institutions.	No; Sharing Disallowed	Scope: Higher Education Institutions Only	
Instructions				
Step 1: Complete the *Qualifiers* section first. **Step 2:** Complete each section answering each set of questions in order from top to bottom; the built-in formatting logic relies on this order. **Step 3:** Submit the completed Higher Education Cloud Vendor Assessment Tool (HECVAT) to the Institution according to institutional procedures.				
Qualifiers		**Vendor Answers**	**Additional Information**	**Guidance**
The Institution conducts Third Party Security Assessments on a variety of third parties. As such, not all assessment questions are relevant to each party. To alleviate complexity, a "qualifier" strategy is implemented and allows for various parties to utilize this common documentation instrument. **Responses to the following questions will determine the need to answer additional questions below**.				
QUAL-01	**Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?**	No		Responses to the questions in the HIPAA section are optional.
QUAL-02	**Does the vended product host/support a mobile application?** (e.g. app)	No		Responses to the questions in the Mobile Application section are optional.
QUAL-03	**Will institution data be shared with or hosted by any third parties?** (e.g. any entity not wholly-owned by your company is considered a third-party)	No		Responses to the questions in the Third Parties section are optional.
QUAL-04	**Do you have a Business Continuity Plan (BCP)?**	Yes		You are required to complete the questions in the Business Continuity section.
QUAL-05	**Do you have a Disaster Recovery Plan (DRP)?**	Yes		You are required to complete the questions in the Disaster Recovery section.
QUAL-06	**Will data regulated by PCI DSS reside in the vended product?**	No		Responses to the questions in the PCI DSS section are optional.
QUAL-07	**Is your company a consulting firm providing only consultation to the Institution?**	No		Responses to the questions in the Consulting section are optional.
Documentation		**Vendor Answers**	**Additional Information**	**Guidance**
DOCU-01	Have you undergone a SSAE 16 audit?	Yes	A SOC 1, Type 2 was conducted on Oct. 1, 2016.	Provide the date of assessment and include a SOC 2 Type 2 (preferred) or SOC 3 report. If you have a SOC3 report, include a URL for the published report.
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?	Yes	https://aws.amazon.com/compliance/csa/ (May 2017)	Please include a copy with your response and include a URL for the published assessment.
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	Yes	https://aws.amazon.com/compliance/csa/ (May 2017)	Provide date of certification, any supporting documentation, and a URL for the certification.

DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Special Publication 800-53, ISO 27001, etc.)	Yes	ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015. Attached documentation.	Provide documentation on how your organization conforms to each framework and indicate current certification levels where appropriate.
DOCU-05	Are you compliant with FISMA standards (indicate at what level)?	Yes	https://aws.amazon.com/compliance/fisma/	Indicate level, agency issuing ATO, and necessary details on ATO. If using FEDRamp, please indicate the supporting details.
DOCU-06	Does your organization have a data privacy policy?	Yes	https://clients.collegesource.com/home/display/UC/Data+Privacy+Policy	Provide your data privacy document upon submission.
Company Overview		**Vendor Answers**	**Additional Information**	**Guidance**
COMP-01	Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.	In 1971, Harry G. Cooper founded the National Microfilm Library to scan U.S. college catalogs onto microfiche. Over time, the name was changed to the Career Guidance Foundation, a non-profit organization providing the same service and adopting the broader mission of providing technology solutions to promote higher student retention rates and a seamless path to post-secondary credentials. In 2003, the company incorporated as CollegeSource. In the spring of 2009, CollegeSource acquired redLantern, LLC and its degree audit, degree planning, and transfer articulation products from Miami University. Since then, redLantern was merged into CollegeSource as its Cincinnati office. Today, CollegeSource currently employs 90 individuals with 49 working out of the San Diego, California, office and 41 working out of the Cincinnati, Ohio, office.		
COMP-02	Describe how long your organization has conducted business in this product area.	See above.		
COMP-03	How many higher education, commercial customers and government customers do you serve in North America? Please provide a higher education customer reference if available.	CollegeSource serves over 2,000 institutions of higher education in the United States and Canada.		
COMP-04	Please explain in detail any involvement in business-related litigation in the last five years by your organization, its management, or the staff that will be providing the administrative services.	No litigation has arisen in the last five years. One piece of minor, ongoing litigation over data rights not relative to uAchieve was initiated by CollegeSource and resolved over two years ago without damages or complications.		
COMP-05	Describe the structure and size of your Security Office and overall information security staff. (e.g. Admin, Engineering, QA/Compliance, etc.)	See response to COMP-06 below. With the initial launch of uAchieve Cloud in June and as customers migrate to the Cloud, technical support and security will expand accordingly to serve our customer base. The choice of AWS as the platform for uAchieve Cloud was predicated on the extent of security and backup/recovery associated with AWS.		
COMP-06	Describe the structure and size of your Software and System Development teams. (e.g. Customer Support, Implementation, Product Management, etc.)	Our technical staff associated with product development, implementation, and support is encompassed in two departments: Product Development and Services/Support. Fourteen team members in Product Development include a Vice President, Product Managers, Developers, User Experience Lead, QA Specialists, and a Technical Writer. In Services/Support, thirteen team members include a Vice President, Project Managers, Programmer/Analysts, and Implementation Specialists. While there is no dedicated Security department, members from both of the aforementioned multi-disciplinary teams are involved with security--from product inception through implementation and system monitoring--with at least two developers assigned to each product handling security.		
COMP-07	Use this area to share information about your environment that will assist those who are evaluating you company data security safeguards.	Amazon Web Services was purposely chosen as the cloud platform given the extensive security and backup/disaster recovery proctocols they have in place, with artificats available related to environment, security, etc. As specific questions arise, we work with schools to direct them to artifacts associated with their concerns.		
Third Parties - Optional based on QUALIFIER response.		**Vendor Answers**	**Additional Information**	**Guidance**

THRD-01	Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.			
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.			
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?			
THRD-04	Describe or provide references to your third party management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.			
Consulting - Optional based on QUALIFIER response.		**Vendor Answers**	**Additional Information**	**Guidance**
CONS-01	Will the consulting take place on-premises or remotely?			
CONS-02	Will the consultant require access to Institution's network resources?			
CONS-03	Will the consultant require access to hardware in the Institution's data centers?			
CONS-04	Will the consultant require an account within the Institution's domain (@*.edu)?			
CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?			
CONS-06	Will any data be transferred to the consultant's possession?			
CONS-07	How long will it remain in their possession?			
CONS-08	Is it encrypted (at rest) while in the consultant's possession?			
CONS-09	Will the consultant need remote access to the Institution's network or systems?			

CONS-10	What software will be used to facilitate that access?			
CONS-11	Can we restrict that access based on source IP address?			
Application/Service Security		**Vendor Answers**	**Additional Information**	**Guidance**
APPL-01	Does the application/service support being virtualized?	Yes	uAchieve suite requires Java and can run on a Tomcat web container connecting to a relational database. All the components can be virtualized.	Describe any infrastructure dependencies.
APPL-02	Are the servers hosting institution data currently deployed in a virtualized environment?	Yes	AWS EC2 instances and AWS Relational Database Service (RDS)	Describe the utilized technology.
APPL-03	Can user access be customized to allow read-only access, update access, or no-access to specific types of records, record attributes, components, or functions?	Yes	uAchieve suite web applications access are role-based. The applications will check users permissions before granting access. Access can be denied, read-only, and read-write based on user permissions and configured application permissions.	If available, submit documentation and/or web resources.
APPL-04	Describe or provide a reference to how user security administration is performed?	Access to the applications is driven by client user management systems. Access to AWS console is strictly controlled by CollegeSource team using Multi-Factor Authentication (MFA).		
APPL-05	Define the access control roles of employees that will have access to the data and in what capacity.	CollegeSource has two types of users that will be accessing data in the Cloud Environment: Functional Users and Technical Users. Functional users will have access to the Encoding Data and Student Data that is used to generate degree audits. Technical Users will have access to all data within the system for debugging purposes.		
APPL-06	Do you allow employees to remotely access data (i.e. work from home)?	Yes	Employees must use the built-in application security of uAchieve suite for access or AWS console or SSH into non-production servers. For the AWS console, MFA is utilized as well as user id and password. For non-prod SSH, a private key is required for the instances to connect. SSH is enabled only for known employee IP addresses.	
APPL-07	Define what controls are in place to secure their remote environment and connection to the institution's data.	Access to the cloud environment is open to IP addresses within CollegeSource's Office Network and strictly controlled IP adresses defined in the AWS console. Environment access outside of defined IP addresses and ranges is denied. For the AWS console, MFA is utilized as well as user id and password. For non-production SSH, a private key is required for the instances to connect. SSH is enabled only for known employee IP addresses.		
APPL-08	What operating system(s) is/are leveraged by the system(s)/application(s) that will have access to institution's data?	Linux will be used for any EC2 instances accessing institution data. Windows 10 and Mac are used for accessing the uAchieve environment from user laptops and AppStream.		List all operating systems and the roles that are fulfilled by each.
APPL-09	Have you or any third party you contract with that may have access or allow access to the institution's data experienced a breach?	No		

APPL-10	Describe or provide a reference to additional software/products necessary to implement a functional system on either the backend or user-interface side of the system.	None		Describe the products and how they will be implemented.
APPL-11	Describe or provide a reference to the overall system and/or application architecture(s), including appropriate diagrams. Include a full description of the data communications architecture for all components of the system.	See the "uAchieve Tech Stack" tab		
APPL-12	Are databases used in the system segregated from front-end systems? (e.g. web and application servers)	Yes	The uAchieve Suite architecture is composed of web applications running on a web server. The uAchieve engine runs on an application server and uAchieve database runs in AWS RDS.	Provide a brief description.
APPL-13	Describe or provide a reference to all web-enabled features and functionality of the system (i.e. accessed via a web-based interface).	Degree audit and academic planning functionality for the uAchieve Cloud is similar to that available with the locally installed version of uAchieve used at the university today. However, migrating to uAchieve Cloud will include an upgrade to the most current release of uAchieve, which will contain new features (as detailed in the release notes section of the CollegeSource Support Center: https://clients.collegesource.com/home/display/STAT/Release+Notes). The only functionality not accessible via web-based interface is degree audit encoding: adding and maintaining degree requirements in the system. Encoding is maintained through the uAchieve Client, a Windows-based app installed on the desktop for the handful of users at each school who perform the encoding. The uAchieve Client is in use with the university's on prem installation of uAchieve today; with uAchieve Cloud, the uAchieve Client will no longer need to be installed on the desktop of the school's encoders since it will be accessible via browser.		Include user-end and adminstrative features and functionality.
APPL-14	Describe or provide a reference to any OS and/or web-browser combinations that are not currently supported.	uAchieve is operating system-independent. For desktop/laptops, all major browsers are supported (Firefox, Chrome, Safari, Internet Explorer/Edge). For mobile devices, only Safari and Chrome are supported.		
APPL-15	Can your system take advantage of mobile and/or GPS enabled mobile devices?	No		
APPL-16	Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and system administration functions.	AWS handles the physical security.		
APPL-17	Describe or provide a reference that details how administrator access is handled (e.g. provisioning, principle of least privilege, deprovisioning, etc.)	AWS handles the physical security. AWS adds and removes servers and storage as needed without any knowledge of which client is using what.		
APPL-18	Does the system provide data input validation and error messages?	Yes	The uAchieve web applications validates user input durin sign-ins, as well as all other values needed to complete application functions. Error messages are displayed where appropriate, and in system log files at the server and database levels.	If available, submit documentation and/or web resources.
APPL-19	Do you employ a single-tenant or multi-tenant strategy in the environment hosting Institution's data?	Multiple-tenant	Multiple-tenant strategy is employed by default, but single-tenant is available at an additional cost.	

APPL-20	Describe or provide references explaining how tertiary services are redundant (i.e. DNS, ISP, etc…).	AWS uses Multi-AZ configurations to ensure separation and redundancy, when needed. Other services used include Route 53, S3 buckets, application load balancers, and autoscaling groups. All services provided by AWS are spread across multiple locations and guaranteed to work, when needed.		

Authentication, Authorization, and Accounting		Vendor Answers	Additional Information	Guidance
AAAI-01	Can you enforce password/passphrase aging requirements?	Yes	User access to Web applications relies on the Client User Management System; any policies that the client is currently able to enact is represented in the uAchieve System.	
AAAI-02	Can you enforce password/passphrase complexity requirements [provided by the institution]?	Yes	User access to Web applications relies on the Client User Management System; any policies that the client is currently able to enact is represented in the uAchieve System.	
AAAI-03	What are the minimum and maximum password lengths supported, and what types of characters are supported?	User access to Web applications relies on the Client User Management System; any policies that the client is currently able to enact is represented in the uAchieve System.		
AAAI-04	Describe the current/default/supported password/passphrase reset procedures?	User access to Web applications relies on the Client User Management System; any policies that the client is currently able to enact is represented in the uAchieve System.		
AAAI-05	Describe or provide a reference to the types of authentication, including standards-based single-sign-on (SSO, InCommon), that are supported by the web-based interface?	The types of authentication supported by the web-based interface include CAS, Shibboleth, LDAP, and Federated SAML.		Include user-end and adminstrative authentication types.
AAAI-06	Are there any passwords/passphrases "hard coded" into your systems or products?	No	No hardcoded passwords are in the code of uAchieve.	
AAAI-07	Are user account passwords/passphrases visible in administration modules?	No	User access to Web applications reliess on the Client User Management System; any policies that the client is currently able to enact is represented in the uAchieve System.	
AAAI-08	Are user account passwords/passphrases stored encrypted?	Yes	Any password information is encrypted when passed to the application, but no password data is stored as part of the authentication process in any of the supported security implementations.	
AAAI-09	Describe or provide a reference to the algorithm/strategy that is used to encrypt stored passwords/passphrases?	N/A		
AAAI-10	Does your *application* and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)	No	The base product does not support DUO authentication. However, should the client use a SSO that is DUO compliant, then it will work as expected.	Describe any plans to provide Duo support.
AAAI-11	List all supported multi-factor authentication methods, technologies, and/or products and provide a brief summary of each.	The base product does not support multi-factor authentication. However, should the client use a SSO that is multi-factor authentication compliant, then it will work as expected.		
AAAI-12	Does your *application* support integration with other authentication and authorization systems such as Active Directory, Kerberos (what version) or another institution centralized authorization service?	Yes	Active Directory	Provide a brief description.

AAAI-13	Will any external authentication or authorization system be utilized by an application with access to the institution's data?	No		
AAAI-14	Does the *system* (servers/infrastructure) support external authentication services (e.g. Active Directory, LDAP) in place of local authentication?	No	Only web applications can work with Client User Management System.	
		No		
AAAI-17	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?	Yes	Access Audit logs are generated with each transaction in the application, which include IP address and action performed (including login and logout events).	Provide a description, if necessary.
AAAI-18	Describe or provide a reference to the system capability to log security/authorization changes as well as user and administrator security (physical or electronic) events (e.g., login failures, access denied, changes accepted), and all requirements necessary to implement logging and monitoring on the system. Include information about SIEM/log collector usage.	When needed, we use AWS CloudTrail to monitor all access to all resources in AWS including API access.		
AAAI-19	Describe or provide a reference to the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how).	AWS CloudTrail tracks changes going back at least six months.		
Business Continuity Plan		**Vendor Answers**	**Additional Information**	**Guidance**
BCPL-01	Describe or provide a reference to your Business Continuity Plan (BCP).	Continuity of service is built into the AWS architecture with distinct regional failovers, self-healing, and other safeguards. Documentation is available at: https://clients.collegesource.com/home/display/UC/uAchieve+Cloud+Disaster+Recovery+Plan		
BCPL-02	Is an owner assigned who is responsible for the maintenance and review of the Business Continuity Plan?	Yes	Our President and Vice President are assigned responsbility for the maintenance and review of the Business Continuity Plan.	Provide details as necessary.
BCPL-03	If possible, can the Institution review your BCP and supporting documentation?	Yes		Provide details as necessary.
	Is there a defined problem/issue escalation plan in your BCP for impacted clients?	Yes	See the System Outage Incident Reporting documentation in the CollegeSource Support Center here: https://clients.collegesource.com/home/pages/viewpage.action?spaceKey=UC&title=System+Outage+Incident+Reporting	Provide a brief description.
BCPL-05	Is there a documented communication plan in your BCP for impacted clients?	Yes	Significant incident and outage notifications are sent within 24 hours of discovery by phone and/or email to clients. All relevant details are included.	Provide a brief description.
BCPL-06	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?	Yes	In addition to routine monitoring, training, and discussions, CollegeSource has an annual security day scheduled to assess and address security, continuity, and recovery issues. This event typically occurs in the last week of September.	Provide a brief description.

BCPL-07	Indicate the last time that the BCP was tested and provide a summary of the results.	Current AWS setup using autoscaling, load balancers, and RDS database in multi-AZ ensures that when a problem occurs, the system will continue to function. Please refer to the DRP reference in the document for more details.		
BCPL-08	Does your organization conduct training and awareness activities to validate its employees understanding of their roles and responsibilities during a crisis?	Yes	In addition to routine monitoring, training, and discussions, CollegeSource has an annual security day scheduled to assess and address security, continuity, and recovery issues. This event typically occurs in the last week of September.	Provide a brief description.
BCPL-09	Are specific crisis management roles and responsibilities defined and documented?	Yes	The cloud support team is aware of their responsiblies and are cross-trained to ensure that anyone can perform the required duties in case of an incident.	Provide a brief description.
BCPL-10	Does your organization have an alternative business site or a contracted Business Recovery provider?	Yes	We utilize AWS multi-AZ deployment of our resources.	Provide the distance (in miles) between the primary and alternaitve locations.
BCPL-11	Does your organization conduct an annual test of relocating to this alternate site for business recovery purposes?	Yes	We utilize AWS multi-AZ deployment of our resources. Therefore, whenever a new EC2 is added to the autoscaling group, it tests the ability to respond in case of an incident in that region.	Provide a brief description.
BCPL-12	Indicate the priority of service restoration for services utilized by the Institution compared to other applications/services the vendor provides.	uAchieve suite utilizes some student data in the institution's SIS as well as their Security Management System. In case of an incident, the SIS and Security Management System maintained by the institution needs to be restored for uAchieve to continue its full functionality.		

Change Management		Vendor Answers	Additional Information	Guidance
CHNG-01	Do you have a documented and currently followed change management process (CMP)?	Yes	Changes are tracked in GitHub for any applications implemented. Any EC2 image created is preserved going back five images in standard storage.	Provide a brief description.
CHNG-02	Indicate all procedures that are implemented in your CMP. a.) An impact analysis of the upgrade is performed. b.) The change is appropriately authorized. c.) Changes are made first in a test environment. d.) The ability to implement the upgrades/changes in the production environment is limited to appropriate IT personnel.	A.) Any upgrade is performed in a new environment prior to being applied to any higher environment. B.) Clients provide authorization of the upgrade after testing the upgraded environment. C.) See A/B. D.) Ability to implement upgrades/changes in Production is limited to CollegeSource's Services and Support Technical team members.		
CHNG-03	How and when will the Institution be notified of major changes to your environment that could impact the Institution's security posture?	Clients will be made aware of any security issues as soon as CollegeSource is aware of them. CollegeSource will notifiy clients via email and provide next steps to resolve the issue at hand.		
CHNG-04	Do clients have the option to not participate in or postpone an upgrade to a new release?	Yes	If a new version has issues preventing the client from using it in production, then client can delay the release.	
CHNG-05	Describe or provide a reference to your solution support strategy in relation to maintaining software currency. (i.e. how many concurrent versions are you willing to run and support?)	CollegeSource intends to support new releases and previous releases in the cloud.		
CHNG-06	Identify the most current version of the software. Detail the percentage of live customers that are utilizing the proposed version of the software as well as each version of the software currently in use.	The most current version of the software is uAchieve v4.5.1.		
CHNG-07	Describe, if applicable, your support for client customizations from one release to another.	Customizations will be carried over from one release to the next, where appropriate. We do not encourage customizations to ensure that upgrades to future releases will not impact or restrict the upgrades.		

CHNG-08	How does your organization ensure that only application software verifiable as authorized, tested, and approved for production, and having met all other requirements and reviews necessary for commissioning, is placed into production?	When a new major release is made available, a new environment is provisioned for the client to test and verify. Only when a client gives the indication of satisfaction with that release is it applied to production.		
CHNG-09	Describe or provide a reference to your release schedule for product updates.	Major releases will be issued every 18-24 months; uAchieve Cloud schools will be upgraded to these major releases by CollegeSource as part of the annual subscription fee. Point releases (minor enhancements and minor bug fixes) are made available every six months in between the major releases. uAchieve Cloud schools can contract with CollegeSource to update their install to a point release, if desired.		
CHNG-10	Describe or provide a reference to your technology roadmap, for the next 2 years, for enhancements and bug fixes for the product/service being assessed.	Our development focus for the next 12-18 months is focused on updating uAchieve Planner and generally improving the student and advising experience. From a technology standpoint, we will continue to explore performance improvements and cost savings as we expand our usage of AWS. Clients can request enhancements, report bugs, and follow issue progress through our Issue Tracker: https://clients.collegesource.com/support/secure/Dashboard.jspa		
CHNG-11	Describe or provide a reference to your expectation of client involvement with product updates?	Clients have the ability to submit bugs and enhancements via the CollegeSource Support Center. The Product Development team meets and organizes those issues/enhancements as they fit into future releases.		
CHNG-12	Provide a brief summary of how critical patches are applied to all systems and applications.	If there is a security patch upon release from our Product Development team, clients will be notified of the patch and when it will be applied to their release. Patches will be applied to the client's dev environment and tested before going to production.		
CHNG-13	Describe or provide a reference to how security risks are mitigated until patches can be applied.	We use AWS' GuardDuty and AWS WAF. Amazon GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behavior to help protect AWS accounts and workloads. It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. GuardDuty also detects potentially compromised instances or reconnaissance by attackers. AWS WAF is used to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for bots. New rules can be deployed within minutes.		
CHNG-14	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?	Yes	During upgrades, CollegeSource will work with clients to determine the best window for upgrades to be applied.	Provide a detailed description.
CHNG-15	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?	Yes	Email will be used to document such requests, in addition to our support ticketing system. We also have implemented a support hotline that institutions can utilize, as needed, during support hours.	Provide a detailed description.
Data		**Vendor Answers**	**Additional Information**	**Guidance**
DATA-01	Describe the highest level of data classification that will be managed within your system(s) and/or application(s).	The highest level of data classification that will be managed within our systems/applications include student courses, grades, and calculated GPA.		
DATA-02	Describe or provide a reference to how institution data is physically and logically separated from that of other customers.	Clients in the multi-tenant environment are contained in the same RDS instance, but separated by database schema. All database schemas are implemented with different security users. CollegeSource database users have the ability to see all schemas, while client users only have access to their own schema. Clients have the option to have their own separate database that will only include and host their data.		

DATA-03	Will Institution's data be stored on any devices (database servers, file servers, SAN, NAS, …) configured with non-RFC 1918/4193 (i.e. publicly routable) IP addresses?	No		
DATA-04	Is sensitive data encrypted in transport?	Yes	uAchieve suite uses SSL.	Provide a detailed description.
DATA-05	Is sensitive data encrypted in storage (e.g. disk encryption, at-rest)?	Yes	Encrypted at Rest.	Provide a detailed description.
DATA-06	Do you employ or allow any cryptographic modules that do not conform to the Federal Information Processing Standards (FIPS PUB 140-2)?	No		
DATA-07	Describe or provide a reference to the encryption technology and strategy you employ for transmitting sensitive information over TCP/IP networks (e.g., SSH, SSL/TLS, VPN).	The encryption technology employed for transmitting sensitive infomration over TCP/IP networks is SSH and SSL.		Include all types of encryption; remote-access, application/database, end-user-to-system, etc.
DATA-08	List all locations (i.e. city + datacenter name) where the institution's data will be stored?	AWS does not provide physical locations for data centers. However, since we utilize US-based regions, data resides within the US. All data centers reside within US-based regions in different physical locations.		
DATA-09	At the completion of this contract, will data be returned to the institution?	Yes		
DATA-10	How will data be returned to the institution and in what format?	Data will be in database format as export/backup.		
DATA-11	How long will the institution's data be available within the system at the completion of this contract?	The institution's data will be available within the system at the completion of this contract for 30 days.		
DATA-12	Can the institution extract a full backup of data?	Yes	CollegeSource currently use Oracle 12c engine running in AWS RDS. Daily backups are taken and manual backups can be generated, as needed. These backups, automated or manual, can be provided to the institution upon request.	Describe frequency and procedures for obtaining a full backup of data.
DATA-13	Are ownership rights to all data, inputs, outputs, and metadata retained by the Institution?	Yes		
DATA-14	Are these rights retained even through a provider acquisition or bankruptcy event?	Yes	Data contained in the database for a client can be returned to the institution when needed.	Provide a brief description.
DATA-15	In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?	Yes	Data contained in the database for a client can be returned to the institution when needed.	Provide a detailed description.
DATA-16	Describe or provide a reference to the backup processes for the servers on which the service and/or data resides.	Snapshots of VM images are taken prior to putting into production and can be launched within seconds. The database is backed up nightly and retained for seven days.		
DATA-17	Are backup copies made according to pre-defined schedules and securely stored and protected?	Yes	AWS maintains backups in our VPC.	Provide a brief description.
DATA-18	How long are data backups stored?	Data backups are stored for seven days.		
DATA-19	Are data backups encrypted?	Yes	Database and all manual and automated backups are encrypted at rest.	Provide a brief summary.

DATA-20	Summarize the encryption algorithm/strategy you are using to secure the backups.	The encryption algorithm/strategy used to secure backups is the AWS-generated encrytion key (AES-256 encryption).		
DATA-21	Describe or provide a reference to your cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement) of all system components (e.g. database, system, web, etc.).	Keys are saved in AWS and only accessible to CollegeSource staff who have been granted access.		
DATA-22	Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?	Yes		
DATA-23	Are you performing offsite backups? (i.e. digitally moved off site)	No		
DATA-24	Are physical backups taken off site? (i.e. physically moved off site)	No		
DATA-25	Do backups containing the institution's data ever leave the United States of America either physically or via network routing?	No		
DATA-26	Describe or provide a reference to your media handling process, that is documented and currently implemented, including end-of-life, repurposing, and data sanitization procedures.	N/A		
DATA-27	Does this process adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?	No	N/A	
DATA-28	Do procedures exist to ensure that retention and destruction of data meets established business and regulatory requirements?	Yes	Audits in the uAchieve schema for clients are maintinated for the period agreed to during contract execution.	Provide a brief description.
DATA-29	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?	Yes		
DATA-30	Will you handle data in a FERPA compliant manner?	Yes		
DATA-31	Is any institution data visible in system administration modules/tools?	No		
Database		**Vendor Answers**	**Additional Information**	**Guidance**
DBAS-01	Does the database support encryption of specified data elements in storage?	Yes	AES-256 encryption.	Describe the type of encryption that is supported.
DBAS-02	Do you currently use encryption in your database(s)?	Yes	The encryption currently used in our database(s) is AES-256 encryption.	Describe how encryption is leveraged.
Datacenter		**Vendor Answers**	**Additional Information**	**Guidance**
DCTR-01	Does your company own the physical data center where the Institution's data will reside?	No	The institution's data will reside in the AWS cloud.	Provide a detailed description of where institution's data will reside.
DCTR-02	Does the hosting provider have a SOC 2 Type 2 report available?	Yes	The SOC 2 Type 2 report is available at AWS artifacts and can be provided.	Obtain the report if possible and add it to your submission.

DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (i.e 24x7x365)?	Yes	The data centers are staffed per the Data Center Control detailed here: https://aws.amazon.com/compliance/data-center/controls/	Describe the on-site staff capabilities.
DCTR-04	Do any of your servers reside in a co-located data center?	Yes	AWS controls the underlying servers: CollegeSource gets VMs in our own VPC. However, since CollegeSource utilizes US-based regions, the data resides within the US.	Provide a brief decription of this arrangement.
DCTR-05	Are your servers separated from other companies via a physical barrier, such as a cage or hardened walls?	No		
DCTR-06	Does the physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?		N/A	
DCTR-07	Select the option that best describes the network segment that servers are connected to.	Flat Shared Network		
DCTR-08	Does this data center operate outside of the United States?	No	Since CollegeSource utilizes US-based regions, the data resides within the US.	
DCTR-09	Will any institution data leave the United States?	No	Since CollegeSource utilizes US-based regions, the data resides within the US.	
DCTR-10	List all datacenters and their cities, states (provinces), and countries where the institution's data will be stored (including within the United States).		See response to DATA-08.	
DCTR-11	Are your primary and secondary data centers geographically diverse?	Yes	AWS uses different zones for hosting server/data. Each zone is physically separated and independent from the other zones.	Provide a brief description.
DCTR-12	If outsourced or co-located, is there a contract in place to prevent data from leaving the United States?	Yes		
DCTR-13	What Tier Level is your data center (per levels defined by the Uptime Institute)?	Tier II	CollegeSource will handle questions beyond client/staff abilities.	
DCTR-14	Is the service hosted in a high availability environment?	Yes	CollegeSource utilizes multiple AWS zones and locations to ensure redundancy and high availability.	Provide a brief description.
DCTR-15	Is redundant power available for all datacenters where institution data will reside?	Yes	Redundant power availability for all datacenters where institution data will reside is detailed here: https://aws.amazon.com/compliance/data-center/	Provide a detailed description of the implemented strategy. (i.e. batteries, generator)
DCTR-16	How often are redundant power strategies tested?	The frequency of testing of redundant power strategies is detailed here: https://aws.amazon.com/compliance/data-center/		
DCTR-17	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.	The availability of cooling and fire suppression systems in all datacenters where institution data will reside is detailed here: https://aws.amazon.com/compliance/data-center/data-centers/		
DCTR-18	State how many Internet Service Providers (ISPs) provide connectivity to each datacenter where the institution's data will reside.	The number of Internet Service Providers (ISPs) providing connectivity to each datacenter where the institution's data will resides is detailed here: https://aws.amazon.com/compliance/data-center/		
DCTR-19	Does every datacenter where the Institution's data will reside have multiple telephone company or network provider entrances to the facility?	Yes	Multiple telephone company/network provider entrances to the datacenters where the institution's data will reside is detailed here: https://aws.amazon.com/compliance/data-center/	Provide a detailed description.

Disaster Recovery Plan	Vendor Answers	Additional Information	Guidance

DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).	The CollegeSource Disaster Recovery Plan (DRP) is detailed here: https://clients.collegesource.com/home/display/UC/uAchieve+Cloud+Disaster+Recovery+Plan+-+Regional		
DRPL-02	Is an owner assigned who is responsible for the maintenance and review of the DRP?	Yes		
DRPL-03	If possible, can the Institution review your DRP and supporting documentation?	Yes	The institution may review the CollegeSource Disaster Recovery Plan (DRP) and supporting documentation detailed here: https://clients.collegesource.com/home/display/UC/uAchieve+Cloud+Disaster+Recovery+Plan+-+Regional	Provide DRP with your submission of this matrix.
DRPL-04	Are any disaster recovery locations outside the United States?	No		
DRPL-05	Does your organization have a Disaster Recovery site or a contracted Disaster Recovery provider?	Yes	The CollegeSource AWS setup ensures that, in case of a disaster, the system self-heals and becomes available in minutes. The database has a synced database in another location; AWS will switch to it if the main database goes down. Duplicate VMs run in different locations. If one or more becomes unavailable, new ones are automatically provisioned and brought up within minutes.	
DRPL-06	What type of availability does your Disaster Recovery site provide?	The CollegeSource Disaster Recover Site using AWS should have availability within minutes.		
DRPL-07	Does your organization conduct an annual test of relocating to this site for disaster recovery purposes?	Yes	The CollegeSource cloud environment is spread across zones. AWS handles the physical testing of the datacenters.	
DRPL-08	Is there a defined problem/issue escalation plan in your DRP for impacted clients?	Yes	The defined problem/issue escalation plan in the CollegeSource Disaster Recovery Plan (DRP) for impacted clients is detailed here: https://clients.collegesource.com/home/display/UC/uAchieve+Cloud+Disaster+Recovery+Plan+-+Regional	Provide a brief description.
DRPL-09	Is there a documented communication plan in your DRP for impacted clients?	Yes	The documented communication plan in the CollegeSource Disaster Recovery Plan (DRP) for impacted clients is detailed here: https://clients.collegesource.com/home/pages/viewpage.action?spaceKey=UC&title=System+Outage+Incident+Reporting	Provide a brief description.
DRPL-10	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)	See response to DRPL-05.		
DRPL-11	Indicate the last time that the Disaster Recovery Plan was tested and provide a summary of the results (including actual recovery time).	During the month of May, access for CollegeSource VMs was revoked to the SIS of one of our clients. The instances automatically became unavailable and new ones were provisioned. The team was notified by AWS Cloudwatch, at which point they went in, contacted the client, and resolved issue. Time to recovery was minutes, and was dependent on client response to reopen access in their firewall to CollegeSourceVMs.		
DRPL-12	Do the documented test results identify your organizations actual recovery time capabilities for technology and facilities?	Yes	See DRPL-11 response.	Provide a brief description.
DRPL-13	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?	Yes	DRP is largely a function of the AWS environment itself. Documentation on how this occurs is updated as AWS employs new technologies.	Describe that process.

DRPL-14	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?	Yes	CollegeSource carries technical errors and omissions coverage in addition to commercial general liability coverage.	Provide a brief description.
Firewalls, IDS, IPS, and Networking		**Vendor Answers**	**Additional Information**	**Guidance**
FIDP-01	Are you utilizing a web application firewall (WAF)?	Yes	CollegeSource uses the AWS web application firewall (WAF): https://aws.amazon.com/waf/	Describe the currently implemented WAF.
FIDP-02	Are you utilizing a stateful packet inspection (SPI) firewall?	Yes	CollegeSource uses the AWS web application firewall (WAF): https://aws.amazon.com/waf/	Describe the currently implemented SPI firewall.
FIDP-03	State and describe who has the authority to change firewall rules?	Those with authority to change firewall rules include Ayman Rabi and Hao Doan.		
FIDP-04	Do you have a documented policy for firewall change requests?	No	Only two individuals have access to modify AWS WAF. If any staff need to update/modify the WAF rules, they can reach out to either Ayman Rabi or Hao Doan.	Provide a brief desciption.
FIDP-05	Have you implemented an Intrusion Detection System (network-based)?	Yes	CollegeSource utilizes AWS GuardDuty: https://aws.amazon.com/guardduty/	Describe the currently implemented IDS.
FIDP-06	Have you implemented an Intrusion Prevention System (network-based)?	Yes	CollegeSource utilizes AWS GuardDuty: https://aws.amazon.com/guardduty/	Describe the currently implemented IPS.
FIDP-07	Do you employ host-based intrusion detection?	Yes	CollegeSource utilizes AWS GuardDuty: https://aws.amazon.com/guardduty/	Describe the currently implemented host-based IDS solution(s).
FIDP-08	Do you employ host-based intrusion prevention?	Yes	CollegeSource utilizes AWS GuardDuty: https://aws.amazon.com/guardduty/	Describe the currently implemented host-based IPS solution(s).
FIDP-09	Describe or provide a reference to any other safeguards used to monitor for attacks?	CollegeSource has built scripts that take the attackers identified by GuardDuty and adds them to the AWS WAF blacklist automatically. The offending IP is also added to our NACL to ensure complete denial of access.		
FIDP-10	Do you monitor for intrusions on a 24x7x365 basis?	Yes	With AWS GuardDuty and WAF, 24/7 monitoring is enabled.	Provide a brief summary of this activity.
FIDP-11	Is intrusion monitoring performed internally or by a third-party service?	Intrusion monitoring is performed internally by AWS services and personnel.		
FIDP-12	Are audit logs available for all changes to the network, firewall, IDS, and/or IPS?	Yes	AWS CloudTrail logs all activity to the AWS account, including API calls.	Describe the current audit strategy.
Mobile Applications - Optional based on QUALIFIER response.		**Vendor Answers**	**Additional Information**	**Guidance**
MAPP-01	On which mobile operating systems is your software or service supported?			
MAPP-02	Describe or provide a reference to the application's architecture and functionality.			
MAPP-03	Is the application available from a trusted source (e.g., iTunes App Store, Android Market, BB World)?			
MAPP-04	Does the application store, process, or transmit critical data?			
MAPP-05	Is Institution data encrypted in transport?			

MAPP-06	Is Institution data encrypted in storage? (e.g. disk encryption, at-rest)			
MAPP-07	Does the mobile application support Kerberos, CAS, or Active Directory authentication?			
MAPP-08	Will any of these systems be implemented on systems hosting the Institution's data?			
MAPP-09	Does the application adhere to secure coding practices?			
MAPP-10	Has the application been tested for vulnerabilities by a third party?			
MAPP-11	State the party that performed the test and the date it was conducted?			
Physical Security		**Vendor Answers**	**Additional Information**	**Guidance**
PHYS-01	Describe or provide a reference to physical safeguards that are placed on facilities housing the institution's data (e.g., video monitoring, restricted access areas, man traps, card access controls, etc.)?	Physical safeguards in place on facilities housing the institution's data are detailed here: https://aws.amazon.com/compliance/data-center/data-centers/		
PHYS-02	Are employees allowed to take home Institution's data in any form?	No		
PHYS-03	Are video monitoring feeds retained?	Yes	Retained video monitoring feeds are detailed here: https://aws.amazon.com/compliance/data-center/data-centers/	State the retention period for security video.
PHYS-04	Is the video feed monitored by data center staff?	No	Monitoring of video feeds by data center staff is detailed here: https://aws.amazon.com/compliance/data-center/data-centers/	Describe plans to have video feed(s) monitored.
PHYS-05	Are individuals required to sign in/out for installation and removal of equipment?	Yes	Requirements for individuals signing in/out for installation and removal of equipment are detailed here: https://aws.amazon.com/compliance/data-center/data-centers/	
PHYS-06	What are the equipment removal procedures for the clients?	Equipment removal procedures for clients are detailed here: https://aws.amazon.com/compliance/data-center/data-centers/		
Policies, Procedures, and Processes		**Vendor Answers**	**Additional Information**	**Guidance**
PPPR-01	Briefly describe your security organization. Include the responsible party for your information security program and the size of your security staff?	CollegeSource utilizes AWS and their staff and security measures that are in place as detailed here: https://aws.amazon.com/compliance/data-center/data-centers/		
PPPR-02	Do you have a documented patch management process?	Yes	AWS provides all patches needed for databases. Patches are applied during specified maintenance windows. For the EC2 instances, CollegeSource staff applies patches, as needed.	Provide a brief description.
PPPR-03	Can you accommodate encryption requirements using open standards?	Yes		
PPPR-04	Have your developers been trained in secure coding techniques?	Yes	Annually, CollegeSource developers attend several conferences in search of best security practices. Additionally, CollegeSource hosts an annual meeting to review security in uAchieve Cloud.	Provide a brief description of the training provided.

PPPR-05	Was your application developed using secure coding techniques?	CollegeSource follows guidelines outlined by the Open Web Application Security Project (OWASP), particularly focusing on mitigating the Top 10 list of security threats. This is performed through a combination of good development practices, Spring Security API, OWASP and other web security project implementations (Antisamy, CSRFGuard, etc), and verification with manual testing and OWASP Zed Attack Proxy testing. See the 2018 internal OWASP tests for uAchieve Self-Service (user interface) and Dashboard (security component of uAchieve) on the CollegeSource Support Center here: https://clients.collegesource.com/home/pages/viewpage.action?preview=%2F107907858%2F186745351%2FDashboard+SelfService+OWASP+Report+451.html&spaceKey=SECU&title=Security+Technical+Documentation and https://clients.collegesource.com/home/download/attachments/107907858/Dashboard%20SelfService%20OWASP%20Report%20451.html?version=2&modificationDate=1528917331203&api=v2		
PPPR-06	Do you subject your code to Static Code Analysis and/or Static Application Security Testing prior to release? If so, what tool(s) do you use?"	No		
PPPR-07	Describe testing processes that are established and followed (e.g., development of test plans, personnel involved in the testing process, and authorized individual accountable for approval and certification of test results)?	CollegeSource uses an iterative and incremental software development approach for uAchieve. "Public" releases are scheduled at six month intervals. Major enhancements and technical changes are included in major releases issued every 18-24 months, with point releases (minor enhancements and minor bug fixes) issued between major releases. Major enhancements and technical changes are assigned to a release 12 – 18 months prior to the release date. The majority of minor enhancements and bug fixes are assigned 3-5 months prior to release, but can be assigned as late as six weeks prior to release. The design process begins 6-18 months prior to release, depending on enhancement complexity. The User Experience (UX) Lead either creates prototypes or working HTML for the developers to work from. The development team works closely with the UX Lead and Subject Matter Experts (SMEs) to ensure features are implemented as designed. Underpinning this working relationship is the Continuous Integration and Build Server. As developers check in code to the repository (at least daily), the source code is recompiled with the latest changes from all developers, all unit tests are run, and the new version is automatically deployed to the development server. Here, all developers, QA, SME, and other interested employees have access to the system. SMEs will run individual test cases to ensure each individual issue is resolved satisfactorily on the development server. A series of automated Quality Assurance tests are also run nightly on the latest build. Once the issue is resolved satisfactorily, documentation is finalized. A code freeze for the current release is enforced 6-8 weeks prior to the release date, at which point the latest code base is rebuilt and deployed to the test server. This is when QA testing begins in earnest. No new issues can be added to the release at this point; however, problems that QA uncovers during testing are resolved. When QA clears the release, the release is published and made available to clients. This incremental and iterative approach provides several advantages for CollegeSource and our clients over other possible approaches: • Dedicated planning and design stages allow for review and discussion of the impact of updates by the entire team (SMEs, QA, developers, UX) prior to implementation. • Continuous integration and continuous deployment ensures recent changes are not breaking existing features, and developers are implementing features as intended by UX and SMEs. • Continuous automated deployment prevents release package bugs from slipping through to published release packages. • Clients can review, create, and vote on enhancement requests and bug fixes. This process helps us prioritize issues. SMEs work closely with clients and act as advocates for their issues during the release planning process. • The process allows CollegeSource and clients to plan updates far enough in advance to accurately gauge their impact and effort, yet remain nimble enough to handle necessary design/implementation changes if the continuous integration process uncovers unintended consequences.		
PPPR-08	Are information security principles designed into the product lifecycle?	Yes	CollegeSource keeps abreast of OWASP-identified application security risks and mitigates at least the top ten threats by reviewing the threats and resolutions with all developers, performing code reviews, and running the Zed Attack Proxy after every build.	Provide a brief description.
PPPR-09	Do you have a documented systems development life cycle (SDLC)?		See response to PPPR-07 above.	

PPPR-10	Describe or provide a reference to your system development life cycle methodology including your environments, version control, and change management (if not already covered in the Change Management section).		See response to PPPR-07 above.	
PPPR-11	Do you have a formal incident response plan?	Yes	See the formal incident response plan detail here: https://clients.collegesource.com/home/display/UC/Information+Security+Incident+Reporting	Provide a brief summary of your incident response plan.
PPPR-12	Will you comply with applicable Breach Notification Laws?	Yes	Compliance with applicable Breach Notification Laws is dependant upon the breach and when/how CollegeSource verifies it.	Describe how long it will take to be notified of a data breach or security incident.
PPPR-13	Will you comply with the Institution's IT policies with regards to user privacy and data protection?	Yes		
PPPR-14	Is your company subject to US laws and regulations?	Yes		
PPPR-15	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?	No		
PPPR-16	Do you require new employees to fill out agreements and review policies?	Yes		
PPPR-17	What agreements are required and policies reviewed? (i.e. confidentiality agreement, etc.)	Required agreements and reviewed policies include the Drug Free Workplace Policy, Employee Handbook, and Confidentiality Agreement.		Provide a copy of all agreements, if possible.
PPPR-18	Do you have a documented information security policy?	No	(See PPPR-11).	
PPPR-19	Do you have an information security awareness program?	No	(See PPPR-11).	
PPPR-20	Is the security awareness training mandatory for all employees?		N/A	
PPPR-21	How frequently are employees required to undergo the security awareness training?	Employees are required to undergo security awareness training annually.		
PPPR-22	Is a process documented, and currently followed, that requires a review and update of the access-list for privileged accounts?	Yes	CollegeSource integrates with the institution’s SSO or LDAP system. While unauthorized access is monitored, the institution is responsible for reviewing the list of valid users in their SSO/LDAP tables.	Provide a brief description and how often this process is executed.
PPPR-23	Describe or provide a reference to your internal audit processes and procedures.	See PPPR-22.		
Product Evaluation		**Vendor Answers**	**Additional Information**	**Guidance**
PROD-01	Do you incorporate customer feedback into security feature requests?	Yes	Clients are able to submit enhancements via the CollegeSource Support Center.	Provide the appropriate method for submitting feature requests.
PROD-02	Can you provide an evaluation site to the institution for testing?	No		
Quality Assurance		**Vendor Answers**	**Additional Information**	**Guidance**

QLAS-01	Provide a general summary of your Quality Assurance program.	The QA team tests an application after every 2-week development sprint, focusing on the issues that were resolved in that sprint. Before every release, a 6-8 week testing cycle occurs, where the QA team performs regression testing of issues included in prior releases, then retests every issue included in the current release. Both automated and manual testing occurs at each phase.		
QLAS-02	Do you comply with ISO 9001?	Yes	ISO 9001 is available at AWS artifacts and can be provided.	If certified, provide documentation.
QLAS-03	Will your company provide quality and performance metrics in relation to the scope of services and performance expectations for the services you are offering?	Yes	CollegeSource provides a weekly report of system traffic and response times.	If possible, provide documentation.
QLAS-04	Have you supplied products and/or services to the Institution (or its Campuses) in the last five years?	Yes	DARwin degree audit install (COBOL) was upgraded to uAchieve (JAVA); uAchieve Planner was licensed and implemented in conjunction with uAchieve degree audit.	Provide the University contact, describe the products and/or services offered, and the total value of the services provided.
QLAS-05	Do you have a program to keep your customers abreast of higher education and/or industry issues?	Yes	Keeping customers abreast of higher education and industry issues occures at the CollegeSource Annual Conference.	If certified, provide documentation.
Systems Management & Configuration		**Vendor Answers**	**Additional Information**	**Guidance**
SYST-01	Are systems that support this service managed via a separate management network?	Yes	The system that supports this serviced via a separate management network is AWS cloud.	Provide a brief description of how this is implemented.
SYST-02	Do you have an implemented system configuration management process? (e.g. secure "gold" images, etc.)	Yes	Implemented system configuration management includes snapshots taken of client VMs, which are kept in AWS for future use, if needed.	Provide a brief description.
SYST-03	Are employee mobile devices managed by your company's Mobile Device Management (MDM) platform?	No		
SYST-04	Provide a general summary of your systems management and configuration strategy, including servers, appliances, and mobile devices (company and employee owned).			
Vulnerability Scanning		**Vendor Answers**	**Additional Information**	**Guidance**
VULN-01	Are your *applications* scanned externally for vulnerabilities?	No	CollegeSource applications are not formally scanned by an outside agency. However, some on-premise clients have run security scans on our products and have reported their findings to us if they discover a problem.	
VULN-02	What was the date of your applications last external assessment? (mm/dd/yyyy)	N/A		

VULN-03	Are your applications scanned for vulnerabilities prior to new releases?	CollegeSource follows the guidelines outlined by the Open Web Application Security Project (OWASP), particularly focusing on mitigating the Top 10 list of security threats. This is performed through a combination of good development practices, Spring Security API, OWASP and other web security project implementations (Antisamy, CSRFGuard, etc), and verification with manual testing and with OWASP Zed Attack Proxy testing. The 2018 internal OWASP tests for uAchieve Self-Service (user interface) and Dashboard (security component of uAchieve) can be found on the CollegeSource Support Center here: https://clients.collegesource.com/home/pages/viewpage.action?preview=%2F107907858%2F186745351%2FDashboard+SelfService+OWASP+Report+451.html&spaceKey=SECU&title=Security+Technical+Documentation and https://clients.collegesource.com/home/download/attachments/107907858/Dashboard%20Self Service%20OWASP%20Report%20451.html?version=2&modificationDate=1528917331203&api=v2		Describe plans to implement application vulnerability scanning prior to release.
VULN-04	Are your *systems* scanned externally for vulnerabilities?	Yes	AWS does port scanning and DOD attack preventions. CollegeSource also uses AWS GuardDuty and WAF.	Provide a brief description.
VULN-05	What was the date of your systems last external assessment? (mm/dd/yyyy)	AWS conducts these tests very often and without notice to us or other clients.		Provide a copy of the assessment report.
VULN-06	Describe or provide a reference to the tool(s) used to scan for vulnerabilities in your applications and systems.	The tool used to scan for application/systems vulnerabilities is OWASP Zed Attack Proxy testing.		
VULN-07	Will you provide results of security scans to the Institution (if requested)?		See response to VULN-03 above.	
VULN-08	Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.).		See response to VULN-03 above.	
VULN-09	Will you allow the institution to perform its own security testing of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?	Yes	The client may conduct tests at any convenient time, provided they give CollegeSource at least two week's notice of the scheduled event. If the test is to occur outside of normal support hours, additional costs may apply for supporting such testing. If the client has chosen to forego a dedicated database for cost reduction, they must notify CollegeSource six weeks in advance. Additionally, other clients must agree to the scheduled outage and may wish to join in testing at the same time.	Provide a brief description.
HIPAA - Optional based on QUALIFIER response.		**Vendor Answers**	**Additional Information**	**Guidance**
HIPA-01	Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act?			
HIPA-02	Do you monitor or receive information regarding changes in HIPAA regulations?			
HIPA-03	Has your organization designated HIPAA Privacy and Security officers as required by the Rules?			
HIPA-04	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?			

HIPA-05	Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?			
HIPA-06	Do you have a plan to comply with the Breach Notification requirements if there is a breach of data?			
HIPA-07	Have you conducted a risk analysis as required under the Security Rule?			
HIPA-08	Have you identified areas of risks?			
HIPA-09	Have you taken actions to mitigate the identified risks?			
HIPA-10	Does your application require user and system administrator password changes at a frequency no greater than 90 days?			
HIPA-11	Does your application require a user to set their own password after an administrator reset or on first use of the account?			
HIPA-12	Does your application lock-out an account after a number of failed login attempts?			
HIPA-13	Does your application automatically lock or log-out an account after a period of inactivity?			
HIPA-14	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?			
HIPA-15	If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?			
HIPA-16	Does your application provide the ability to define user access levels?			
HIPA-17	Does your application support varying levels of access to administrative tasks defined individually per user?			
HIPA-18	Does your application support varying levels of access to records based on user ID?			
HIPA-19	Is there a limit to the number of groups a user can be assigned?			
HIPA-20	Do accounts used for vendor supplied remote support abide by the same authentication policies and access logging as the rest of the system?			
HIPA-21	Does the application log record access including specific user, date/time of access, and originating IP or device?			

HIPA-22	Does the application log administrative activity, such user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?			
HIPA-23	How long does the application keep access/change logs?			
HIPA-24	Can the application logs be archived?			
HIPA-25	Can the application logs be saved externally?			
HIPA-26	Does your data backup and retention policies and practices meet HIPAA requirements?			
HIPA-27	Do you have a disaster recovery plan and emergency mode operation plan?			
HIPA-28	Have the policies/plans mentioned above been tested?			
HIPA-29	Can the application logs be saved externally?			
HIPA-30	Can you provide a HIPAA compliance attestation document?			
HIPA-31	Are you willing to enter into a Business Associate Agreement (BAA)?			
HIPA-32	Have you entered into a BAA with all subcontractors who may have access to protected health information (PHI)?			
PCI DSS - Optional based on QUALIFIER response.		**Vendor Answers**	**Additional Information**	**Guidance**
PCID-01	Does your systems or products store, process, or transmit cardholder (payment/credit/debt card) data?			
PCID-02	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?			
PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?			
PCID-04	Are you classified as a service provider?			
PCID-05	Are you on the list of VISA approved service providers?			
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?			
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.			

PCID-08	What payment processors/gateways does the system support?			
PCID-09	Can the application be installed in a PCI DSS compliant manner ?			
PCID-10	Is the application listed as an approved PA-DSS application?			
PCID-11	Does the systems or products use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?			
PCID-12	Include documentation describing the systems' abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.			