EDUCAUSE

Shared Assessments Introduction

Campus IT environments are rapidly changing and the speed of cloud service adoption is increasing. Institutions looking for ways to do more with less see cloud services as a good way to save resources. As campuses deploy or identify cloud services, they must ensure the cloud services are appropriately assessed for managing the risks to the confidentiality, integrity and availability of sensitive institutional information and the PII of constituents. Many campuses have established a cloud security assessment methodology and resources to review cloud services for privacy and security controls. Other campuses don't have sufficient resources to assess their cloud services in this manner. On the vendor side, many cloud services providers spend significant time responding to the individualized security assessment requests made by campus customers, often answering similar questions repeatedly. Both the provider and consumer of cloud services are wasting precious time creating, responding, and reviewing such assessments.

The **Higher Education Community Vendor Assessment Toolkit** (**HECVAT**) attempts to generalize higher education information security and data protections and issues for consistency and ease of use. Some institutions may have specific issues that must be addressed in addition to the general questions sets provided in the toolkit. It is anticipated that the HECVAT will be revised over time to account for changes in services provisioning and the information security and data protection needs of higher education institutions.

The Higher Education Community Vendor Assessment Toolkit:
- Helps higher education institutions ensure that vendor services are appropriately assessed for security and privacy needs, including some that are unique to higher education
- Allows a consistent, easily-adopted methodology for campuses wishing to reduce costs through vendor services without increasing risks
- Reduces the burden that service providers face in responding to requests for security assessments from higher education institutions

The Higher Education Community Vendor Assessment Toolkit is a suite of tools built around the original HECVAT (known now as HECVAT - Full) to allow institutions to adopt, implement, and maintain a consistent risk/security assessment program. Tools include:
- **HECVAT - Triage**: Used to initiate risk/security assessment requests - review to determine assessment requirements
- **HECVAT - Full**: Robust questionnaire used to assess the most critical data sharing engagements
- **HECVAT - Lite**: A lightweight questionnaire used to expedite the vendor assessment process
- **HECVAT - On-Premise**: Unique questionnaire used to evaluate on-premise appliances and software

The HECVAT (and Toolkit) was created by the Higher Education Information Security Council Shared Assessments Working Group. Its purpose is to provide a starting point for the assessment of vendor provided services and resources. Over time, the Shared Assessments Working Group hopes to create a framework that will establish a community resource where institutions and cloud services providers will share completed Higher Education Cloud Vendor Assessment Tool assessments.

https://www.educause.edu/hecvat
https://www.ren-isac.net/hecvat

This Higher Education Cloud Vendor Assessment Toolkit is brought to you by the Higher Education Information Security Council, and members from EDUCAUSE, Internet2, and the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC).

Proceed to the next tab, Instructions.

HECVAT - Lite | Instructions

Target Audience

These instructions are for **vendors** interested in providing the Institution with a software and/or a service and for **security assessors** assessing the software and/or service. The purpose of this worksheet (i.e., the HECVAT - Lite tab) is for a vendor to submit robust security safeguard information in regards to the product (software/service) being assessed in the Institution's assessment process. Consumers do not populate this tool.

Document Layout

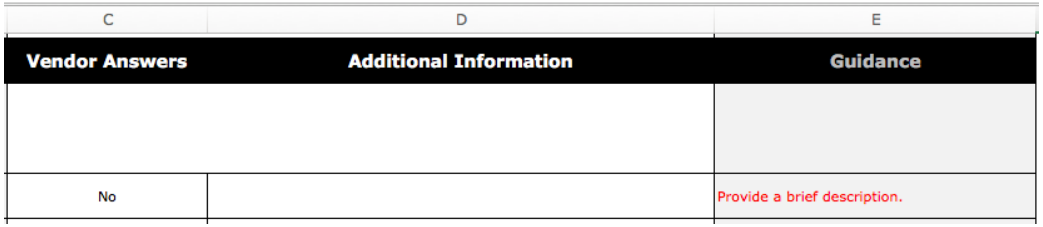
There are four main sections of the Higher Education Community Vendor Assessment Tool - Lite, all listed below and outlined in more detail. Within each section, answer each question top-to-bottom. Some questions are nested and may be blocked out via formatting based on previous answers. Populating this document in the correct order improves efficiency.
Do not overwrite selection values (data validation) in column C of the HECVAT - Lite tab.

General Information	This section is self-explanatory; product specifics and contact information.
Documentation	Focused on external documentation, the Institution is interested in the frameworks that guide your security strategy and what has been done to certify these implementations.
Company Overview	This section is focused on company background, size, and business area experience.
Safeguards	The remainder of the document consists of various safeguards, grouped generally by section.

Document Layout

Vendor responses are captured exclusively in the "HECVAT - Lite" tab. Responses should only be entered into columns C and D [of the HECVAT - Lite tab], "Vendor Answers" and "Additional Information" respectively. Sometimes C and D are separate and other times they are merged (refer to Figure 1 below). If they are separate, C will be a selectable, drop-down menu and supporting information should be added to column D. If C and D are merged, the question is looking for the answer to be in narrative form. At the far right is a column titled “Guidance”. When answering questions, check this column to ensure you have submitted information/documentation to sufficiently answer the question. Use the “Additional Information” column to provide any requested details.

Figure 1:



C	D	E
Vendor Answers	**Additional Information**	**Guidance**
No		Provide a brief description.

Definitions	
Institution	Any school, college, or university using the Higher Education Community Vendor Assessment Tool - Lite
Vendor Hosting Regions	The country/region in which the vendor's infrastructure(s) is/are located, including all laws and regulations in-scope within that country/region.
Vendor Work Locations	The country/region(s) in which the vendor's employees and sub-contractors are located.

Data Reporting & Scoring

To update data in the Report tabs, click Refresh All in the Menu tab. Input provided in the HECVAT tab is assessed a preliminary score pending review by the assessing institution.
Note for institution assessors and vendors: Until an institution assesses HECVAT responses, the scoring is incomplete. Assessors must complete Step 2 in the Analyst Report tab to convert qualitative responses to quantitative values. Once this step is complete, the scoring system is fully populated.

Proceed to the next tab, HECVAT - Lite | Vendor Response.

Assessment Instructions For Risk/Security Assessors

1. **Begin** your assessment by selecting the Analyst Report tab.
2. **Select** the appropriate security standard used in your institution (cell C10) before you begin.
3. **Select** compliant states for vendor responses in column G. Yes means compliant. No means not compliant.
   Note: Review the Analyst Reference tab for guidance and question/response interpretation.
4. **Override** default weights to meet your Institution's needs in column I.
5. **Navigate** to the Summary Report tab once all responses are evaluated and compliance indicated, as appropriate.
6. **Review** details in the Summary Report and based on your assessment findings, follow-up with vendor for clarification(s) or add the Summary Report output to your Institution's reporting documents.
7. **Connect** with your higher education peers by joining the EDUCAUSE HECVAT Users Community Group at https://connect.educause.edu.

HECVAT - Lite | Vendor Response

Version 3.04

Vendor Response

DATE-01	**Date**	*6/6/2023*

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 Community Vendor Assessment Toolkit. 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.

GNRL-01	Vendor Name	*EDUCATION MANAGEMENT SOLUTIONS*
GNRL-02	Product Name	*Competency AI*
GNRL-03	Product Description	*Brief Description of the Product*
GNRL-04	Web Link to Product Privacy Notice	*https://www.SIMULATIONiQ.com*
GNRL-05	Web Link to Accessibility Statement or VPAT	*https://www.vendor.domain/accessibilitystatement*
GNRL-06	Vendor Contact Name	*Vendor Contact Name*
GNRL-07	Vendor Contact Title	*Vendor Contact Title*
GNRL-08	Vendor Contact Email	*Vendor Contact E-mail Address*
GNRL-09	Vendor Contact Phone Number	*555-555-5555*
GNRL-10	Vendor Accessibility Contact Name	*Vendor Accessibility Contact Name*
GNRL-11	Vendor Accessibility Contact Title	*Vendor Accessibility Contact Title*
GNRL-12	Vendor Accessibility Contact Email	*Vendor Accessibility Contact Email*
GNRL-13	Vendor Accessibility Contact Phone Number	*555-555-5555*
GNRL-14	Vendor Hosting Regions	*See Instructions tab for guidance*
GNRL-15	Vendor Work Locations	*See Instructions tab for guidance*

Vendor Instructions

Step 1: Complete each section answering each set of questions in order from top to bottom; the built-in formatting logic relies on this order. **Step 2**: Submit the completed Higher Education Community Vendor Assessment Toolkit - Lite to the requesting institution.

Company Overview		Vendor Answers	Additional Information	Guidance	Analyst Notes
COMP-01	Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.	EMS is an industry pioneer in simulation-based solutions for healthcare training environments ranging from integrated clinical simulation management software and audio-video recording, to counselor		N/A	
COMP-02	Have you had an unplanned disruption to this product/service in the last 12 months?	No		N/A	
COMP-03	Do you have a dedicated Information Security staff or office?	Yes	EMS has a dedicated Software and System Development team that includes Software Development, QA, Client Support, IT Implementation, and Product Management departments that work in concert to provide complete lifecycle management of software and system development environment.	Describe your Information Security Office, including size, talents, resources, etc.	
COMP-04	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)	No		Describe any plans to create a dedicated Software and System Development team.	
COMP-05	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?	No	SIMULATIONiQ CompetencyAI is used for healthcare simulation training and doesn't store real patient data, and therefore encryption for data at rest has not been a typical requirement. However, database encryption is supported and can be enabled if required by Client.		
COMP-06	Will data regulated by PCI DSS reside in the vended product?	No			
COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.	EMS uses SANS CIS Critical Security Controls; CIS 20 controls are designed to help us safeguard our systems and data from known attack vectors. These Controls are implemented using policy, security		N/A	

Documentation		Vendor Answers	Additional Information	Guidance	Analyst Notes
DOCU-01	Have you undergone a SSAE 18 / SOC 2 audit?	No	We are under process to go for SOC2 audit in Q2 2024	Describe any plans to undergo a SSAE 18 audit.	

DOCU-02	Have you completed the Cloud Security Alliance (CSA) CAIQ?	No		Describe any plans to complete the CSA CAIQ.	
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	No		Describe any plans to obtain CSA STAR certification.	
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)	Yes	EMS uses SANS CIS Critical Security Controls; CIS 20 controls are designed to help us safeguard our systems and data from known attack vectors. These Controls are implemented using policy, security tools, training, management at the disposal of EMS.	Provide documentation on how your organization conforms to your chosen framework and indicate current certification levels, where appropriate.	
DOCU-05	Can the systems that hold the institution's data be compliant with NIST SP 800-171 and/or CMMC Level 3 standards?	No		Describe any plans to provide NIST SP 800-171 or CMMC Level 3 services.	
DOCU-06	Can you provide overall system and/or application architecture diagrams including a full description of the data flow for all components of the system?	Yes		Provide your diagrams (or a valid link to it) upon submission.	
DOCU-07	Does your organization have a data privacy policy?	Yes		Provide your data privacy document (or a valid link to it) upon submission.	
DOCU-08	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?	Yes		Provide a reference to your employee onboarding and offboarding policy and supporting documentation or submit it along with this fully-populated HECVAT.	
DOCU-09	Do you have a well documented Business Continuity Plan (BCP) that is tested annually?	Yes		Provide a reference to your BCP and supporting documentation or submit it along with this fully-populated HECVAT.	
DOCU-10	Do you have a well documented Disaster Recovery Plan (DRP) that is tested annually?	Yes		Provide a reference to your DRP and supporting documentation or submit it along with this fully-populated HECVAT.	
DOCU-11	Do you have a documented change management process?	Yes		Summarize your current change management process.	
DOCU-12	Has a VPAT or ACR been created or updated for the product and version under consideration within the past year?	No		Please state your plans (when and by whom) to complete a VPAT.	
DOCU-13	Do you have documentation to support the accessibility features of your product?	Yes		Provide examples with links where possible.	
IT Accessibility		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
ITAC-01	Has a third party expert conducted an accessibility audit of the most recent version of your product?	No	We are under process of implementation.	Please provide plans (when and by whom) any audit is planned, if any or rationale if not.	
ITAC-02	Do you have a documented and implemented process for verifying accessibility conformance?	Yes	We are under process of implementation.	Describe your processes and methodologies for validating accessibility conformance.	
ITAC-03	Have you adopted a technical or legal accessibility standard of conformance for the product in question?	Yes	We are under process of implementation.	Indicate which primary standards and comment upon any additional standards the product meets.	
ITAC-04	Can you provide a current, detailed accessibility roadmap with delivery timelines?	Yes		Comment upon how far into the future the roadmap extends. Provide evidence (including links) of having delivered upon the accessibility roadmap in the past.	
ITAC-05	Do you expect your staff to maintain a current skill set in IT accessibility?	Yes		Provide any further relevant information about how expertise is maintained; include any accessibility certifications staff may hold (e.g., IAAP WAS <https://www.accessibilityassociation.org/certifications> or DHS Trusted Tester <https://section508.gov/test/trusted-tester>.	

ITAC-06	Do you have a documented and implemented process for reporting and tracking accessibility issues?	Yes		Describe the process and any recent examples of fixes as a result of the process.	
ITAC-07	Do you have documented processes and procedures for implementing accessibility into your development lifecycle?	Yes		Provide further details or multiple means in Additional Information.	
ITAC-08	Can all functions of the application or service be performed using only the keyboard?	Yes		State when and on which platform this was verified.	
ITAC-09	Does your product rely on activating a special 'accessibility mode,' a 'lite version' or accessing an alternate interface for accessibility purposes?	No			
Application/Service Security		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
HLAP-01	Are access controls for institutional accounts based on structured rules, such as role-based access control (RBAC), attribute-based access control (ABAC) or policy-based access control (PBAC)?	Yes	RBAC is implemented in application	Describe available roles.	
HLAP-02	Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?	Yes	RBAC is implemented in application		
HLAP-03	Do you have a documented and currently implemented strategy for securing employee workstations when they work remotely? (i.e. not in a trusted computing environment)	Yes	We ensure they only work on EMS VPN environment and no client data can be tranfered to employee's local system.	Provide supporting documentation of your strategy.	
HLAP-04	Does the system provide data input validation and error messages?	Yes	Validation messages are self explainatory	Describe how your system(s) provide data input validation and error messages.	
HLAP-05	Are you using a web application firewall (WAF)?	No	We are planning to use WAF by Q4 2023	Describe compensating controls that protect your web application, if applicable.	
HLAP-06	Do you have a process and implemented procedures for managing your software supply chain (e.g. libraries, repositories, frameworks, etc)	Yes	We utilize Azure DevOPS tool for this.	Provide supporting documentation of your processes.	
Authentication, Authorization, and Accounting		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
HLAA-01	Does your solution support single sign-on (SSO) protocols for user and administrator authentication?	Yes	Our application supports SAML based SSO implementation	Describe how strong authentication is enforced (e.g., complex passwords, multifactor tokens, certificates, biometrics, aging requirements, re-use policy).	
HLAA-02	Does your organization participate in InCommon or another eduGAIN affiliated trust federation?	No	Marketing team's response needed	Describe plans to participate in InCommon or another eduGAIN affiliated trust federation.	
HLAA-03	Does your application support integration with other authentication and authorization systems?	Yes	LDAP, ADFS, SAML	List which systems and versions supported (such as Active Directory, Kerberos, or other LDAP compatible directory) in Additional Info.	
HLAA-04	Does your solution support any of the following Web SSO standards? [e.g., SAML2 (with redirect flow), OIDC, CAS, or other]	Yes	SAML	State the Web SSO standards supported by your solution and provide additional details about your support, including framework(s) in use, how information is exchanged securely, etc.	
HLAA-05	Do you support differentiation between email address and user identifier?	Yes	Can be implemented on-demand		
HLAA-06	Do you allow the customer to specify attribute mappings for any needed information beyond a user identifier? [e.g., Reference eduPerson, ePPA/ePPN/ePE]	Yes	Attributes can be mapped using custom fields		

HLAA-07	Are audit logs available to the institution that include AT LEAST all of the following; login, logout, actions performed, timestamp, and source IP address?	Yes			
HLAA-08	If you don't support SSO, does your application and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)	Yes	OTP (Email & SMS)	List all supported multi-factor authentication methods, technologies, and/or products and provide a brief summary of each.	
HLAA-09	Does your application automatically lock the session or log-out an account after a period of inactivity?	Yes	60 minutes of default idle timeout, can be modified based on client's requirement	Describe the default behavior of this capability.	
Systems Management		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
HLSY-01	Do you have a systems management and configuration strategy that encompasses servers, appliances, cloud services, applications, and mobile devices (company and employee owned)?	Yes	Complany owns all the devices.	Summarize your systems management and configuration strategy.	
HLSY-02	Will the institution be notified of major changes to your environment that could impact the institution's security posture?	Yes	We notify using our customer support team in advance.	State how and when the institution will be notified of major changes to your environment.	
HLSY-03	Are your systems and applications scanned for vulnerabilities [that are then remediated] prior to new releases?	Yes	we do test for vulnerabilities before any new release.	Provide a brief description.	
HLSY-04	Have your systems and applications had a third party security assessment completed in the last year?	Yes	We conducted a pentest by third party.	Provide the results with this document (link or attached), if possible. State the date of the last completed third party security assessment.	
HLSY-05	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?	No	We are under process to implement this	State your plans to implement policy and procedure(s) guiding risk mitigation practices before critical patches can be applied.	
Data		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
HLDA-01	Does the environment provide for dedicated single-tenant capabilities? If not, describe how your product or environment separates data from different customers (e.g., logically, physically, single tenancy, multi-tenancy).	No	Our product is multi-tenent	Describe your plan to separate institution data from other customers.	
HLDA-02	Is sensitive data encrypted, using secure protocols/algorithms, in transport? (e.g. system-to-client)	Yes	We use tls 1.3 encryption in transport	Summarize your transport encryption strategy	
HLDA-03	Is sensitive data encrypted, using secure protocols/algorithms, in storage? (e.g. disk encryption, at-rest, files, and within a running database)	Yes	All data in -rest is secured using Azure encrypted vaults.	Summarize your data encryption strategy and state what encryption options are available.	
HLDA-04	Are involatile backup copies made according to pre-defined schedules and securely stored and protected?	Yes	We backup all the servers with 7 days retention period	If your strategy uses different processes for services and data, ensure that all strategies are clearly stated and supported.	
HLDA-05	Can the Institution extract a full or partial backup of data?	Yes	we can extract data within 7 days retention period	Provide a general summary of how full and partial backups of data can be extracted.	
HLDA-06	Do you have a media handling process, that is documented and currently implemented that meets established business needs and regulatory requirements, including end-of-life, repurposing, and data sanitization procedures?	Yes		Provide documented details of this process (link or attached).	
HLDA-07	Does your staff (or third party) have access to Institutional data (e.g., financial, PHI or other sensitive information) within the application/system?	Yes	Our product doesn't store any financial / PHI / sensitive data	Summarize what access staff (or third parties) have to institutional data.	
Datacenter		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
HLDC-01	Does your company manage the physical data center where the institution's data will reside?	No	This is hosted by Microsoft	Provide a detailed description of where the institution's data will reside.	
HLDC-02	Are you generally able to accomodate storing each institution's data within their geographic region?	Yes	Can be implemented on-demand		

HLDC-03	Does the hosting provider have a SOC 2 Type 2 report available?	Yes	This is hosted by Microsoft	Obtain the report if possible and add it to your submission.	
HLDC-04	Does your organization have physical security controls and policies in place?	Yes	This is hosted by Microsoft	Describe your physical security strategy.	
HLDC-05	Do you have physical access control and video surveillance to prevent/detect unauthorized access to your data center?	Yes	This is hosted by Microsoft	Describe how you prevent and detect unauthorized access to your data center.	
Networking		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
HLNT-01	Do you enforce network segmentation between trusted and untrusted networks (i.e., Internet, DMZ, Extranet, etc.)?	Yes	This is managed within Microsoft Azure.	Provide a brief summary of how trusted and untrusted networks are segmented.	
HLNT-02	Are you utilizing a stateful packet inspection (SPI) firewall?	Yes	This is managed within Microsoft Azure.	Describe the currently implemented SPI firewall.	
HLNT-03	Do you use an automated IDS/IPS system to monitor for intrusions?	Yes	This is managed within Microsoft Azure.	Describe the currently implemented IDS/IPS.	
HLNT-04	Are you employing any next-generation persistent threat (NGPT) monitoring?	Yes	This is managed within Microsoft Azure.	Describe your NGPT monitoring strategy.	
HLNT-05	Do you require connectivity to the Institution's network for support/administration or access into any existing systems for integration purposes?	Yes	This is managed within Microsoft Azure.	Describe the tools and technical controls implemented to secure remote access.	
Incident Handling		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
HLIH-01	Do you have a formal incident response plan?	Yes		Summarize or provide a link to your formal incident response plan.	
HLIH-02	Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?	Yes		Summarize your incident response and reporting processes.	
HLIH-03	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?	Yes		Summarize your cyber insurance strategy.	
HLIH-04	Do you have either an internal incident response team or retain an external team?	Yes	Internal	Summarize your internal approach or reference your third party contractor.	
HLIH-05	Do you have the capability to respond to incidents on a 24x7x365 basis?	Yes		Describe the implemented procedure for 24/7/365 coverage.	
Policies, Procedures, and Processes		**Vendor Answers**	**Additional Information**	**Guidance**	**Analyst Notes**
HLPP-01	Can you share the organization chart, mission statement, and policies for your information security unit?	Yes	Org chart is confidential rest can be provided	Provide a links to these documents in Additional Information or attach them with your submission.	
HLPP-02	Are information security principles designed into the product lifecycle?	Yes		Summarize the information security principles designed into the product lifecycle.	
HLPP-03	Do you have a documented information security policy?	Yes		Provide a reference to your information security policy or submit documentation with this fully-populated HECVAT-Lite.	
Third Party Assessment			**Additional Information**	**Guidance**	**Analyst Notes**
HLTP-01	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		No need to answer HLTP-02 through 04	
HLTP-02	Do you perform security assessments of third party companies with which you share data? (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.).	Yes		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.	

HLTP-03	Do you have an implemented third party management strategy?	No		State your plans to implement a third-party management strategy.	
HLTP-04	Do you have a process and implemented procedures for managing your hardware supply chain? (e.g., telecommunications equipment, export licensing, computing devices)	Yes		State what countries and/or regions this process is compliant with.	

HECVAT - Lite | Analyst Reference

Connect with your higher education peers by joining the **EDUCAUSE HECVAT Users Community Group** at https://connect.educause.edu.

Instructions

Use this reference guide to assess vendor responses in relation to your institution's environment. The context of HECVAT questions can change, depending on implementation specifics so these recommendations and follow-up response are not exhaustive and are meant to improve assessment and report capabilities within your institution's security/risk assessment program.

Analyst tip #1: For any answer that is deemed "non-compliant" by your institution, ask the vendor if there is a timeline for implementation, a sincere commitment to customer development engagement, and/or possible implementation of compensating control(s) that offsite the risks of another component.

Analyst tip #2: If a vendor's response to a follow-up inquiry is vague or seems off-point or dismissive, respond back to the vendor contact with clear expectations for a response. Responses that fail to meet expectations thereafter should be negatively assessed based on your institution's risk tolerance and the criticality of the data involved.

Analyst tip #3: The most important tip - reject a HECVAT from a vendor if; the vendor provides the institution with a insufficiently populated HECVAT; or the vendor responses are vague and/or do not answer questions directly; or significant discrepancies are found, making the HECVAT difficult to assess.

Company Overview		Reason for Question	Follow-up Inquiries/Responses
COMP-01	Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.	Defining scale of company (support, resources, skillsets), General information about the organization that may be concerning.	Follow-up responses to this one are normally unique to their response. Vague answers here usually result in some footprinting of a vendor to determine their "reputation".
COMP-02	Have you had an unplanned disruption to this product/service in the last 12 months?	We want transparency from the vendor and an honest answer to this question, regardless of the response, is a good step in building trust.	If a vendor says "No", it is taken at face value. If your organization is capable of conducting reconnaissance, it is encouraged. If a vendor has experienced a breach, evaluate the circumstance of the incident and what the vendor has done in response to the breach.
COMP-03	Do you have a dedicated Information Security staff or office?	Understanding the security program size (and capabilities) of a vendor has a significant impact on their ability to respond effectively to a security incident. The size of a vendor will determine their SO size, or lack thereof. Use the knowledge of this response when evaluating other vendor statements.	Vague responses to this question should be investigated further. Vendors without dedicated security personnel commonly have no security or security is embedded or dual-homed within operations (administrators). Ask about separation of duties, principle of least privilege, etc. - there are many ways to get additional program state information from the vendor.
COMP-04	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)	Understanding the development team size (and capabilities) of a vendor has a significant impact on their ability to produce and maintain code, adhering to secure coding best practices. The size of a vendor will determine their use of dedicated development teams, or lack thereof. Use the knowledge of this response when evaluating other vendor statements.	Follow-up inquiries for vendor team strategies will be unique to your institution and may depend on the underlying infrastructures needed to support a system for your specific use case.
COMP-05	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?	Responses to this question may indicate the presence of PHI data in the vended product.	Determine if the HECVAT Lite is appropriate for assessing products hosting and/or interacting with PHI. HECVAT Full may be more appropriate, depending on your risk tolerance and use case.

COMP-06	Will data regulated by PCI DSS reside in the vended product?	Responses to this question may indicate the presence of PCI DSS regulated data in the vended product.	Determine if the HECVAT Lite is appropriate for assessing products hosting and/or interacting with PCI DSS regulated data. HECVAT Full may be more appropriate, depending on your risk tolerance and use case.
COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.	For the 20% that HECVAT may not cover, this gives the vendor a chance to support their other responses. Beware when this area is populated with sales hype or other non-relevant information. Thorough documentation, supporting evidence, and/or robust responses go a long way in building trust in this assessment process.	This is a freebie to help the vendor state their "case". If a vendor does not add anything here (or it is just sales stuff), we can assume it was filled out by a sales engineer and questions will be evaluated with higher scrutiny.
Documentation		**Reason for Question**	**Follow-up Inquiries/Responses**
DOCU-01	Have you undergone a SSAE 18 / SOC 2 audit?	Standard documentation, relevant to institutions requiring a vendor to undergo SSAE 18 audits.	Follow-up inquiries for SSAE 18 content will be institution/implementation specific.
DOCU-02	Have you completed the Cloud Security Alliance (CSA) CAIQ?	Many vendors have populated a CAIQ or at least a self-assessment. Although lacking in some areas important to Higher Ed, these documents are useful for supplemental assessment.	Follow-up inquiries for CSA content will be institution/implementation specific.
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	If a vendor is STAR certified, vendor responses can theoretically be more trusted since CSA has verified their responses. Trust, but verify for yourself, as needed.	If STAR certification is important to your institution you may have specific follow-up details for documentation purposes.
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)	The details of the standard are not the focus here, it is the fact that a vendor builds their environment around a standard and that they continually evaluate and assess their security programs.	In an ideal world, a vendor will conform to an industry framework that is adopted by an institution. When this synergy does not exist, the interpretation of the vendor's responses must be interpreted in the context of the institution's environment. Follow-up inquires for industry frameworks (and levels of adoption) will be institution/implementation specific.
DOCU-05	Can the systems that hold the institution's data be compliant with NIST SP 800-171 and/or CMMC Level 3 standards?	For institutions that collaborate with the United States government, FISMA compliance may be required.	Follow-up inquiries for FISMA compliance will be institution/implementation specific.
DOCU-06	Can you provide overall system and/or application architecture diagrams including a full description of the data flow for all components of the system?	Many systems can be used a variety of ways. We want these implementation type diagrams so that we can understand the "real" use of the product.	Additional requests for documentation are made when other parts of the HECVAT are insufficient. Although helpful, many vendors do not provide supporting documentation. We try to be specific with our follow-up questions so that vendors understand we are not looking for 20-50 page whitepapers (sales documentation).
DOCU-07	Does your organization have a data privacy policy?	Managing and protecting institution data is the reason organizations perform security and risk assessments. Privacy policies outline how vendors will obtain, use, share, and protect institutional data and as such, should be robust in its language. Beware of vaguely worded privacy policies.	Inquire about any privacy language the vendor may have. It may not be ideal but there may be something available to assess or enough to have your legal counsel or policy/privacy professionals review.

DOCU-08	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?	Managing and protecting a vendor's assets through appropriate human resource management is of the upmost importance. Knowing how roles and access controls are implemented (directed by policy) within a vendor's infrastructure during the onboarding and offboarding processes are indicative of how access control is regarded in other areas on the provider (vendor).	Unsatisfactory answers should be met with questions about access control authority, roles and responsibilities (of access grantors), administrative privileges within the vendor's infrastructure(s), etc.
DOCU-09	Do you have a well documented Business Continuity Plan (BCP) that is tested annually?	It is expected that a vendor will maintain an accurate BCP and for it to be tested at a regular interval. Any variance to this should be clearly explained. A vendor's response to this question can reveal the value that they place on testing their BCP (and possibly other aspects of their programs).	If the vendor does not have a BCP, point them to https://www.sans.org/reading-room/whitepapers/recovery/business-continuity-planning-concept-operations-1653
DOCU-10	Do you have a well documented Disaster Recovery Plan (DRP) that is tested annually?	It is expected that a vendor will maintain an accurate DRP and for it to be tested at a regular interval. Testing a DRP is an important action that improves the efficiency and accuracy of a vendor's recovery plans. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.	If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164
DOCU-11	Do you have a documented change management process?	The lack of a change management function is indicative of immature program processes. Answers to this question can provide insight into how well their responses (on the HECVAT) represent their actual environment(s).	If a weak response is given to this answer, response scrutiny should be increased. Questions about configuration management, system authority, and documentation are appropriate.
DOCU-12	Has a VPAT or ACR been created or updated for the product and version under consideration within the past year?	VPATs (Voluntary Product Accessibility Template) / ACRs (Accessibility Conformance Report, a completed VPAT) are standard accessibility reporting formats from the ITIC <https://www.itic.org/policy/accessibility/vpat>. They can be self-assessments from a vendor, though higher confidence is given if completed by expert third parties. It is important to confirm the version of the	Cross-reference Accessibility Conformance Reports (ACR) with any answers from ITAC-04 about product roadmaps for accessibility improvements.
DOCU-13	Do you have documentation to support the accessibility features of your product?	Has the vendor documented any additional information needed by users in order to create accessible products with the tool or platform? Are there tutorials, if needed, on how assistive technology users can best use the product (platforms tested and works best, shortcuts) etc.? In other words, are they taking care of the end users? Accessibility is more than completing	If specific configurations, settings, themes, author guides or instructions are needed to ensure accessibility, are instructions on how to do so provided for administrators and end users?
Application/Service Security		**Reason for Question**	**Follow-up Inquiries/Responses**
HLAP-01	Are access controls for institutional accounts based on structured rules, such as role-based access control (RBAC), attribute-based access control (ABAC) or policy-based access control (PBAC)?	Understanding access control capabilities allows an institution to estimate the type of maintenance efforts will be involved to manage a system. Depending on the users, concerns may or not be elevated. The value of this question is largely determined by the deployment strategy and use case of the software/product/service under review. This question is specific to end-users.	Ask the vendor to summarize the best practices to restrict/control the access given to the institution's end-users without the use of RBAC. Make sure to understand the administrative requirements/overhead introduced in the vendor's environment.
HLAP-02	Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?	Managing a software/product/service may rely on various professionals to administrate a system. This question is focused on how administration, and the segregation of functions, is implemented within the vendor's infrastructure.	Managing a complex infrastructure requires diligence in protecting access and authority. Unsatisfactory responses may indicate the lack of maturity with a vendor and/or a flat infrastructure with few individuals with broad authority. Inquire about separation of duties and look for areas of inappropriate functional overlap.

HLAP-03	Do you have a documented and currently implemented strategy for securing employee workstations when they work remotely? (i.e. not in a trusted computing environment)	Telecommuting in the IT world is the norm and an institution should know that proper safeguards are in place when remote access is allowed. Vendor responses vary greatly so confirm the context of the response if it is not clear. Many cloud services can only be managed remotely so there is often a gray area to interpret for this response.	Request additional documentation that outlines the security controls implemented to safeguard your institutional data.
HLAP-04	Does the system provide data input validation and error messages?	Input validation is a secure coding best practices so confirming its implementation is normally a high priority. Error messages (to the system and user) can be used to detect abnormal use and to better protect institutional data. Depending on the criticality of data and the flow of said data, an institution's risk tolerance will be unique to their environment.	Inquire about any planned improvements to these capabilities. Ask about their product(s) roadmap and try to understand how they prioritize security concerns in their environment.
HLAP-05	Are you using a web application firewall (WAF)?	The use case, vendor infrastructure, and types of services offered will greatly affect the need for various firewalling devices. The focus of this question is integrity, ensuring that the systems hosting institutional data are limited in need-only communications. The use of a WAF is important in systems in which a vendor has limited access to the to code infrastructure.	If a vendors states that they outsource their code development and do not run a WAF, there is elevated reason for concern. Verify how code is tested, monitored, and controlled in production environments.
HLAP-06	Do you have a process and implemented procedures for managing your software supply chain (e.g. libraries, repositories, frameworks, etc)	Understanding system requirements and/or dependencies (e.g., open source libraries, repositories, frameworks, toolkits, modules, etc.) can reveal infrastructure risks that may not be apparent by other means. In some cases, the use of trusted components may be favorable. In others, it may initiate the assessment of the vendor's environment in more detail and/or expand the scope of the institution's assessment.	Follow-up inquiries concerning software supply chain will be institution/implementation specific.
Authentication, Authorization, and Accounting		**Reason for Question**	**Follow-up Inquiries/Responses**
HLAA-01	Does your solution support single sign-on (SSO) protocols for user and administrator authentication?	This question is to set account management expectations for the institution. A system that can integrate with existing, vetted solutions, has its advantages and may have less administrative overhead. Also, adherence to standards here gives credit to other standards-oriented questions/responses.	Follow-up inquiries for IAM requirements will be institution/implementation specific.
HLAA-02	Does your organization participate in InCommon or another eduGAIN affiliated trust federation?	This question defines the vendors scope of federated identity practices and their willingness to embrace higher education requirements.	If a vendor indicates that a system is standalone and cannot integrate with community standards, follow-up with maturity questions and ask about other commodity type functions or other system requirements your institution may have.
HLAA-03	Does your application support integration with other authentication and authorization systems?	This question is to set account management expectations for the institution. A system that can integrate with existing, vetted solutions, has its advantages and may have less administrative overhead. Also, adherence to standards here gives credit to other standards-oriented questions/responses.	If a vendor indicates that a system is standalone and cannot integrate with the institution's infrastructure, follow-up with maturity questions and ask about other commodity type functions or other system requirements your institution may have.

HLAA-04	Does your solution support any of the following Web SSO standards? [e.g., SAML2 (with redirect flow), OIDC, CAS, or other]	This question is to set account management expectations for the institution. A system that can integrate with existing, vetted solutions, has its advantages and may have less administrative overhead. Also, adherence to standards here gives credit to other standards-oriented questions/responses.	Follow-up inquiries for IAM requirements will be institution/implementation specific.
HLAA-05	Do you support differentiation between email address and user identifier?	This questions allows an institution to know vendor system limitations and to help them gauge the resources (that may be needed to implement) required to successfully integrate the product/service with institution systems.	Follow-up inquiries for identifier requirements will be institution/implementation specific.
HLAA-06	Do you allow the customer to specify attribute mappings for any needed information beyond a user identifier? [e.g., Reference eduPerson, ePPA/ePPN/ePE]	This questions allows an institution to know vendor system limitations and to help them gauge the resources (that may be needed to implement) required to successfully integrate the product/service with institution systems.	Follow-up inquiries for attirbute mapping requirements will be institution/implementation specific.
HLAA-07	Are audit logs available to the institution that include AT LEAST all of the following; login, logout, actions performed, timestamp, and source IP address?	Strong logging capabilities are vital to the proper management of a system. Implementing an immature system that lacks sufficient logging capabilities exposes an institution to great risk. Depending on your risk tolerance and the use case, your institution may or may not be concerned. The focus of this question is end-user logs.	If a weak response is given to this answer, it is appropriate to ask directed answers to get specific information. Ensure that questions are targeted to ensure responses will come from the appropriate party within the vendor.
HLAA-08	If you don't support SSO, does your application and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)	2FA/MFA, implemented correctly, strengthens the security state of a system. 2FA/MFA is commonly implemented and in many use cases, a requirement for account protection purposes.	Ask the vendor about hardware and software options, future roadmap for implementations and support, etc.
HLAA-09	Does your application automatically lock the session or log-out an account after a period of inactivity?	This is a question to ensure account integrity and institutional data confidentiality.	Follow-up inquiries for IAM requirements will be institution/implementation specific.
Systems Management		**Reason for Question**	**Follow-up Inquiries/Responses**
HLSY-01	Do you have a systems management and configuration strategy that encompasses servers, appliances, cloud services, applications, and mobile devices (company and employee owned)?	In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed by authorized users. Additionally, it is expected that devices (for administrators, vendor staff, and affiliates)that are used to access the vendor's systems are properly managed and secured.	Follow-up with a robust question set if the vendor cannot clearly state full-control of the integrity of their system(s). Questions about administrator access on end-user devices and other maintenance and patching type questions are appropriate.
HLSY-02	Will the institution be notified of major changes to your environment that could impact the institution's security posture?	Notification expectations should be set earlier in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.	If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
HLSY-03	Are your systems and applications scanned for vulnerabilities [that are then remediated] prior to new releases?	Modern technologies allow for rapid deployment of features and with them, come changes to an established code environment. The focus of this question is to verify a vendor's practice of regression testing their code and verifying that previously non-existent risks are introduced into a known, secured environment.	Ask if there are plans to implement these processes. Ask the vendor to summarize their decision behind not scanning their applications for vulnerabilities prior to release.

HLSY-04	Have your systems and applications had a third party security assessment completed in the last year?	External verification of system and application security controls are important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face-value, and verified within reason, in most cases. When a vendor can attest to, and provide externally-provided evidence supporting that attestation, it goes a long way in building trust that the vendor will appropriately protect institutional data.	Ask if there has ever been a vulnerability scan. A short lapse in external assessment validity can be understood (if there is a planned assessment) but a significant time lapse or none whatsoever is cause for elevated levels of concern.
HLSY-05	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?	New vulnerabilities are published every day and vendors have a responsibility to maintain their software(s). The fundamental nature of operation will expose some risks to the system but it is crucial that a vendor recognize their responsibilities and have a plan to implement them, when this time arrives.	Follow-up inquiries for the vendors patching practices will be institution/implementation specific.
Data		**Reason for Question**	**Follow-up Inquiries/Responses**
HLDA-01	Does the environment provide for dedicated single-tenant capabilities? If not, describe how your product or environment separates data from different customers (e.g., logically, physically, single tenancy, multi-tenancy).	A vendor's response to this question can reveal a system's infrastructure quickly. Off-point responses are common here so general follow-up is often needed. Understanding how a vendor segments its customers data (or doesn't) affects various other controls, including network settings, use of encryption, access controls, etc.). A vendor's response here will influence potential follow-up inquiries for other HECVAT questions.	Based on the vendor's response, ask the vendor to appropriately summarize how their environment/strategy is implemented and what compensating controls they have in place to ensure appropriate levels of confidentiality and integrity.
HLDA-02	Is sensitive data encrypted, using secure protocols/algorithms, in transport? (e.g. system-to-client)	The need for encryption in transport is unique to your institution's implementation of a system. In particular, the data flow between the system and the end-users of the software/product/service.	Follow-up inquiries for data encryption between the system and end-users will be institution/implementation specific. You may want to inquire if the authentication transaction is encrypted.
HLDA-02	Is sensitive data encrypted, using secure protocols/algorithms, in transport? (e.g. system-to-client)	The need for encryption in transport is unique to your institution's implementation of a system. In particular, the data flow between the system and the end-users of the software/product/service.	Follow-up inquiries for data encryption between the system and end-users will be institution/implementation specific. You may want to inquire if the authentication transaction is encrypted.
HLDA-03	Is sensitive data encrypted, using secure protocols/algorithms, in storage? (e.g. disk encryption, at-rest, files, and within a running database)	The need for encryption at-rest is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows, all factor into the need for this control.	Follow-up inquiries for data encryption at-rest will be institution/implementation specific.
HLDA-04	Are involatile backup copies made according to pre-defined schedules and securely stored and protected?	Ransomware is a significant and growing threat. Every hosted service should include offline or involitile storage to mitigate this risk.	An institution's use case will drive the requirements for backup strategy. Ensure that the institution's use case and risk tolerance can be met by vendor systems.
HLDA-05	Can the Institution extract a full or partial backup of data?	When cancelling a software/product/service, an institution will commonly want all institutional data that was provided to a vendor. The vendor's response should verify if the institution can extract data or if it is a manual extraction by vendor staff.	A vendor's response should be clear and concise. Be wary of vague responses to this questions and inquire about export specifics, as needed.

HLDA-07	Does your staff (or third party) have access to Institutional data (e.g., financial, PHI or other sensitive information) within the application/system?	Confidentiality is the focus of this question. Based on the capabilities of vendor administrators, the institution may require additional safeguards to protect the confidentiality of data stored by/shared with a vendor (e.g., additional layer of encryption, etc.).	If Institutional data is visible by the vendor's system administrators, follow-up with the vendor to understand the scope of visibility, process/procedure that administrators follow, and use cases when administrators are allowed to access (view) Institutional data.
Datacenter		**Reason for Question**	**Follow-up Inquiries/Responses**
HLDC-01	Does your company manage the physical data center where the institution's data will reside?	Data ownership, availability, and the use of third-parties are all somewhat connected to the response of this question.	Simple responses without supporting documentation should be met with concern. Follow-up with a vendor and request supporting documentation if the answer is in any way dismissive or off-point.
HLDC-02	Are you generally able to accomodate storing each institution's data within their geographic region?	An institution's location will dictate what laws and regulations apply to them. As vendor's may not know where all of their customers may reside, it is imperative that vendors are able to accomodate geographic requirements for their customers. Although unfair to expect support for all geographic regions in common infrastructure/platform/software-as-a-service, it is expected that vendor's be absolutely clear about the regions they leverage and/or support.	If a vendor is unable to accomodate storing/processing institutional data within specific regions, ask them why they are unable to? Try to determine if its an infrastructure issue (scalability), a cost-reduction strategy (size/maturity), or some other issue.
HLDC-03	Does the hosting provider have a SOC 2 Type 2 report available?	Understanding the ownership structure of the facility that will host institutional data is important for setting availability expectations and ensure proper contract terms are in place to protect the institution due to use of third-parties. If a vendor uses a third-party vendor to provide datacenter solutions, having that vendor's SOC 2 Type 2 provides additional insight. The ability to assess these "forth-party" vendors is based on your institution's resources. The vendor is responsible for providing this information - ensure that they handle their vendors properly.	Follow-up inquiries for additional vendor's SOC 2 Type 2 reports will be institution/implementation specific.
HLDC-04	Does your organization have physical security controls and policies in place?	This question is primarily focused on system(s) integrity. If institutional data is stored in a system that is not physically secured from unauthorized access, the need for compensating controls is often higher. That means that although this question is in the Datacenter section, this question also encompasses office (and other) spaces used by the vendor to conduct operations.	If a weak response is given to this answer, response scrutiny should be increased. Inquire about the size of an organization, how it is physically deployed, how employees interact with each other and verify each others credibility. Any follow-up question related to physical integrity of institutional data is relevant here.
HLDC-05	Do you have physical access control and video surveillance to prevent/detect unauthorized access to your data center?	it is important to physically protect and monitor an infrastructure. The purpose of this question is to determine that appropriate protections are in-place at a vendor's data center.	If a vendor answers unsatisfactorily, follow-up with questions about their physical infrastructure strategy (why they are self hosting), geographic redundancy (to determine if the data center is colocated with staff), and any compensating controls they may have in place.
Networking		**Reason for Question**	**Follow-up Inquiries/Responses**
HLNT-01	Do you enforce network segmentation between trusted and untrusted networks (i.e., Internet, DMZ, Extranet, etc.)?	Networks are excellent at segmenting trusted and untrusted networks, a best practice used by many. Implementations can range from simple to complex but at a minimum, need to appropriately implemented and maintained.	The lack of segmentation indicates a flat network is in use. If this is the case, other compensating controls (e.g., host-based tools) will need to be in place to properly manage network communications within a vendor's infrastructure. Ask why the vendor has used this strategy and what they are doing to safeguard institutional data in this environment.

HLNT-02	Are you utilizing a stateful packet inspection (SPI) firewall?	The use case, vendor infrastructure, and types of services offered will greatly affect the need for various firewalling devices. The focus of this question is integrity, ensuring that the systems hosting institutional data are limited in need-only communications. The use of a WAF is important in systems in which a vendor has limited access to the to code infrastructure.	If a vendor states that they do not run a SPI firewall, there is elevated reason for concern. Ensure how network traffic is monitored and managed as well as any compensating controls currently implemented.
HLNT-03	Do you use an automated IDS/IPS system to monitor for intrusions?	It is important to have detective and preventive capabilities in an information system to protect institutional data. Somewhat expected in information systems, vendors without IDS/IPSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the vendor.	A security program with limited resources for event detection and prevention is not effective. Inquiries should include training for staff, reasoning behind not using IDS/IPS technologies, and how systems are monitored. Additional questions about a SIEM and other tooling may be appropriate. Ask how systems are actively protected and how malicious activity is stopped.
HLNT-04	Are you employing any next-generation persistent threat (NGPT) monitoring?	This question is primarily focused on the maturity of a vendor's security program. Technologies are rapidly introduced and the toolsets needed to monitor, manage, and secure them need to keep up. Vendor responses to this question can give an institution insight into the maturity and overall state of a vendor's security.	Follow-up inquiries for NGPT monitoring will be institution/implementation specific.
HLNT-05	Do you require connectivity to the Institution's network for support/administration or access into any existing systems for integration purposes?	This question is about what level of network access is needed by the vendor's administrators. If all that is needed is a web connection, then even simple, on-premise access to a guest network can be considered. But if it requires connectivity to a highly protected resource (for example: A database server on an isolated VLAN and only accepting traffic from a specific front end), then the vendor's administrators may need to be given access to a datacenter's network. Again, the purpose here is to determine what level of access is the minimum required and what controls to put in place to secure that access.	Follow-up inquiries for institution network connectivity resource requirements will be institution/implementation specific.
Incident Response		**Reason for Question**	**Follow-up Inquiries/Responses**
HLIH-01	Do you have a formal incident response plan?	The ability for the vendor to respond effectively (and quickly) to a security incident is of the utmost importance. The size of a vendor's security office will determine their capabilities during a security incident but the incident response plan will oftentimes determine their effectiveness. Use the knowledge of this response when evaluating other vendor statements, particularly when discussing degraded operation states.	If the vendor does not have an incident response plan, direct them to the NIST Computer Security Incident Handling Guide at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
HLIH-02	Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?	The ability for the vendor to investigate security incidents is of the utmost importance. Reviewing alerts but then taking no action is not security, only compliance. Incident reports and indications of compromise must be reviewed by qualified staff and they must have the capability to investigate further, as needed.	If the vendor does not have an incident response plan, direct them to the NIST Computer Security Incident Handling Guide at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
HLIH-03	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?	Vendor responses to this questions need to be evaluated in the context of use case, data criticality, institutional risk tolerance, and value of the software/product/service to the institution's mission.	Follow-up inquiries for cyber-risk insurance will be institution/implementation specific.

HLIH-04	Do you have either an internal incident response team or retain an external team?	The incident team structure (internal vs. external), size, and capabilities of a vendor has a significant impact on their ability to respond to and protect an institution's data. Use the knowledge of this response when evaluating other vendor statements.	If the vendor does not have an incident response team, direct them to the NIST Computer Security Incident Handling Guide at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
HLIH-05	Do you have the capability to respond to incidents on a 24x7x365 basis?	The capacity for the vendor to respond effectively (and quickly) to a security incident is of the utmost importance. The size and talent of a vendor's incident response team will determine their capabilities during a security incident. Use the knowledge of this response when evaluating other vendor statements, particularly when discussing degraded operation states.	If the vendor does not have an incident response plan, point them to the NIST Computer Security Incident Handling Guide at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
Policies, Procedures, and Processes		**Reason for Question**	**Follow-up Inquiries/Responses**
HLPP-01	Can you share the organization chart, mission statement, and policies for your information security unit?	Understanding the security program size (and capabilities) of a vendor has a significant impact on their ability to respond effectively to a security incident. Vendor's will share organizational charts and additional documentation of their security program, if needed. The point of this question is to verify vendor security program maturity or confirm other findings and/or assessments.	Vague responses to this question should be investigated further. Vendors unwilling to share additional supporting documentation decrease the trust established with other responses.
HLPP-02	Are information security principles designed into the product lifecycle?	The adherence to secure coding best practices better positions a vendor to maintain the CIA triad. Use the knowledge of this response when evaluating other vendor statements, particularly those focused on development and the protection of communications.	If information security principles are not designed into the product lifecycle, point the vendor to OWASP's Secure Coding Practices - Quick Reference Guide at https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
HLPP-03	Do you have a documented information security policy?	A shared security [responsibility] environment is expected of vendors in today's world. Security office's cannot solely protect an institution's data. Information security, ingrained in an organization, is the best case scenario for the protection of institutional data. Security awareness and practice start in a vendor's policies.	If the vendor does not have a documented information security policy, follow-up questions about training, company practices, awareness efforts, auditing, and system protection practices are appropriate.
Third Party Assessment		**Reason for Question**	**Follow-up Inquiries/Responses**
HLTP-01	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)	Management networks and end-user networks are often exclusive, with the intent of limiting access to elevated authorization tools. When a vendor states these networks are merged in operation, it should be met with elevated levels of concern. The focus of this question is to verify a common best practice in system management, allowing an institution to gain insight into a vendor's operating environment.	Verify if the vendor's practice is constrained by a technology or if it is just a best practice that is not adopted. In the case of constraints, ask for additional best practice implementation strategies that may compensate for the elevated risk(s).
HLTP-02	Do you perform security assessments of third party companies with which you share data? (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.).	In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed by authorized users. Additionally, it is expected that devices (for administrators, vendor staff, and affiliates)that are used to access the vendor's systems are properly managed and secured.	Follow-up with a robust question set if the vendor cannot clearly state full-control of the integrity of their system(s). Questions about administrator access on end-user devices and other maintenance and patching type questions are appropriate.

HLTP-03	Do you have an implemented third party management strategy?	Every organization needs to actively understand and manage their supply chain, this vendor's understanding of who their third party partners are and their ability to manage those relationships effectively and consistently speaks to the amount of risk your institution is takin on by contracting with them.	If "No", inquire if there are plans to implement a policy or if the vendor has a set of documented and consistent procedures that they are using to manage their third party relationships.
HLTP-04	Do you have a process and implemented procedures for managing your hardware supply chain? (e.g., telecommunications equipment, export licensing, computing devices)	Understanding a vendor's hardware supply chain can reveal infrastructure risks that may not be apparent by other means. In some cases, the use of trusted components may be favorable. In others, it may initiate the assessment of the vendor's environment in more detail and/or expand the scope of the institution's assessment.	Follow-up inquiries concerning hardware supply chain will be institution/implementation specific.

HECVAT - Lite | Analyst Report

Version 3.04

Institution Assessment

Instructions

Step 1: Select the security framework used at your institution in cell B10. **Step 2:** Convert qualitative vendor responses into quantitative values, starting at cell G32. **Step 3:** Review converted values, ensuring full population of report. **Step 4:** Move to the Summary Report tab.

Vendor Name	EDUCATION MANAGEMENT SOLUTIONS			**Product Name**	Competency AI
Vendor Contact Name	Vendor Contact Name			**Product Description**	Brief Description of the Product
Vendor Contact Title	Vendor Contact Title			**HECVAT Version**	Lite
Vendor Email Address	Vendor Contact E-mail Address			**Date Prepared**	45083

Step 1: Select your institution's security framework	

Report Sections	Max_Score		Score	Score %
Company	135		110	81%
Documentation	215		145	67%
IT Accessibility	180		160	89%
Application Security	130		105	81%
Authentication, Authorization, and Accounting	185		165	89%
Systems Manangement	70		55	79%
Data	165		100	61%
Datacenter	160		160	100%
Networking	155		155	100%
Incident Handling	155		155	100%
Policies, Procedures, and Practices	85		85	100%
Third Party Assessment	40		40	100%
Overall Score	**1675**		**1435**	**86%**

				Analyst Notes	Step 2: Override/Correct Vendor Responses and Set Weights Per Institution's Use Case			
ID	**Question**	**Vendor Answer**	**Additional Information**	**Notes shown in Col F on HECVAT - Lite tab)**	**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
		The vendor's selected responses are displayed here for easier reference.	The vendor's narrative responses are displayed here for easier reference.	As an analyst/assessor, use the column to make notes of concerns, follow-up questions for the vendor, needed documentation, etc.	The preferred response is that which is scored positively.	Analysts should use this dropdown to override inappropriate / incorrect vendor answers to affect scoring appropriately.	The default weight of a question is set by the makers of HECVAT tooling and is used to set a baseline.	Institutions may weight question responses differently in their assessments, based on their use of the vendor product. Adjust weights to affect final scoring appropriately.
Company Overview	**Question**	**Vendor Answer**	**Additional Information**		**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
COMP-01	Describe your organization's business background and	EMS is an industry pioneer in simulation-based solutions for healthcare training environments ranging from integrated clinical simulation management			Yes		5	
COMP-02	Have you had an unplanned disruption to this product/service in	No	0		No		20	
COMP-03	Do you have a dedicated Information Security staff or office?	Yes	EMS has a dedicated Software and System Development team that		Yes		10	
COMP-04	Do you have a dedicated Software and System Development team(s)?	No	SIMULATIONiQ CompetencyAI is used for healthcare simulation		Yes		15	
COMP-05	Does your product process protected health information (PHI) or any	No	#REF!		No		40	
COMP-06	Will data regulated by PCI DSS reside in the vended product?	No	0		No		40	
COMP-07	Use this area to share information about your environment that will	EMS uses SANS CIS Critical Security Controls; CIS 20 controls are designed to help us safeguard our systems and data from known attack vectors. These Controls			Qualitative Question		5	
Documentation	**Question**	**Vendor Answer**	**Additional Information**		**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
DOCU-01	Have you undergone a SSAE 18 / SOC 2 audit?	No	We are under process to go for SOC2 audit in Q2 2024		Yes		15	
DOCU-02	Have you completed the Cloud Security Alliance (CSA) CAIQ?	No	0		Yes		10	
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	No	0		Yes		15	
DOCU-04	Do you conform with a specific industry standard security	Yes	EMS uses SANS CIS Critical Security Controls; CIS 20 controls are		Yes		25	
DOCU-05	Can the systems that hold the institution's data be compliant with	No	0		Yes		10	
DOCU-06	Can you provide overall system and/or application architecture	Yes	0		Yes		25	

DOCU-07	Does your organization have a data privacy policy?	Yes	0		Yes		20	
DOCU-08	Do you have a documented, and currently implemented,	Yes	0		Yes		10	
DOCU-09	Do you have a well documented Business Continuity Plan (BCP)	Yes	0		Yes		10	
DOCU-10	Do you have a well documented Disaster Recovery Plan (DRP)	Yes	0		Yes		10	
DOCU-11	Do you have a documented change management process?	Yes	0		Yes		25	
DOCU-12	Has a VPAT or ACR been created or updated for the product and version	No	0		Yes		20	
DOCU-13	Do you have documentation to support the accessibility	Yes	0		Yes		20	

IT Accessibility	Question	Vendor Answer	Additional Information		Preferred Response	Compliant Override	Default Weight	Weight Override
ITAC-01	Has a third party expert conducted an accessibility audit of the	No	We are under process of implementation.		Yes		20	
ITAC-02	Do you have a documented and implemented process for	Yes	We are under process of implementation.		Yes		20	
ITAC-03	Have you adopted a technical or legal accessibility standard of	Yes	We are under process of implementation.		Yes		20	
ITAC-04	Can you provide a current, detailed accessibility roadmap	Yes	0		Yes		20	
ITAC-05	Do you expect your staff to maintain a current skill set in IT	Yes	0		Yes		20	
ITAC-06	Do you have a documented and implemented process for	Yes	0		Yes		20	
ITAC-07	Do you have documented processes and procedures for	Yes	0		Yes		20	
ITAC-08	Can all functions of the application or service be performed using only the	Yes	0		Yes		20	
ITAC-09	Does your product rely on activating a special 'accessibility mode,' a	No	0		No		20	

Application/Service Security	Question	Vendor Answer	Additional Information		Preferred Response	Compliant Override	Default Weight	Weight Override
HLAP-01	Are access controls for institutional accounts based on structured	Yes	RBAC is implemented in application		Yes		25	
HLAP-02	Are access controls for staff within your organization based on	Yes	RBAC is implemented in application		Yes		15	
HLAP-03	Do you have a documented and currently implemented	Yes	We ensure they only work on EMS VPN environment and no client data can be		Yes		20	
HLAP-04	Does the system provide data input validation and error messages?	Yes	Validation messages are self explainatory		Yes		25	
HLAP-05	Are you using a web application firewall (WAF)?	No	We are planning to use WAF by Q4 2023		Yes		25	
HLAP-06	Do you have a process and implemented procedures for managing	Yes	We utilize Azure DevOPS tool for this.		Yes		20	

Authentication, Authorization, and Accounting	Question	Vendor Answer	Additional Information		Preferred Response	Compliant Override	Default Weight	Weight Override
HLAA-01	Does your solution support single sign-on (SSO) protocols for user	Yes	Our application supports SAML based SSO implementation		Yes		20	
HLAA-02	Does your organization participate in InCommon or another eduGAIN	No	Marketing team's response needed		Yes		20	
HLAA-03	Does your application support integration with other authentication and authorization systems?	Yes	LDAP, ADFS, SAML		Yes		15	
HLAA-04	Does your solution support any of the following Web SSO	Yes	SAML		Yes		20	
HLAA-05	Do you support differentiation between email address and user	Yes	Can be implemented on-demand		Yes		20	
HLAA-06	Do you allow the customer to specify attribute mappings for any needed information	Yes	Attributes can be mapped using custom fields		Yes		20	
HLAA-07	Are audit logs available to the institution that include AT LEAST all of the following; login, logout, actions	Yes	0		Yes		40	
HLAA-08	If you don't support SSO, does your application and/or user-frontend/portal support	Yes	OTP (Email & SMS)		Yes		15	
HLAA-09	Does your application automatically lock the session or log-out an	Yes	60 minutes of default idle timeout, can be modified based on client's		Yes		15	

Systems Management	Question	Vendor Answer	Additional Information		Preferred Response	Compliant Override	Default Weight	Weight Override
HLSY-01	Do you have a systems management and configuration strategy	Yes	Complany owns all the devices.		Yes		15	
HLSY-02	Will the institution be notified of major changes to your	Yes	We notify using our customer support team in advance.		Yes		15	
HLSY-03	Are your systems and applications scanned for vulnerabilities [that are	Yes	we do test for vulnerabilities before any new release.		Yes		10	

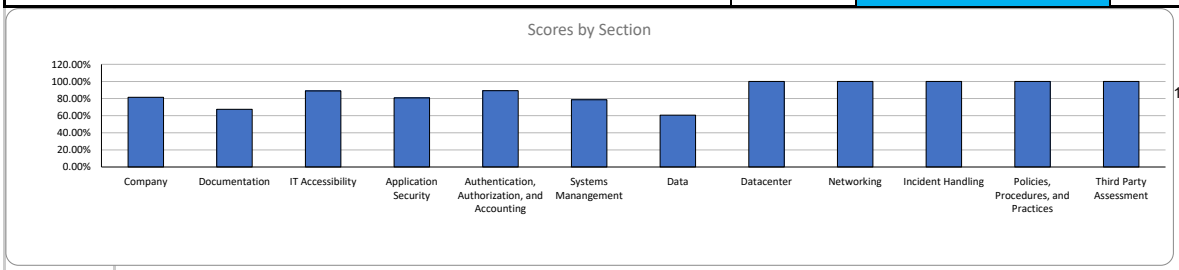
HLSY-04	Have your systems and applications had a third party security	Yes	We conducted a pentest by third party.		Yes		15	
HLSY-05	Do you have policy and procedure, currently implemented, guiding	No	We are under process to implement this		Yes		15	
Data	**Question**	**Vendor Answer**	**Additional Information**		**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
HLDA-01	Does the environment provide for dedicated single-tenant	No	Our product is multi-tenent		Yes		25	
HLDA-02	Is sensitive data encrypted, using secure protocols/algorithms, in	Yes	We use tls 1.3 encryption in transport		Yes		20	
HLDA-03	Is sensitive data encrypted, using secure protocols/algorithms, in	Yes	All data in -rest is secured using Azure encrypted vaults.		Yes		20	
HLDA-04	Are involatile backup copies made according to pre-defined schedules	Yes	We backup all the servers with 7 days retention period		Yes		15	
HLDA-05	Can the Institution extract a full or partial backup of data?	Yes	we can extract data within 7 days retention period		Yes		25	
HLDA-06	Do you have a media handling process, that is documented and	Yes	0		Yes		20	
HLDA-07	Does your staff (or third party) have access to Institutional data (e.g.,	Yes	Our product doesn't store any financial / PHI / sensitive data		No		40	
Datacenter	**Question**	**Vendor Answer**	**Additional Information**		**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
HLDC-01	Does your company manage the physical data center where the	No	This is hosted by Microsoft		No		0	
HLDC-02	Are you generally able to accomodate storing each institution's data within	Yes	Can be implemented on-demand		Yes		40	
HLDC-03	Does the hosting provider have a SOC 2 Type 2 report available?	Yes	This is hosted by Microsoft		Yes		40	
HLDC-04	Does your organization have physical security controls and policies in	Yes	This is hosted by Microsoft		Yes		40	
HLDC-05	Do you have physical access control and video surveillance to	Yes	This is hosted by Microsoft		Yes		40	
Networking	**Question**	**Vendor Answer**	**Additional Information**		**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
HLNT-01	Do you enforce network segmentation between trusted and untrusted	Yes	This is managed within Microsoft Azure.		Yes		40	
HLNT-02	Are you utilizing a stateful packet inspection (SPI) firewall?	Yes	This is managed within Microsoft Azure.		Yes		40	
HLNT-03	Do you use an automated IDS/IPS system to monitor for	Yes	This is managed within Microsoft Azure.		Yes		40	
HLNT-04	Are you employing any next-generation persistent threat (NGPT)	Yes	This is managed within Microsoft Azure.		Yes		20	
HLNT-05	Do you require connectivity to the Institution's network for	Yes	This is managed within Microsoft Azure.		Yes		15	
Incident Handling	**Question**	**Vendor Answer**	**Additional Information**		**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
HLIH-01	Do you have a formal incident response plan?	Yes	0		Yes		40	
HLIH-02	Do you have an incident response process and reporting in place to	Yes	0		Yes		15	
HLIH-03	Do you carry cyber-risk insurance to protect against unforeseen	Yes	0		Yes		20	
HLIH-04	Do you have either an internal incident response team or retain	Yes	Internal		Yes		40	
HLIH-05	Do you have the capability to respond to incidents on a 24x7x365	Yes	0		Yes		40	
Policies, Procedures, and Processes	**Question**	**Vendor Answer**	**Additional Information**		**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
HLPP-01	Can you share the organization chart, mission statement, and	Yes	Org chart is confidential rest can be provided		Yes		20	
HLPP-02	Are information security principles designed into the product lifecycle?	Yes	0		Yes		25	
HLPP-03	Do you have a documented information security policy?	Yes	0		Yes		40	
Third Party Assessment	**Question**	**Vendor Answer**	**Additional Information**		**Preferred Response**	**Compliant Override**	**Default Weight**	**Weight Override**
HLTP-01	Will institution data be shared with or hosted by any third parties? (e.g.	No	0		No		40	
HLTP-02	Do you perform security assessments of third party companies with	Yes	0		Yes		0	
HLTP-03	Do you have an implemented third party management strategy?	No	0		Yes		0	
HLTP-04	Do you have a process and implemented procedures for managing	Yes	0		Yes		0	

HECVAT - Lite | Summary Report

Version 3.04

Vendor	EDUCATION MANAGEMENT SOLUTIONS	**Product**	Competency AI
Description	Brief Description of the Product		

Overall Score:	
86%	**B**



High Risk, Non-Compliant Responses

			Institution's Security Framework	
ID	**Question**	**Additional Info**		
COMP-05	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?			
COMP-06	Will data regulated by PCI DSS reside in the vended product?			
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)	EMS uses SANS CIS Critical Security Controls; CIS 20 controls are designed to help us safeguard our systems and data from known attack vectors. These Controls are implemented using policy, security tools, training, management at the disposal of EMS.		
DOCU-06	Can you provide overall system and/or application architecture diagrams including a full description of the data flow for all components of the system?			
DOCU-11	Do you have a documented change management process?			
HLAP-01	Are access controls for institutional accounts based on structured rules, such as role-based access control (RBAC), attribute-based access control (ABAC) or			
HLAP-04	Does the system provide data input validation and error messages?	60 minutes of default idle timeout, can be modified based on client's requirement		
HLAP-05	Are you using a web application firewall (WAF)?	60 minutes of default idle timeout, can be modified based on client's requirement		
HLAA-07	Are audit logs available to the institution that include AT LEAST all of the following: login, logout			
HLDA-01	Does the environment provide for dedicated single-tenant capabilities? If not	60 minutes of default idle timeout, can be modified based on client's requirement		
HLDA-05	Can the Institution extract a full or partial backup of data?	60 minutes of default idle timeout, can be modified based on client's requirement		
HLDC-02	Are you generally able to accomodate storing each institution's data within their geographic region?	Can be implemented on-demand		

HLDC-03	Does the hosting provider have a SOC 2 Type 2 report available?	This is hosted by Microsoft		
HLDC-04	Does your organization have physical security controls and policies in place?	This is hosted by Microsoft		
HLDC-05	Do you have physical access control and video surveillance to	This is hosted by Microsoft		
HLNT-01	Do you enforce network segmentation between trusted and untrusted networks (i.e., Internet,			
HLNT-02	Are you utilizing a stateful packet inspection (SPI) firewall?			
HLNT-03	Do you use an automated IDS/IPS system to monitor for intrusions?			
HLIH-01	Do you have a formal incident response plan?	This is hosted by Microsoft		
HLIH-04	Do you have either an internal incident response	Internal		
HLIH-05	Do you have the capability to respond to incidents on a 24x7x365 basis?			
HLPP-02	Are information security principles designed into the product lifecycle?			
HLPP-03	Do you have a documented information security policy?			
HLTP-02	Do you perform security assessments of third party companies with which you share data? (i.e. hosting providers, cloud services,			
HLTP-03	Do you have an implemented third party management strategy?			
HLTP-04	Do you have a process and implemented procedures for managing your hardware supply chain? (e.g.,			

HECVAT - Lite | Standards Crosswalk

HEISC Shared Assessments Working Group

	Standard Reference URL:	https://www.cisecurity.org/controls/	https://www.hhs.gov/hipaa/for-	https://www.iso.org/standard/54533.html	https://www.nist.gov/cyberframework	https://csrc.nist.gov/publications/detail/sp/800-171/rev-	https://csrc.nist.gov/publications/detail/sp/800-53/rev-	https://www.trustedci.org/framework/core	https://www.pcisecuritystandards.org/document_library
Company Overview		**CIS Critical Security Controlsv8.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r5**	**Trusted CI**	**PCI DSS 3.2.1**
COMP-01	Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.							1: Mission Focus, 2: Stakeholders and obligations	
COMP-02	Have you had an unplanned disruption to this product/service in the last 12 months?							10: Evaluation and Refinement	
COMP-03	Do you have a dedicated Information Security staff or office?			15.2.1				7: Cybersecurity Lead, 13: Personnel	
COMP-04	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)			15.2.2					
COMP-05	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?			15.2.1				2: Stakeholders and Obligations	
COMP-06	Will data regulated by PCI DSS reside in the vended product?			14.2.1				2: Stakeholders and Obligations	
COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.			15.2.1					PCI-DSS SAQs - part 2
Documentation		**CIS Critical Security Controlsv8.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r5**	**Trusted CI**	**PCI DSS 3.2.1**
DOCU-01	Have you undergone a SSAE 18 / SOC 2 audit?			15.2.1			SA-9	10: Evaluation & Refinement	
DOCU-02	Have you completed the Cloud Security Alliance (CSA) CAIQ?			15.2.1			PE-2, PE-3, PE-5, PE-11, PE-13, PE-14, SA-9	10: Evaluation & Refinement, 14 external resources	
DOCU-03	Have you received the Cloud Security Alliance STAR certification?			15.2.1			PE-2, PE-3, PE-5, PE-11, PE-13, PE-14, SA-9	10: Evaluation & Refinement	
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)			18.1.1			SA-9	15: Baseline Control Set	
DOCU-05	Can the systems that hold the institution's data be compliant with NIST SP 800-171 and/or CMMC Level 3 standards?			18.1.1			SA-9	2: Stakeholders and Obligations	
DOCU-06	Can you provide overall system and/or application architecture diagrams including a full description of the data flow for all components of the system?		§164.308(a)(1)(i)	18.1.4	ID.GV-3		SA-9	3: Information Assets	1.1.2
DOCU-07	Does your organization have a data privacy policy?							9: Policy	12.6
DOCU-08	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?							9: Policy	8.1
DOCU-09	Do you have a well documented Business Continuity Plan (BCP) that is tested annually?						3.6.1	6: Risk Acceptance, 9: Policy, 10: Evaluation & Refinement	12.10.1
DOCU-10	Do you have a well documented Disaster Recovery Plan (DRP) that is tested annually?							6: Risk Acceptance, 9: Policy, 10: Evaluation & Refinement	12.10.1
DOCU-11	Do you have a documented change management process?					3.4.3		10: Evaluation and Refinement	6.3.2 & 6.4.6
Application/Service Security		**CIS Critical Security Controlsv8.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r5**	**Trusted CI**	**PCI DSS 3.2.1**
HLAP-01	Are access controls for institutional accounts based on structured rules, such as role-based access control (RBAC), attribute-based access control (ABAC) or policy-based access control (PBAC)?	CSC 14		9.2.2	PR.AC-4	3.1.1, 3.1.2, 3.1.7	AC-2, AC-3, AC-6	4: Asset Classification, 8: Comprehensive Application, 15: Baseline Control Set	7.1 & 7.1.1

HLAP-02	Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?	CSC 16		9.1.1	PR.AC-4, PR.PT-3	3.4.9	CM-11	4: Asset Classification, 8: Comprehensive Application, 15: Baseline Control Set	
HLAP-03	Do you have a documented and currently implemented strategy for securing employee workstations when they work remotely? (i.e. not in a trusted computing environment)	CSC 12		6.2	PR.PT-3	3.1.12, 3.1.13, 3.1.14, 3.1.15, 3.1.8, 3.1.20, 3.7.5, 3.8.2, 3.13.7	AC-3, CM-7; NIST SP 800-46	8: Comprehensive Application, 15: Baseline Control Set	
HLAP-04	Does the system provide data input validation and error messages?	CSC 2		12.1.1	ID.AM-1, ID.AM-2, ID.AM-4		CA-9, SC-4	15: Baseline Control Set	
HLAP-05	Are you using a web application firewall (WAF)?	CSC 16		14.2.5	PR.DS-6			15: Baseline Control Set	1.1
HLAP-06	Do you have a process and implemented procedures for managing your software supply chain (e.g. libraries, repositories, frameworks, etc)	CSC 12		14.2.5			RA-2	8: Comprehensive Application	2.4
Authentication, Authorization, and Accounting		**CIS Critical Security Controlsv8.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r5**	**Trusted CI**	**PCI DSS 3.2.1**
HLAA-01	Does your solution support single sign-on (SSO) protocols for user and administrator authentication?	CSC 16		9.2.3, 9.3.1, 9.4.3	PR.AC-1	3.5.7	IA-5(1)	15: Baseline Control Set	
HLAA-02	Does your organization participate in InCommon or another eduGAIN affiliated trust federation?	CSC 16		9.1.1, 9.2.3, 9.3.1, 9.4.3	PR.AC-1	3.5.1	IA-2, IA-5	14: External Resources, 15: Baseline Control Set	
HLAA-03	Does your application support integration with other authentication and authorization systems?	CSC 16		9.4.3	PR.AC-1, PR.AC-4			14: External Resources, 15: Baseline Control Set	
HLAA-04	Does your solution support any of the following Web SSO standards? [e.g., SAML2 (with redirect flow), OIDC, CAS, or other]	CSC 16		9.4.3	PR.AC-1, PR.AC-4			15: Baseline Control Set	
HLAA-05	Do you support differentiation between email address and user identifier?	CSC 6		12.4	PR.PT-1	3.1.7, 3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.4.3, 3.7.1, 3.7.6, 3.10.4, 3.10.5	AU-2(3), AU-6, AU-12, AC-6(9), CM-3, MA-2, MA-5, PE-3	15: Baseline Control Set	
Systems Management		**CIS Critical Security Controlsv8.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r5**	**Trusted CI**	**PCI DSS 3.2.1**
HLSY-01	Do you have a systems management and configuration strategy that encompasses servers, appliances, cloud services, applications, and mobile devices (company and employee owned)?					3.4.1		8: Comprehensive Application	2.2
HLSY-02	Will the institution be notified of major changes to your environment that could impact the institution's security posture?					3.4.4		2: Stakeholders and Obligations, 9: Policy	
HLSY-03	Are your systems and applications scanned for vulnerabilities [that are then remediated] prior to new releases?					3.11.2		15: Baseline Control Set	11.2
HLSY-04	Have your systems and applications had a third party security assessment completed in the last year?							10: Evaluation and Refinement	
HLSY-05	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?					3.14.1		6: Risk Acceptance, 9: Policy	11.2.2
Data		**CIS Critical Security Controlsv8.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r5**	**Trusted CI**	**PCI DSS 3.2.1**
HLDA-01	Does the environment provide for dedicated single-tenant capabilities? If not, describe how your product or environment separates data from different customers (e.g., logically, physically, single tenancy, multi-tenancy).	CSC 12			PR.AC-2, PR.IP-5	3.1.3, 3.8.1	AC-4, MP-2, MP-4	15: Baseline Control Set	
HLDA-02	Is sensitive data encrypted, using secure protocols/algorithms, in transport? (e.g. system-to-client)	CSC 13		8.2.3, 10.1.1	PR.DS-1, PR.DS-2	3.1.19, 3.8.1	MP-2, AC-19(5)	2: Stakeholders & Obligations, 15: Baseline Control Set	2.3 & 4.1
HLDA-03	Is sensitive data encrypted, using secure protocols/algorithms, in storage? (e.g. disk encryption, at-rest, files, and within a running database)	CSC 13		8.2.3, 10.1.1	PR.DS-1	3.1.19, 3.8.1	MP-2, AC-19(5)	2: Stakeholders & Obligations, 15: Baseline Control Set	8.2.1
HLDA-04	Are involatile backup copies made according to pre-defined schedules and securely stored and protected?	CSC 13		12.3.1		3.8.9	CP-9, MP-5	15: Baseline Control Set	
HLDA-05	Can the Institution extract a full or partial backup of data?	CSC 13		8.3.1	PR.DS-3	3.7.1, 3.7.2, 3.8.3	CP-9 MP-6, NIST SP 800-60, NIST SP 800-88, AC-2, AC-6, IA-4, PM-2, PM-10, SI-5, MA-2, MA-3, MP-6	15: Baseline Control Set	

HLDA-06	Do you have a media handling process, that is documented and currently implemented that meets established business needs and regulatory requirements, including end-of-life, repurposing, and data sanitization procedures?	CSC 13, CSC 14		14.2.5	PR.AC-4			9: Policy	9.6
HLDA-07	Does your staff (or third party) have access to Institutional data (e.g., financial, PHI or other sensitive information) within the application/system?							2: Stakeholders & Obligations, 9: Policy	6.4.2 & 7.1 &7.1.1
Datacenter		**CIS Critical Security Controlsv8.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r5**	**Trusted CI**	**PCI DSS 3.2.1**
HLDC-01	Does your company manage the physical data center where the institution's data will reside?	CSC 12		11.2.1				1: Mission Focus, 2: Stakeholders and Obligations	9.1
HLDC-02	Are you generally able to accomodate storing each institution's data within their geographic region?	CSC 14		11.1.1	PR.AC-2, PR.IP-5			2: Stakeholders and Obligations	
HLDC-03	Does the hosting provider have a SOC 2 Type 2 report available?	CSC 13		11.1.1				2: Stakeholders and Obligations, 10: Evaluation & Refinement, 14: External Resources , 15: Baseline Control Set	
HLDC-04	Does your organization have physical security controls and policies in place?	CSC 14		11.1.1, 11.1.2	PR.AC-2	3.8.1, 3.8.2		9: Policy, 15: Baseline Control Set	
HLDC-05	Do you have physical access control and video surveillance to prevent/detect unauthorized access to your data center?					3.10.2		15: Baseline Control Set	9.1.1
Networking		**CIS Critical Security Controlsv8.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r5**	**Trusted CI**	**PCI DSS 3.2.1**
HLNT-01	Do you enforce network segmentation between trusted and untrusted networks (i.e., Internet, DMZ, Extranet, etc.)?					3.13.1, 3.13.5		15: Baseline Control Set	10.8
HLNT-02	Are you utilizing a stateful packet inspection (SPI) firewall?					3.1.3		15: Baseline Control Set	
HLNT-03	Do you use an automated IDS/IPS system to monitor for intrusions?					3.14.6		15: Baseline Control Set	
HLNT-04	Are you employing any next-generation persistent threat (NGPT) monitoring?							15: Baseline Control Set	
HLNT-05	Do you require connectivity to the Institution's network for support/administration or access into any existing systems for integration purposes?							9: Policy	
Incident Response		**CIS Critical Security Controlsv8.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r5**	**Trusted CI**	**PCI DSS 3.2.1**
HLIH-01	Do you have a formal incident response plan?					3.6.1		9: Policy	12.5.3
HLIH-02	Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?					3.6.2		9: Policy	12.5.3
HLIH-03	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?							6: Risk Acceptance	
HLIH-04	Do you have either an internal incident response team or retain an external team?					3.6.1		13: Personnel, 14: External Resources	
HLIH-05	Do you have the capability to respond to incidents on a 24x7x365 basis?							15: Baseline Control Set	
Policies, Procedures, and Processes		**CIS Critical Security Controlsv8.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r5**	**Trusted CI**	**PCI DSS 3.2.1**
HLPP-01	Can you share the organization chart, mission statement, and policies for your information security unit?							1: Mission Focus, 9: Policy	
HLPP-02	Are information security principles designed into the product lifecycle?							8: Comprehensive Application, 9: Policy	
HLPP-03	Do you have a documented information security policy?							9: Policy	12.1

Third Party Assessment		CIS Critical Security Controlsv8.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r5	Trusted CI	PCI DSS 3.2.1
HLTP-01	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)							2: Stakeholders & Obligations, 8: Comprehensive Application, 9: Policy	12.8.1
HLTP-02	Do you perform security assessments of third party companies with which you share data? (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.).							8: Comprehensive Application, 10: Evaluation & Refinement	12.8.2
HLTP-03	Do you have an implemented third party management strategy?							2: Stakeholders & Obligations, 9: Policy	12.8
HLTP-04	Do you have a process and implemented procedures for managing your hardware supply chain? (e.g., telecommunications equipment, export licensing, computing devices)							8: Comprehensive Application, 9: Policy, 15: Baseline Control Set	

EDUCAUSE

Acknowledgments

The Higher Education Information Security Council Shared Assessments Working Group contributed their vision and significant talents to the conception, creation, and completion of this resource.

Members that contributed in 2020, 2021, and 2022:

- Mary Albert, Princeton University
- Jon Allen, Baylor University (HECVAT Users CG chair)
- Jill Bateman, Ohio University
- Vince Bonura, Fordham University
- Gwen A. Bostic, Western Michigan University
- Josh Callahan, Cal Poly Humboldt
- Meryl Bursic, Cornell University
- Christopher Cashmere, University of Nebraska
- Jiatyan Chen, Stanford University
- Tom Coffy, University of Tennessee, Knoxville
- Doug Cox, University of Michigan
- Michael Cyr, University of Maine System, IT Accessibility CG Co-Chair
- Glenn Dausch, Stony Brook University
- Suzanne Elhorr, American University of Beirut
- Charles Escue, Indiana University (HECVAT Users CG co-chair)
- Laura Fathauer, Miami University [OH]
- Sean Hagan, University of Alaska
- Greg Hanek, Indiana University
- Tania Heap, University of North Texas
- Lori Kressin, University of Virginia
- Avinash Kundu, EAB Global, Inc.
- Dennis Leber, UTHSC
- Thierry Lechler, UCF
- Sung Lee, Howard Community College
- Matthew Long, University of NebraskaMary McKee, Duke University
- Jeff Miller, University of Central Oklahoma
- Steven Premeau, University of Maine

- Laura Raderman, Carnegie Mellon University
- Mark Rank, Cirrus Identity
- Nicole Roy, Internet2
- Carmen Schafer, University of Missouri
- Kyle Shachmut, Harvard University, IT Accessibility CG Co-Chair
- Eudora Struble, Wake Forest University
- Kate Tipton, California State University at Northridge
- Jeffrey Tomaszewski, University of Michigan
- Luke Watson, Virginia Tech
- Todd Weissenberger, University of Iowa
- William Wetherill, University of North Carolina Wilmington
- John Zage, University of Illinois- National Center for Supercomputing Applications
- Deb Zsigalov, Tennessee Technological University

Members that contributed to Phase IV (2019) of this effort are:

- Jon Allen, Baylor University (working group chair)
- Matthew Buss, Internet2
- Josh Callahan, Humboldt State University
- Andrea Childress, University of Nebraska
- Tom Coffy, University of Tennessee
- Susan Coleman, REN-ISAC
- Susan Cullen, CSU Office of the Chancellor
- Michael Cyr, University of Maine System
- Debra Dandridge, Texas A&M University
- Niranjan Davray, Colgate University
- Charles Escue, Indiana University
- Carl Flynn, Baylor University
- Ruth Ginzberg, University of Wisconsin System
- Sean Hagan, Yavapai College
- Daphne Ireland, Princeton
- Brian Kelly, EDUCAUSE
- Amy Kobezak, Virginia Tech
- Nick Lewis, Internet2
- Sue McGlashan, University of Toronto
- Hector Molina, East Carolina University
- Mark Nichols, Virginia Tech

- Mark Nichols, Virginia Tech
- Laura Raderman, Carnegie Mellon University
- Kyle Shachmut, Harvard University
- Bob Smith, Longwood University
- Kyle Smith, Georgia Tech
- Christian Vinten-Johansen, Penn State University
- Valerie Vogel, EDUCAUSE

Members that contributed to Phase III (2018) of this effort are:
- Jon Allen, Baylor University
- Josh Callahan, Humboldt State University
- Susan Coleman, REN-ISAC
- Charles Escue, Indiana University
- Joanna Grama, EDUCAUSE
- Todd Herring, REN-ISAC
- Jefferson Hopkins, Purdue University
- Alex Jalso, West Virginia University
- Nick Lewis, Internet2
- Kim Milford, REN-ISAC
- Amanda Sarratore, University of Notre Dame
- Gary Taylor, York University
- Valerie Vogel, EDUCAUSE
- Gene Willacker, Michigan State University
- David Zeichick, California State University, Chico

Members that contributed to Phase II (2017) of this effort are:
- Jon Allen, Baylor University
- Samantha Birk, IMS Global Learning Consortium
- Jeff Bohrer, IMS Global Learning Consortium
- Sarah Braun, University of Colorado - Denver
- David Cassada, University of California - Davis
- Matthew Dalton, University of Massachusetts Amherst
- Charles Escue, Indiana University
- Joanna Grama, EDUCAUSE

- Todd Herring, REN-ISAC
- Kolin Hodgson, University of Notre Dame
- Tom Horton, Cornell University
- Leo Howell, North Carolina State University
- Alex Jalso, West Virginia University
- Nick Lewis, Internet2
- Wyman Miles, Cornell University
- Kim Milford, REN-ISAC
- Valerie Vogel, EDUCAUSE

Members that contributed to Phase I (2016) of this effort are:

- Jon Allen, Baylor University
- John Bruggeman, Hebrew Union College, Jewish Institute of Religion
- Charles Escue, Indiana University
- Joanna Grama, EDUCAUSE
- Karl Hassler, University of Delaware
- Todd Herring, REN-ISAC
- Nick Lewis, Internet2
- Kim Milford, REN-ISAC
- Craig Munson, Minnesota State Colleges & Universities
- Mitch Parks, University of Idaho
- Laura Raderman, Carnegie Mellon University
- Valerie Vogel, EDUCAUSE

Higher Education Community Vendor Assessment Toolkit - Lite - Change Log

HEISC Shared Assessments Working Group

Version	Date	Description of Change
v0.6	8/4/2016	Merged initial comments and suggestions of sub-group members.
v0.7	8/14/2016	Completed base formulas for all Guidance fields. Changed Qualifier formatting to make questions readable (and optional).
v0.8	8/15/2016	Added SOC2T2 question to datacenter section.
v0.9	8/16/2016	Added Systems and Configuration Management section, added MDM, sep. management networks, system configuration images, Internal audit processes and procedures.
v0.91	8/24/2016	Added input from WG meeting on 8/22, removed RiskMgmt section, added question ID's, and removed dup network question.
v0.92	8/25/2016	Added Introduction, Sharing Read Me, and Acknowledgements tabs and content. Also updated report specifics in Documentation.
v0.93	8/26/2016	Integrated grammatical corrections set by Karl, fixed a minor formula error in a guidance cell.
v0.94	8/26/2016	Added Instructions tab, adjusted question ID background color, updated DRP/BCP copy error.
v0.95	9/21/2016	Changed document title to HECVAT. Integrated KDH input.
v0.96	9/23/2016	Added input from NL, 36 modifications across all sections.
v0.97	9/26/2016	Updated Sharing Read Me tab with final language and options table.
v0.98	10/6/2016	Sharing Confirmation section added, updated instructions, updated Sharing Read Me tab, fixed a ton of conditional formatting issues.
v1.00	10/17/2016	Finalized for distribution.
v1.01	11/16/2016	Corrections for grammar, conditional formatting, and question clarification.
v1.02	11/21/2016	Added tertiary services narrative question (DNS, ISP, etc.).
v1.03	11/23/2016	Grammar and spelling cleanup.
v1.06	10/24/2017	Added standards crosswalk and Cloud Broker Index (CBI) information, changed HLAP-03, HLAA-02, HLAA-03, and HLDA-04 to freeform text. Changed University mentions to Institution.

v1.10beta	8/2/2018	Preparing for major changes. Scoring system prep.
v1.11beta	8/3/2018	Removed Sharing Tab and HESA section
v2.00	10/13/2018	Major revision. Visit https://www.educause.edu/hecvat for details.
v2.01	11/1/2018	Minor calculation revision in Summary Report scoring.
v2.02	1/25/2019	Cleaned up old question references, added Excel backwards compatibility through named ranges, and fixed analyst report view.
v2.03	3/19/2019	Summary Report scoring issues fixed (calculation ranges in the Questions tab, synchronized calculation steps for reporting in both the Full and Lite versions of the HECVAT); Analyst and Summary Report question references returning "#N/A" fixed. No changes to questions - no previous 2.0x version response values are affected.
v2.04	5/8/2019	Fixed versioning issues
v2.1	10/4/2019	Updated name, fixed calculation error on comp-06, changed question text on Standards Crosswalk to vlookups, added Analyst Reference tab, fixed external links
v2.11	11/7/2019	Fixed conditional formatting issue on HECVAT-Lite tab, corrected compliant answer values on HLDA-04 and HLDA-06. normalized font and size for Additional Info column
v3.00	10/20/2021	Major revision. Visit https://www.educause.edu/hecvat for details.
v3.04	2/6/2023	Numerous scoring fixes and grammar refinements.
