

Higher Education Load

HEISC Shared Asses

Version	Date
v0.6	8/4/2016
v0.7	8/14/2016
v0.8	8/15/2016
v0.9	8/16/2016
v0.91	8/24/2016
v0.92	8/25/2016
v0.93	8/26/2016
v0.94	8/26/2016
v0.95	9/21/2016
v0.96	9/23/2016

v0.97	9/26/2016
v0.98	10/6/2016
v1.00	10/17/2016
v1.01	11/16/2016
v1.02	11/21/2016
v1.03	11/23/2016
v1.06	10/24/2017
v1.10beta	8/2/2018
v1.11beta	8/3/2018
v2.00	10/13/2018
v2.01	11/1/2018
v2.02	1/25/2019
v2.03	3/19/2019

--	--

tion Community Vendor Assessment Toolkit - Lite - Change

Assessments Working Group

Description of Change

Merged initial comments and suggestions of sub-group members.

Completed base formulas for all Guidance fields. Changed Qualifier formatting to make questions readable (and optional).

Added SOC2T2 question to datacenter section.

Added Systems and Configuration Management section, added MDM, sep. management networks, system configuration images, Internal audit processes and procedures.

Added input from WG meeting on 8/22, removed RiskMgmt section, added question ID's, and removed dup network question.

Added Introduction, Sharing Read Me, and Acknowledgements tabs and content. Also updated report specifics in Documentation.

Integrated grammatical corrections set by Karl, fixed a minor formula error in a guidance cell.

Added Instructions tab, adjusted question ID background color, updated DRP/BCP copy error.

Changed document title to HECVAT. Integrated KDH input.

Added input from NL, 36 modifications across all sections.

Updated Sharing Read Me tab with final language and options table.
Sharing Confirmation section added, updated instructions, updated Sharing Read Me tab, fixed a ton of conditional formatting issues.
Finalized for distribution.
Corrections for grammar, conditional formatting, and question clarification.
Added tertiary services narrative question (DNS, ISP, etc.).
Grammar and spelling cleanup.
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.
Preparing for major changes. Scoring system prep.
Removed Sharing Tab and HESA section
Major revision. Visit https://www.educause.edu/hecvat for details.
Minor calculation revision in Summary Report scoring.
Cleaned up old question references, added Excel backwards compatibility through named ranges, and fixed analyst report view.
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.



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

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 question sets provided in the toolkit. It is anticipated that the HECVAT will be revised over

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 reduced time 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

- **HECVAT - Triage:** Used to triage 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 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. The current version, documentation, and other information about HECVAT can be found at:

<https://www.educause.edu/hecvat>

A listing of completed HECVATs can be found in the REN-ISAC Community Broker Index at:

<https://www.ren-isac.net/hecvat/cbi.html>

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

If you would like to reach out to the HECVAT Team, we can be reached at: hecvat@educause.edu.

(C) EDUCAUSE 2023

THIS WORK IS LICENSED UNDER A CREATIVE COMMONS ATTRIBUTION-NONCOMMERCIAL-SHAREALIKE 4.0 INTERNATIONAL LICENSE (CC BY-NC-SA 4.0)

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

Proceed to the next tab, Instructions.

HECVAT - Lit

Target Audience

These instructions are for the software and/or service security safeguard information not populate this tool.

Document Layout

There are four main sections. Within each section, answers. Populating this

Do not overwrite selected

General Information

Documentation

Company Overview

Safeguards

Document Layout

Vendor responses are captured in the HECVAT - Lite | Vendor Responses. At other times they are merged into the main report and should be added to columns titled "Guidance." When asked to answer a question, use the "Ac"

Figure 1:

Definitions

Institution


**Vendor Hosting
Regions**

**Vendor Work
Locations**

Data Reporting & Scoring

Note for institution assessments: Step 2 in the Analyst Report is populated.

Proceed to the next step

-
- 
1. **Begin** your assessment
 2. **Select** the appropriate
 3. **Select** compliant state
Note: Review the Anal
 4. **Override** default weig
 5. **Navigate** to the Sumr
 6. **Review** details in the :
Report output to your Ins
 7. **Connect** with your hig

te | Instructions

- **vendors** interested in providing the institution with a software and/or a service and for **security assessors** assessing ce. The purpose of this worksheet (i.e., the HECVAT - Lite | Vendor Response tab) is for a vendor to submit robust ation in regards to the product (software/service) being assessed in the Institution's assessment process. Consumers do

ons of the Higher Education Community Vendor Assessment Tool - Lite, all listed below and outlined in more detail. ver each question top to bottom. Some questions are nested and may be blocked out via formatting based on previous document in the correct order improves efficiency.

tion values (data validation) in column C of the HECVAT - Lite | Vendor Response tab.

This section is self-explanatory; product specifics and contact information.

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.

This section is focused on company background, size, and business area experience.

The remainder of the document consists of various safeguards, grouped generally by section.

aptured exclusively in the HECVAT - Lite | Vendor Response tab. Responses should only be entered into columns C and D Vendor Response tab, "Vendor Answers" and "Additional Information," respectively. Sometimes C and D are separate, and merged (refer to Figure 1 below). If they are separate, C will be a selectable, drop-down menu and supporting information in 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 answering questions, check this column to ensure you have submitted information/documentation to sufficiently answer "Additional Information" column to provide any requested details.

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

Any school, college, or university using the Higher Education Community Vendor Assessment Tool - Lite

The country/region in which the vendor's infrastructure(s) is/are located, including all laws and regulations in-scope within that country/region

The country/region(s) in which the vendor's employees and subcontractors are located

bring

sors and vendors: Until an institution assesses HECVAT responses, the scoring is incomplete. Assessors must complete port tab to convert qualitative responses to quantitative values. Once this step is complete, the scoring system is fully

xt tab, HECVAT - Lite | Vendor Response.

Assessment Instructions For Risk/Security Assessors

nt by selecting the Analyst Report tab.

se security standard used in your institution (cell C10) before you begin.

es for vendor responses in column G. **Yes** means compliant. **No** means not compliant.

yst Reference tab for guidance and question/response interpretation.

hts to meet your Institution's needs in column I.

nary Report tab once all responses are evaluated and compliance indicated, as appropriate.

Summary Report and based on your assessment findings, follow-up with vendor for clarification(s) or add the Summary
stitution's reporting documents.

gher education peers by joining the EDUCAUSE HECVAT Users Community Group at <https://connect.educause.edu>.

HECVAT - Lite | Vendor Response

Vendor Response

DATE-01

Date

General Information

In order to protect the institution and its systems, vendors whose products and/or services (referred to as the Assessment Toolkit). Throughout this tool, anywhere where the term "data" is used, this is an all-enclosed submission. This process will assist the institution in preventing breaches of protected information and Security Assessment and should be completed by a vendor.

GNRL-01	Vendor Name
GNRL-02	Product Name
GNRL-03	Product Description
GNRL-04	Web Link to Product Privacy Notice
GNRL-05	Web Link to Accessibility Statement or VPAT
GNRL-06	Vendor Contact Name
GNRL-07	Vendor Contact Title
GNRL-08	Vendor Contact Email
GNRL-09	Vendor Contact Phone Number
GNRL-10	Vendor Accessibility Contact Name

GNRL-11	Vendor Accessibility Contact Title
GNRL-12	Vendor Accessibility Contact Email
GNRL-13	Vendor Accessibility Contact Phone Number
GNRL-14	Vendor Hosting Regions
GNRL-15	Vendor Work Locations

Vendor Instructions

Step 1: Complete each section answering each set of questions in order from top to bottom; the built-in auto-save feature will save your responses as you work.
Step 2: Submit the completed Higher Education Community Vendor Assessment Toolkit - Lite to the vendor portal.

Company Overview	Column1
COMP-01	Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.
COMP-02	Have you had an unplanned disruption to this product/service in the past 12 months?

COMP-03	Do you have a dedicated Information Security staff or office?
COMP-04	Do you have a dedicated Software and System Development team(s)? (e.g., Customer Support, Implementation, Product Management, etc.)
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?
COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.
Documentation	
DOCU-01	Have you undergone a SSAE 18 / SOC 2 audit?

DOCU-02	Have you completed the Cloud Security Alliance (CSA) CAIQ?
DOCU-03	Have you received the Cloud Security Alliance STAR certification?
DOCU-04	Do you conform with a specific industry standard security framework? (e.g., NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)
DOCU-05	Can the systems that hold the institution's data be compliant with NIST SP 800-171 and/or CMMC Level 2 standards?
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-07	Does your organization have a data privacy policy?

DOCU-08	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?
DOCU-09	Do you have a well-documented Business Continuity Plan (BCP) that is tested annually?
DOCU-10	Do you have a well-documented Disaster Recovery Plan (DRP) that is tested annually?
DOCU-11	Do you have a documented 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?
DOCU-13	Do you have documentation to support the accessibility features of your product?

IT Accessibility

ITAC-01	Has a third-party expert conducted an accessibility audit of the most recent version of your product?
ITAC-02	Do you have a documented and implemented process for verifying accessibility conformance?
ITAC-03	Have you adopted a technical or legal accessibility standard of conformance for the product in question?
ITAC-04	Can you provide a current, detailed accessibility roadmap with delivery timelines?
ITAC-05	Do you expect your staff to maintain a current skill set in IT accessibility?

ITAC-06	Do you have a documented and implemented process for reporting and tracking accessibility issues?
ITAC-07	Do you have documented processes and procedures for implementing accessibility into your development lifecycle?
ITAC-08	Can all functions of the application or service be performed using only the keyboard?
ITAC-09	Does your product rely on activating a special "accessibility mode," a "lite version," or accessing an alternate interface for accessibility purposes?
Application/Service Security	
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)?

HLAP-02	Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?
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)?
HLAP-04	Does the system provide data input validation and error messages?
HLAP-05	Are you using a web application firewall (WAF)?
HLAP-06	Do you have a process and implemented procedures for managing your software supply chain (e.g., libraries, repositories, frameworks, etc.)?

Authentication, Authorization, and Accounting

HLAA-01	Does your solution support single sign-on (SSO) protocols for user and administrator authentication?
HLAA-02	Does your organization participate in InCommon or another eduGAIN-affiliated trust federation?
HLAA-03	Does your application support integration with other authentication and authorization systems?
HLAA-04	Does your solution support any of the following Web SSO standards? [e.g., SAML2 (with redirect flow), OIDC, CAS, or other]
HLAA-05	Do you support differentiation between email address and user identifier?
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)

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?
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.)
HLAA-09	Does your application automatically lock the session or log-out an account after a period of inactivity?
Systems Management	
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)?
HLSY-02	Will the institution be notified of major changes to your environment that could impact the institution's security posture?
HLSY-03	Are your systems and applications scanned for vulnerabilities [that are then remediated] prior to new releases?

HLSY-04	Have your systems and applications had a third-party security assessment completed in the past year?
HLSY-05	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?
Data	
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).
HLDA-02	Is sensitive data encrypted, using secure protocols/algorithms, in transport? (e.g., system-to-client)
HLDA-03	Is sensitive data encrypted, using secure protocols/algorithms, in storage? (e.g., disk encryption, at-rest, files, and within a running database)
HLDA-04	Are involatile backup copies made according to predefined schedules and securely stored and protected?

HLDA-05	Can the institution extract a full or partial backup of data?
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?
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?
Datacenter	
HLDC-01	Does your company manage the physical data center where the institution's data will reside?
HLDC-02	Are you generally able to accomodate storing each institution's data within their geographic region?
HLDC-03	Does the hosting provider have a SOC 2 Type 2 report available?
HLDC-04	Does your organization have physical security controls and policies in place?

HLDC-05	Do you have physical access control and video surveillance to prevent/detect unauthorized access to your data center?
Networking	
HLNT-01	Do you enforce network segmentation between trusted and untrusted networks (i.e., Internet, DMZ, Extranet, etc.)?
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?
HLNT-04	Are you employing any next-generation persistent threat (NGPT) monitoring?
HLNT-05	Do you require connectivity to the institution's network for support/administration or access into any existing systems for integration purposes?
Incident Handling	
HLIH-01	Do you have a formal incident response plan?

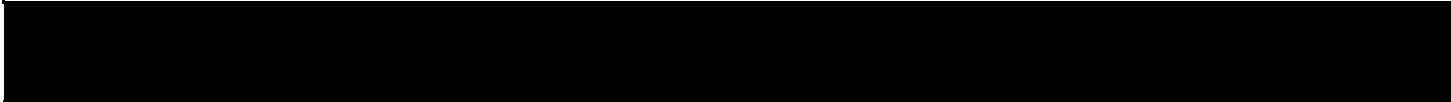
HLIH-02	Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?
HLIH-03	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?
HLIH-04	Do you have either an internal incident response team or retain an external team?
HLIH-05	Do you have the capability to respond to incidents on a 24 x 7 x 365 basis?

Policies, Procedures, and Processes

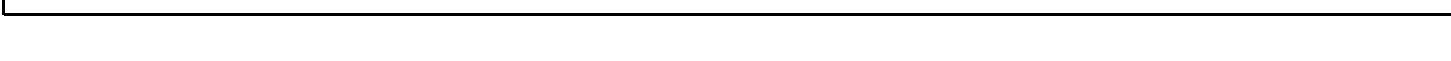
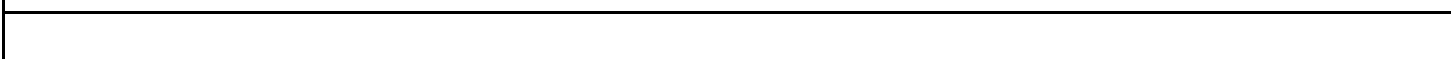
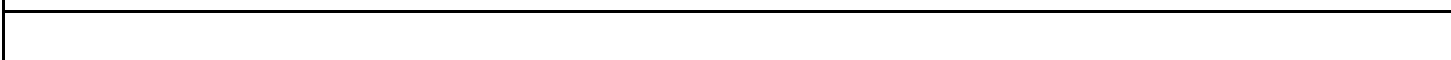
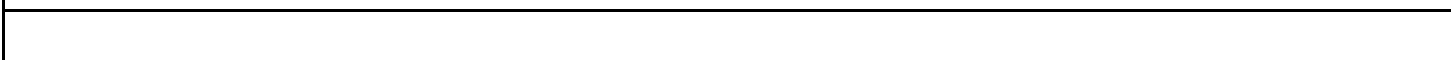
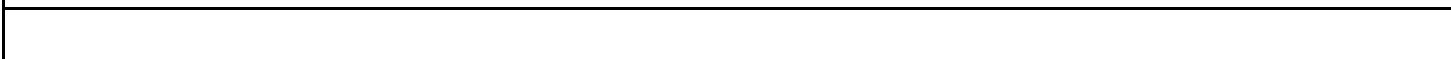
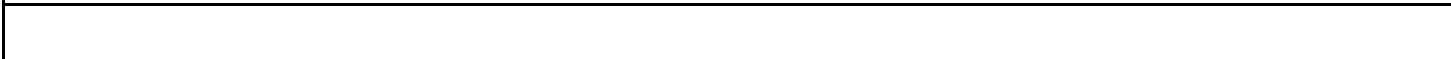
HLPP-01	Can you share the organization chart, mission statement, and policies for your information security unit?
HLPP-02	Are information security principles designed into the product lifecycle?
HLPP-03	Do you have a documented information security policy?

Third Party Assessment

HLTP-01	Will institutional 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)
HLTP-02	Do you perform security assessments of third-party companies with which you share data? (e.g., hosting providers, cloud services, PaaS, IaaS, SaaS)
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., telecommunications equipment, export licensing, computing devices)



to as "product") will access and/or host institutional data must complete the Higher Education Data Access and Use Policy (HDAUP) encompassing term including at least data and metadata. Answers will be reviewed by institution and must comply with institution policy and state and federal laws. This is intended for use by vendors.





t-in formatting logic relies on this order.
requesting institution.

Vendor Answers	Additional Information
-----------------------	-------------------------------

--	--

--	--

Vendor Answers	Additional Information

Vendor Answers	Additional Information

Vendor Answers	Additional Information

Vendor Answers	Additional Information

Vendor Answers	Additional Information

Vendor Answers	Additional Information

Vendor Answers	Additional Information
Vendor Answers	Additional Information

Vendor Answers	Additional Information

Additional Information

Version 3.06

ation Community Vendor
ion security analysts upon
ors participating in a Third-Party

Share any details that would help information security analysts assess your product.	
Guidance	Analyst Notes

A HECVAT Full is recommended if this level of full NIST SP 800-171 compliance is required for the application.	

If your answer is "I do not know," select "No." If the VPAT/ACR is for an older version of the product or has not been updated, its information does not accurately reflect accessibility of the product under consideration.	

Guidance	Analyst Notes

Guidance	Analyst Notes
This includes end-users, administrators, service accounts, etc. PBAC would include various dynamic controls such as conditional access, risk-based access, location-based access, or system activity based access.	

<p>This includes system administrators and third party personnel with access to the system. PBAC would include various dynamic controls such as conditional access, risk-based access, location-based access, or</p>	
<p>Include any in-house developed or contract development</p>	
<p>Guidance</p>	<p>Analyst Notes</p>

Answer "Yes" only if user AND administrator authentication is supported. If partially supported, answer "No." Ensure you respond to any guidance in the Additional Information column.	
An answer of "Yes" should be well-supported in the Additional Information column, and all elements of interest should be sufficiently addressed.	

Guidance	Analyst Notes

Guidance	Analyst Notes
Ensure that response addresses involatile storage.	

Guidance	Analyst Notes
Please indicate which geographic regions you can provide storage in the Additional Information column.	
If not using a hosting provider, you are the hosting provider; answer accordingly.	

Guidance	Analyst Notes
Describe this connectivity.	
Guidance	Analyst Notes

Guidance	Analyst Notes

Guidance	Analyst Notes
The institution views hosted solutions such as AWS, Rackspace, Azure, and other PaaS/SaaS offerings as third parties. If services such as these are used in your environment, respond "Yes."	
Ensure that all elements of HLTP-01 are clearly stated in your response.	
Robust answers from the vendor improve the quality and efficiency of the security assessment process.	
Make sure you address any national or regional regulations.	

HECVAT - Lite | Analyst Report

Institution Assessment

Instructions

Step 1: Select the security framework used at your institution in cell C10. s
population of report. **Step 4:** Move to the Summary Report tab.

Vendor Name	
Vendor Contact Name	
Vendor Contact Title	
Vendor Email Address	

Step 1: Select your institution's security framework

Report Sections
Company
Documentation
IT Accessibility
Application Security
Authentication, Authorization, and Accounting

Systems Management
Data
Datacenter
Networking
Incident Handling
Policies, Procedures, and Practices
Third Party Assessment
Overall Score

ID	Question	Vendor Answer
		The vendor's selected responses are displayed here for easier reference.
Company Overview	Question	Vendor Answer
COMP-01	Describe your organization's business background and	
COMP-02	Have you had an unplanned disruption to this product/service in	0

COMP-03	Do you have a dedicated Information Security staff or office?	0
COMP-04	Do you have a dedicated Software and System Development team(s)?	0
COMP-05	Does your product process protected health information (PHI) or any	0
COMP-06	Will data regulated by PCI DSS reside in the vended product?	0
COMP-07	Use this area to share information about your environment that will	

Documentation	Question	Vendor Answer
DOCU-01	Have you undergone a SSAE 18 / SOC 2 audit?	0
DOCU-02	Have you completed the Cloud Security Alliance (CSA) CAIQ?	0
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	0
DOCU-04	Do you conform with a specific industry standard security	0
DOCU-05	Can the systems that hold the institution's data be compliant with	0
DOCU-06	Can you provide overall system and/or application architecture	0
DOCU-07	Does your organization have a data privacy policy?	0
DOCU-08	Do you have a documented, and currently implemented,	0

DOCU-09	Do you have a well-documented Business Continuity Plan (BCP)	0
DOCU-10	Do you have a well-documented Disaster Recovery Plan (DRP)	0
DOCU-11	Do you have a documented change management process?	0
DOCU-12	Has a VPAT or ACR been created or updated for the product and version	0
DOCU-13	Do you have documentation to support the accessibility	0
IT Accessibility		
	Question	Vendor Answer
ITAC-01	Has a third-party expert conducted an accessibility audit of the	0
ITAC-02	Do you have a documented and implemented process for	0
ITAC-03	Have you adopted a technical or legal accessibility standard of	0
ITAC-04	Can you provide a current, detailed accessibility roadmap	0
ITAC-05	Do you expect your staff to maintain a current skill set in IT	0
ITAC-06	Do you have a documented and implemented process for	0
ITAC-07	Do you have documented processes and procedures for	0
ITAC-08	Can all functions of the application or service be performed using only the	0

ITAC-09	Does your product rely on activating a special "accessibility mode," a	0
---------	--	---

Application/Service Security	Question	Vendor Answer
-------------------------------------	-----------------	----------------------

HLAP-01	Are access controls for institutional accounts based on structured	0
---------	--	---

HLAP-02	Are access controls for staff within your organization based on	0
---------	---	---

HLAP-03	Do you have a documented and currently implemented	0
---------	--	---

HLAP-04	Does the system provide data input validation and error messages?	0
---------	---	---

HLAP-05	Are you using a web application firewall (WAF)?	0
---------	---	---

HLAP-06	Do you have a process and implemented procedures for managing	0
---------	---	---

Authentication, Authorization, and Accounting	Question	Vendor Answer
--	-----------------	----------------------

HLAA-01	Does your solution support single sign-on (SSO) protocols for user	0
---------	--	---

HLAA-02	Does your organization participate in InCommon or another eduGAIN-	0
---------	--	---

HLAA-03	Does your application support integration with other authentication and authorization systems?	0
---------	--	---

HLAA-04	Does your solution support any of the following Web SSO	0
---------	---	---

HLAA-05	Do you support differentiation between email address and user	0
HLAA-06	Do you allow the customer to specify attribute mappings for any needed information	0
HLAA-07	Are audit logs available to the institution that include AT LEAST all of the following: login, logout, actions performed, timestamp	0
HLAA-08	If you don't support SSO, does your application and/or user-frontend/portal support multi-factor	0
HLAA-09	Does your application automatically lock the session or log-out an	0

Systems Management	Question	Vendor Answer
---------------------------	-----------------	----------------------

HLSY-01	Do you have a systems management and configuration strategy	0
HLSY-02	Will the institution be notified of major changes to your	0
HLSY-03	Are your systems and applications scanned for vulnerabilities [that are	0
HLSY-04	Have your systems and applications had a third-party security	0
HLSY-05	Do you have policy and procedure, currently implemented, guiding	0

Data	Question	Vendor Answer
-------------	-----------------	----------------------

HLDA-01	Does the environment provide for dedicated single-tenant	0
---------	--	---

HLDA-02	Is sensitive data encrypted, using secure protocols/algorithms, in	0
HLDA-03	Is sensitive data encrypted, using secure protocols/algorithms, in	0
HLDA-04	Are involatile backup copies made according to predefined schedules	0
HLDA-05	Can the institution extract a full or partial backup of data?	0
HLDA-06	Do you have a media handling process that is documented and	0
HLDA-07	Does your staff (or third party) have access to institutional data (e.g.,	0

Datacenter	Question	Vendor Answer
-------------------	-----------------	----------------------

HLDC-01	Does your company manage the physical data center where the	0
HLDC-02	Are you generally able to accomodate storing each institution's data within	0
HLDC-03	Does the hosting provider have a SOC 2 Type 2 report available?	0
HLDC-04	Does your organization have physical security controls and policies in	0
HLDC-05	Do you have physical access control and video surveillance to	0

Networking	Question	Vendor Answer
-------------------	-----------------	----------------------

HLNT-01	Do you enforce network segmentation between trusted and untrusted	0
---------	---	---

HLNT-02	Are you utilizing a stateful packet inspection (SPI) firewall?	0
HLNT-03	Do you use an automated IDS/IPS system to monitor for	0
HLNT-04	Are you employing any next-generation persistent threat (NGPT)	0
HLNT-05	Do you require connectivity to the institution's network for	0

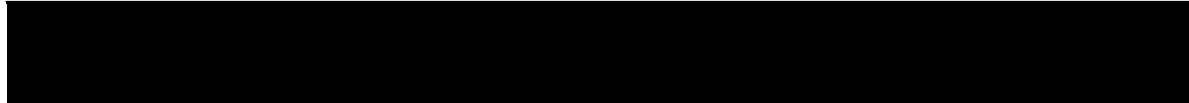
Incident Handling	Question	Vendor Answer
--------------------------	-----------------	----------------------

HLIH-01	Do you have a formal incident response plan?	0
HLIH-02	Do you have an incident response process and reporting in place to	0
HLIH-03	Do you carry cyber-risk insurance to protect against unforeseen	0
HLIH-04	Do you have either an internal incident response team or retain	0
HLIH-05	Do you have the capability to respond to incidents on a 24 x 7 x	0

Policies, Procedures, and Processes	Question	Vendor Answer
--	-----------------	----------------------

HLPP-01	Can you share the organization chart, mission statement, and	0
HLPP-02	Are information security principles designed into the product lifecycle?	0
HLPP-03	Do you have a documented information security policy?	0

Third Party Assessment	Question	Vendor Answer
HLTP-01	Will institutional data be shared with or hosted by any third parties? (e.g.,	0
HLTP-02	Do you perform security assessments of third-party companies with	0
HLTP-03	Do you have an implemented third-party management strategy?	0
HLTP-04	Do you have a process and implemented procedures for managing	0



Step 2: Convert qualitative vendor responses into quantitative values, sta

		Product Name
		Product Description
		HECVAT Version
		Date Prepared

Max_Score		Score
135		0
215		0
180		0
130		0
185		0

70		0
165		0
160		0
155		0
155		0
85		0
120		0
1755		0

	Analyst Notes	Step 2: Override/Case Use Case
Additional Information	Notes shown in Col F on HECVAT - Lite tab)	Preferred Response
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.
Additional Information		Preferred Response
0		Qualitative Question
0		No

0		No
---	--	----

Additional Information		Preferred Response
-------------------------------	--	---------------------------

0		Yes
---	--	-----

0		Yes
---	--	-----

0		Yes
---	--	-----

0		Yes
---	--	-----

0		Yes
---	--	-----

0		Yes
---	--	-----

Additional Information		Preferred Response
-------------------------------	--	---------------------------

0		Yes
---	--	-----

0		Yes
---	--	-----

0		Yes
---	--	-----

0		Yes
---	--	-----

0		Yes
0		Yes
0		Yes
0		Yes
0		Yes

Additional Information	Preferred Response
-------------------------------	---------------------------

0		Yes
0		Yes
0		Yes
0		Yes
0		Yes

Additional Information	Preferred Response
-------------------------------	---------------------------

0		Yes
---	--	-----

0		Yes
0		Yes
0		Yes
0		Yes
0		Yes
0		No

Additional Information		Preferred Response
-------------------------------	--	---------------------------

0		No
0		Yes
0		Yes
0		Yes
0		Yes

Additional Information		Preferred Response
-------------------------------	--	---------------------------

0		Yes
---	--	-----

0		Yes
0		Yes
0		Yes
0		Yes

Additional Information		Preferred Response
-------------------------------	--	---------------------------

0		Yes
0		Yes
0		Yes
0		Yes
0		Yes

Additional Information		Preferred Response
-------------------------------	--	---------------------------

0		Yes
0		Yes
0		Yes

Additional Information		Preferred Response
0		No
0		Yes
0		Yes
0		Yes

Version 3.06

orting at cell G31. **Step 3:** Review converted values, ensuring full

Lite

1/0/1900

Score %

0%

0%

0%

0%

0%

0%
0%
0%
0%
0%
0%
0%
0%
0%

Correct Vendor Responses and Set Weights Per Institution's

Compliant Override	Default Weight	Weight Override
Analysts should use this drop-down 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.
Compliant Override	Default Weight	Weight Override
	5	
	20	

	10	
	15	
	40	
	40	
	5	
Compliant Override	Default Weight	Weight Override
	15	
	10	
	15	
	25	
	10	
	25	
	20	
	10	

	20	
Compliant Override	Default Weight	Weight Override
	25	
	15	
	20	
	25	
	25	
	20	
Compliant Override	Default Weight	Weight Override
	20	
	20	
	15	
	20	

	20	
	20	
	40	
	15	
	15	
Compliant Override	Default Weight	Weight Override
	15	
	15	
	10	
	15	
	15	
Compliant Override	Default Weight	Weight Override
	25	

	20	
	20	
	15	
	25	
	20	
	40	
Compliant Override	Default Weight	Weight Override
	0	
	40	
	40	
	40	
	40	
Compliant Override	Default Weight	Weight Override
	40	

	40	
	40	
	20	
	15	

Compliant Override	Default Weight	Weight Override
-------------------------------	-----------------------	------------------------

	40	
	15	
	20	
	40	
	40	

Compliant Override	Default Weight	Weight Override
-------------------------------	-----------------------	------------------------

	20	
	25	
	40	

Compliant Override	Default Weight	Weight Override
	0	
	40	
	40	
	40	

HECVAT - Lite | Analyst Reference

Connect with your higher education peers by joining the **EDUCAUSE HE**

Instructions

Use this reference guide to assess vendor responses in relation to your institution's er these recommendations and follow-up response are not exhaustive and are meant to

Analyst tip #1: For any answer that is deemed "noncompliant" by your institution, as development engagement, and/or possible implementation of compensating control(s)

Analyst tip #2: If a vendor's response to a follow-up inquiry is vague or seems off-p Responses that fail to meet expectations thereafter should be negatively assessed bas

Analyst tip #3: This is the most important tip. Reject a HECVAT from a vendor if the vague and/or do not answer questions directly, or if significant discrepancies are found

Company Overview

COMP-01	Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.
---------	--

COMP-02	Have you had an unplanned disruption to this product/service in the past 12 months?
COMP-03	Do you have a dedicated Information Security staff or office?
COMP-04	Do you have a dedicated Software and System Development team(s)? (e.g., Customer Support, Implementation, Product Management, etc.)
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?
COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.
Documentation	
DOCU-01	Have you undergone a SSAE 18 / SOC 2 audit?
DOCU-02	Have you completed the Cloud Security Alliance (CSA) CAIQ?
DOCU-03	Have you received the Cloud Security Alliance STAR certification?

DOCU-04	Do you conform with a specific industry standard security framework? (e.g., NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)
DOCU-05	Can the systems that hold the institution's data be compliant with NIST SP 800-171 and/or CMMC Level 2 standards?
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-07	Does your organization have a data privacy policy?

DOCU-08	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?
DOCU-09	Do you have a well-documented Business Continuity Plan (BCP) that is tested annually?
DOCU-10	Do you have a well-documented Disaster Recovery Plan (DRP) that is tested annually?
DOCU-11	Do you have a documented 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?
DOCU-13	Do you have documentation to support the accessibility features of your product?
Application/Service Security	
ITAC-01	Has a third-party expert conducted an accessibility audit of the most recent version of your product?

ITAC-02	Do you have a documented and implemented process for verifying accessibility conformance?
ITAC-03	Have you adopted a technical or legal accessibility standard of conformance for the product in question?
ITAC-04	Can you provide a current, detailed accessibility roadmap with delivery timelines?

ITAC-05	Do you expect your staff to maintain a current skill set in IT accessibility?
ITAC-06	Do you have a documented and implemented process for reporting and tracking accessibility issues?
ITAC-07	Do you have documented processes and procedures for implementing accessibility into your development lifecycle?
ITAC-08	Can all functions of the application or service be performed using only the keyboard?

ITAC-09	Does your product rely on activating a special "accessibility mode," a "lite version," or accessing an alternate interface for accessibility purposes?
---------	--

Application/Service Security

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)?
---------	---

HLAP-02	Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?
---------	--

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)?
HLAP-04	Does the system provide data input validation and error messages?
HLAP-05	Are you using a web application firewall (WAF)?

HLAP-06	Do you have a process and implemented procedures for managing your software supply chain (e.g., libraries, repositories, frameworks, etc.)?
Authentication, Authorization, and Accounting	
HLAA-01	Does your solution support single sign-on (SSO) protocols for user and administrator authentication?
HLAA-02	Does your organization participate in InCommon or another eduGAIN-affiliated trust federation?

HLAA-03	Does your application support integration with other authentication and authorization systems?
HLAA-04	Does your solution support any of the following Web SSO standards? [e.g., SAML2 (with redirect flow), OIDC, CAS, or other]
HLAA-05	Do you support differentiation between email address and user identifier?
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)

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?
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.)
HLAA-09	Does your application automatically lock the session or log-out an account after a period of inactivity?
Systems Management	
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)?

HLSY-02	Will the institution be notified of major changes to your environment that could impact the institution's security posture?
HLSY-03	Are your systems and applications scanned for vulnerabilities [that are then remediated] prior to new releases?
HLSY-04	Have your systems and applications had a third-party security assessment completed in the past year?
HLSY-05	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?

Data

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).
HLDA-02	Is sensitive data encrypted, using secure protocols/algorithms, in transport? (e.g., system-to-client)
HLDA-02	Is sensitive data encrypted, using secure protocols/algorithms, in transport? (e.g., system-to-client)
HLDA-03	Is sensitive data encrypted, using secure protocols/algorithms, in storage? (e.g., disk encryption, at-rest, files, and within a running database)

HLDA-04	Are involatile backup copies made according to predefined schedules and securely stored and protected?
HLDA-05	Can the institution extract a full or partial backup of data?
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?
Datacenter	
HLDC-01	Does your company manage the physical data center where the institution's data will reside?

HLDC-02	Are you generally able to accomodate storing each institution's data within their geographic region?
HLDC-03	Does the hosting provider have a SOC 2 Type 2 report available?
HLDC-04	Does your organization have physical security controls and policies in place?

HLDC-05	Do you have physical access control and video surveillance to prevent/detect unauthorized access to your data center?
---------	---

Networking

HLNT-01	Do you enforce network segmentation between trusted and untrusted networks (i.e., Internet, DMZ, Extranet, etc.)?
---------	---

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?
HLNT-04	Are you employing any next-generation persistent threat (NGPT) monitoring?
HLNT-05	Do you require connectivity to the institution's network for support/administration or access into any existing systems for integration purposes?

Incident Response

HLIH-01	Do you have a 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?
HLIH-03	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?
HLIH-04	Do you have either an internal incident response team or retain an external team?

HLIH-05	Do you have the capability to respond to incidents on a 24 x 7 x 365 basis?
---------	---

Policies, Procedures, and Processes

HLPP-01	Can you share the organization chart, mission statement, and policies for your information security unit?
---------	---

HLPP-02	Are information security principles designed into the product lifecycle?
---------	--

HLPP-03	Do you have a documented information security policy?
---------	---

Third Party Assessment

HLTP-01	Will institutional 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)
---------	--

HLTP-02	Do you perform security assessments of third-party companies with which you share data? (e.g., hosting providers, cloud services, PaaS, IaaS, SaaS)
---------	---

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., telecommunications equipment, export licensing, computing devices)

HECVAT Users Community Group at <https://connect.educause.edu>.

environment. The context of HECVAT questions can change, depending on implementation specifics, so improve assessment and report capabilities within your institution's security/risk assessment program.

ask the vendor if there is a timeline for implementation, a sincere commitment to customer service, and other factors that offset the risks of another component.

If the response is evasive, vague, or dismissive, respond back to the vendor contact with clear expectations for a response. Consider the vendor's response based on your institution's risk tolerance and the criticality of the data involved.

If the vendor provides the institution with an insufficiently populated HECVAT, if the vendor responses are incomplete or unclear, making the HECVAT difficult to assess.

Reason for Question	Follow-up Inquiries/Responses
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."

<p>We want transparency from the vendor and an honest answer to this question, regardless of the response, is a good step in building trust.</p>	<p>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 circumstances of the incident and what the vendor has done in response to the breach.</p>
<p>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.</p>	<p>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.</p>
<p>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.</p>	<p>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.</p>
<p>Responses to this question may indicate the presence of PHI data in the vended product.</p>	<p>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.</p>

<p>Responses to this question may indicate the presence of PCI DSS regulated data in the vended product.</p>	<p>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.</p>
<p>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 irrelevant information. Thorough documentation, supporting evidence, and/or robust responses go a long way in building trust in this assessment process.</p>	<p>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.</p>
<p>Reason for Question</p>	<p>Follow-up Inquiries/Responses</p>
<p>Standard documentation, relevant to institutions requiring a vendor to undergo SSAE 18 audits.</p>	<p>Follow-up inquiries for SSAE 18 content will be institution/implementation specific.</p>
<p>Many vendors have populated a CAIQ or at least a self-assessment. Although lacking in some areas important to higher education, these documents are useful for supplemental assessment.</p>	<p>Follow-up inquiries for CSA content will be institution/implementation specific.</p>
<p>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.</p>	<p>If STAR certification is important to your institution you may have specific follow-up details for documentation purposes.</p>

<p>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.</p>	<p>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.</p>
<p>For institutions that collaborate with the United States government, FISMA compliance may be required.</p>	<p>Follow-up inquiries for FISMA compliance will be institution/implementation specific.</p>
<p>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.</p>	<p>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).</p>
<p>Managing and protecting institutional 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.</p>	<p>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.</p>

<p>Managing and protecting a vendor's assets through appropriate human resource management is of the utmost 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).</p>	<p>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.</p>
<p>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).</p>	<p>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</p>
<p>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.</p>	<p>If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164</p>
<p>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).</p>	<p>If a weak response is given to this answer, response scrutiny should be increased. Questions about configuration management, system authority, and documentation are appropriate.</p>

<p>A combination of most responses to Q-03 would be ideal and a sign of a mature accessibility program. The goal of accessibility is ultimately usability by persons with disabilities, and so successful testing among that population indicates greater access. Expert staff and automated testing are important, but automated tools can only detect ~25% of issues so must be supplemented with additional methodologies. The use of overlays or plugins to help products "automatically conform" with accessibility guidelines are presently inadequate and should impact scores negatively.</p>	<p>Follow-up inquiries for IT Accessibility content will be institution/implementation specific.</p>
<p>The Web Content Accessibility Guidelines (WCAG) <https://www.w3.org/WAI/standards-guidelines/wcag> from the W3C are widely accepted measures of accessibility conformance. WCAG AA conformance is the most common level of accessibility adoption, with preference given to the most recently released version: 2.1 (released 2018) or 2.0 (released 2008). Additionally, some federal or local requirements may incorporate or supplement the technical standards, including Section 508 <https://www.section508.gov/manage/laws-and-policies> of the Rehabilitation Act (U.S.), EN 301 549 <https://ec.europa.eu/eip/ageing/standards/ict-and-communication/accessibility-and-design-for-all_en.html> (E.U.) etc.</p>	<p>If a vendor is unfamiliar with either, they may be directed to learn more about technical <https://www.w3.org/WAI/> or governmental <https://www.section508.gov/> standards for accessibility.</p>
<p>If products do not fully conform to accessibility standards, it is important that vendors have a roadmap specifying how they will work to achieve it. A roadmap with delivery timelines is best supported by evidence of prior delivery on such timelines. Analysts can better predict time to conformance and institutions can plan accordingly.</p>	<p>Follow-up inquiries for IT Accessibility content will be institution/implementation specific.</p>

<p>Having accessibility expertise within the staff supports the proactive development of accessible products. If staff lack sufficient accessibility expertise, then accessibility improvements may only be the result of the vendor reacting to issues or reports of access barriers submitted by clients of the vendor.</p>	<p>Follow-up inquiries for IT Accessibility content will be institution/implementation specific.</p>
<p>Tracking and addressing technical issues is a natural part of any web or software product. Critical accessibility issues can cause a product to become unusable. Vendors should have a process to intake, triage, and address accessibility issue reports. Vendors that treat accessibility as "feature requests" for future versions of a product or as nontracked bug reports (i.e., bug reports lacking accessibility tags) should score lower.</p>	<p>Follow-up inquiries for IT Accessibility content will be institution/implementation specific.</p>
<p>This question is designed to understand how accessibility is included in new versions and features of products, particularly with vendors that implement Agile or similar methodologies where software is updated frequently and continuously.</p>	<p>Follow-up inquiries for IT Accessibility content will be institution/implementation specific.</p>
<p>One critical accessibility requirement is the full use of a product using only the keyboard--no mouse or trackpad. This requirement is easy for a nontechnical or non-accessibility expert to understand and verify.</p>	<p>Follow-up inquiries for IT Accessibility content will be institution/implementation specific.</p>

<p>Separate accessibility modes or interfaces are indicative of a product design creating an attempted "separate but equal" environment for disabled users. In practice, separate modes or interfaces for accessibility almost never have feature parity and typically get new features less frequently and after the primary version. They therefore provide unequal experiences for disabled users compared with their non-disabled peers. Interfaces, overlays, or extensions that create a separate experience or mimic such an environment should be avoided.</p>	<p>Follow-up inquiries for IT Accessibility content will be institution/implementation specific.</p>
<p>Reason for Question</p>	<p>Follow-up Inquiries/Responses</p>
<p>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.</p>	<p>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.</p>
<p>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.</p>	<p>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.</p>

<p>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. In the context of the CIA triad, this question is focused on confidentiality. Printed</p>	<p>Request additional documentation that outlines the security controls implemented to safeguard your institutional data.</p>
<p>Input validation is a secure coding best practice, 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.</p>	<p>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.</p>
<p>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.</p>	<p>If a vendor 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.</p>

<p>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.</p>	<p>Follow-up inquiries concerning software supply chain will be institution/implementation specific.</p>
<p>Reason for Question</p>	<p>Follow-up Inquiries/Responses</p>
<p>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.</p>	<p>Follow-up inquiries for IAM requirements will be institution/implementation specific.</p>
<p>This question defines the vendor's scope of federated identity practices and their willingness to embrace higher education requirements.</p>	<p>If a vendor indicates that a system is stand-alone 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.</p>

<p>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.</p>	<p>If a vendor indicates that a system is stand-alone 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.</p>
<p>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.</p>	<p>Follow-up inquiries for IAM requirements will be institution/implementation specific.</p>
<p>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.</p>	<p>Follow-up inquiries for identifier requirements will be institution/implementation specific.</p>
<p>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.</p>	<p>Follow-up inquiries for attribute mapping requirements will be institution/implementation specific.</p>

<p>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.</p>	<p>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.</p>
<p>2FA/MFA, implemented correctly, strengthens the security state of a system. 2FA/MFA is commonly implemented and in many use cases is a requirement for account protection purposes.</p>	<p>Ask the vendor about hardware and software options, future roadmap for implementations and support, etc.</p>
<p>This is a question to ensure account integrity and institutional data confidentiality.</p>	<p>Follow-up inquiries for IAM requirements will be institution/implementation specific.</p>
Reason for Question	Follow-up Inquiries/Responses
<p>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.</p>	<p>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.</p>

<p>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.</p>	<p>If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.</p>
<p>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 nonexistent risks are not introduced into a known, secured environment.</p>	<p>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.</p>
<p>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.</p>	<p>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.</p>
<p>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.</p>	<p>Follow-up inquiries for the vendors patching practices will be institution/implementation specific.</p>

Reason for Question	Follow-up Inquiries/Responses
<p>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.</p>	<p>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.</p>
<p>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.</p>	<p>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.</p>
<p>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.</p>	<p>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.</p>
<p>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.</p>	<p>Follow-up inquiries for data encryption at-rest will be institution/implementation specific.</p>

<p>An institution's location will dictate what laws and regulations apply to them. As vendors may not know where all of their customers may reside, it is imperative that vendors are able to accommodate geographic requirements for their customers. Although it is unfair to expect support for all geographic regions in common infrastructure/platform/software-as-a-service, vendors are expected to be absolutely clear about the regions they leverage and/or support.</p>	<p>If a vendor is unable to accommodate storing/processing institutional data within specific regions, ask them why they are unable to. Try to determine if it's an infrastructure issue (scalability), a cost-reduction strategy (size/maturity), or some other issue.</p>
<p>Understanding the ownership structure of the facility that will host institutional data is important for setting availability expectations and ensuring 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.</p>	<p>Follow-up inquiries for additional vendor's SOC 2 Type 2 reports will be institution/implementation specific.</p>
<p>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.</p>	<p>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, and 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.</p>

<p>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.</p>	<p>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.</p>
<p>Reason for Question</p>	<p>Follow-up Inquiries/Responses</p>
<p>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 be appropriately implemented and maintained.</p>	<p>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.</p>
<p>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.</p>	<p>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.</p>

<p>It is important to have detective capabilities in an information system to protect institutional data. Because this is somewhat expected in information systems, vendors without IDSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the vendor.</p>	<p>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.</p>
<p>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.</p>	<p>Follow-up inquiries for NGPT monitoring will be institution/implementation specific.</p>
<p>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.</p>	<p>Follow-up inquiries for institution network connectivity resource requirements will be institution/implementation specific.</p>

Reason for Question	Follow-up Inquiries/Responses
<p>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.</p>	<p>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</p>
<p>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.</p>	<p>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</p>
<p>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.</p>	<p>Follow-up inquiries for cyber-risk insurance will be institution/implementation specific.</p>
<p>The incident team structure (internal vs. external), size, and capabilities of a vendor have 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.</p>	<p>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</p>

<p>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.</p>	<p>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</p>
<p>Reason for Question</p>	<p>Follow-up Inquiries/Responses</p>
<p>Understanding the security program size (and capabilities) of a vendor has a significant impact on their ability to respond effectively to a security incident. Vendors 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.</p>	<p>Vague responses to this question should be investigated further. Vendors unwilling to share additional supporting documentation decrease the trust established with other responses.</p>
<p>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.</p>	<p>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</p>

<p>A shared security [responsibility] environment is expected of vendors in today's world. Security offices 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. 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</p>	<p>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.</p>
<p>Reason for Question</p>	<p>Follow-up Inquiries/Responses</p>
<p>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.</p>	<p>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).</p>
<p>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.</p>	<p>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.</p>

<p>Every organization needs to actively understand and manage their supply chain and the 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 taking on by contracting with them. Modern technologies allow for rapid deployment of features and with them, come changes to an</p>	<p>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.</p>
<p>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.</p>	<p>Follow-up inquiries concerning hardware supply chain will be institution/implementation specific.</p>

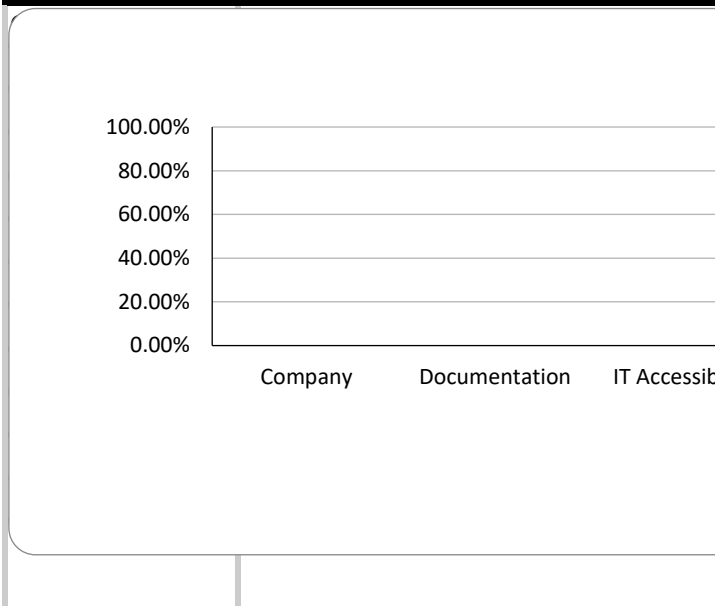
HECVAT - Lite | Summary

--	--

Vendor	
---------------	--

Description	
--------------------	--

--	--



High Risk, Noncompliant Resp

--	--

ID	Question
-----------	-----------------

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.)
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?

HLAP-05	Are you using a web application firewall (WAF)?
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,
HLDA-05	Can the Institution extract a full or partial backup of data?
HLDC-02	Are you generally able to accomodate storing each institution's data within their geographic region?
HLDC-03	Does the hosting provider have a SOC 2 Type 2 report available?
HLDC-04	Does your organization have physical security controls and policies in place?
HLDC-05	Do you have physical access control and video surveillance to prevent/detect unauthorized
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?
HLIH-04	Do you have either an internal incident response team or retain an external
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, PaaS, IaaS, SaaS, etc.).
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., telecommunications equipment, export licensing, computing devices)

Summary Report

	Product
--	----------------

--	--

	0%
--	----

Scores by Section

Availability Application Security Authentication, Authorization, and Accounting Systems Management Data Datacenter Network

Responses

	Institution's Score
--	----------------------------

Additional Info	
------------------------	--

HECVAT - Lite | Standards Crosswalk

HEISC Shared Assessments Working Group

Standard Reference URL:		https://www.cisecurity.org/controls/	https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/	https://www.iso.org/standard/54533.html	https://www.nist.gov/cyberframework	https://csrc.nist.gov/publications/detail/sp/800-171/rev-2
Company Overview		CIS Critical Security Controls v8.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r2
COMP-01	Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.					
COMP-02	Have you had an unplanned disruption to this product/service in the past 12 months?					
COMP-03	Do you have a dedicated Information Security staff or office?			15.2.1		
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		
COMP-06	Will data regulated by PCI DSS reside in the vended product?			14.2.1		
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		
Documentation		CIS Critical Security Controls v8.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r2
DOCU-01	Have you undergone a SSAE 18 / SOC 2 audit?			15.2.1		
DOCU-02	Have you completed the Cloud Security Alliance (CSA) CAIQ?			15.2.1		
DOCU-03	Have you received the Cloud Security Alliance STAR certification?			15.2.1		
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		
DOCU-05	Can the systems that hold the institution's data be compliant with NIST SP 800-171 and/or CMMC Level 2 standards?			18.1.1		

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	
DOCU-07	Does your organization have a data privacy policy?					
DOCU-08	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?					
DOCU-09	Do you have a well-documented Business Continuity Plan (BCP) that is tested annually?					
DOCU-10	Do you have a well-documented Disaster Recovery Plan (DRP) that is tested annually?					
DOCU-11	Do you have a documented change management process?					3.4.3
Application/Service Security		CIS Critical Security Controls v8.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r2
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
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
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
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	
HLAP-05	Are you using a web application firewall (WAF)?	CSC 16		14.2.5	PR.DS-6	
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		
Authentication, Authorization, and Accounting		CIS Critical Security Controls v8.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r2
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
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

HLAA-03	Does your application support integration with other authentication and authorization systems?	CSC 16		9.4.3	PR.AC-1, PR.AC-4	
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	
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
Systems Management		CIS Critical Security Controls v8.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r2
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
HLSY-02	Will the institution be notified of major changes to your environment that could impact the institution's security posture?					3.4.4
HLSY-03	Are your systems and applications scanned for vulnerabilities [that are then remediated] prior to new releases?					3.11.2
HLSY-04	Have your systems and applications had a third-party security assessment completed in the past year?					
HLSY-05	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?					3.14.1
Data		CIS Critical Security Controls v8.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r2
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
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
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
HLDA-04	Are involatile backup copies made according to predefined schedules and securely stored and protected?	CSC 13		12.3.1		3.8.9
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
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	

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?					
Datacenter		CIS Critical Security Controls v8.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r2
HLDC-01	Does your company manage the physical data center where the institution's data will reside?	CSC 12		11.2.1		
HLDC-02	Are you generally able to accommodate storing each institution's data within their geographic region?	CSC 14		11.1.1	PR.AC-2, PR.IP-5	
HLDC-03	Does the hosting provider have a SOC 2 Type 2 report available?	CSC 13		11.1.1		
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
HLDC-05	Do you have physical access control and video surveillance to prevent/detect unauthorized access to your data center?					3.10.2
Networking		CIS Critical Security Controls v8.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r2
HLNT-01	Do you enforce network segmentation between trusted and untrusted networks (i.e., Internet, DMZ, Extranet, etc.)?					3.13.1, 3.13.5
HLNT-02	Are you utilizing a stateful packet inspection (SPI) firewall?					3.1.3
HLNT-03	Do you use an automated IDS/IPS system to monitor for intrusions?					3.14.6
HLNT-04	Are you employing any next-generation persistent threat (NGPT) monitoring?					
HLNT-05	Do you require connectivity to the institution's network for support/administration or access into any existing systems for integration purposes?					
Incident Response		CIS Critical Security Controls v8.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r2
HLIH-01	Do you have a formal incident response plan?					3.6.1
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

HLIH-03	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?					
HLIH-04	Do you have either an internal incident response team or retain an external team?					3.6.1
HLIH-05	Do you have the capability to respond to incidents on a 24 x 7 x 365 basis?					
Policies, Procedures, and Processes		CIS Critical Security Controls v8.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r2
HLPP-01	Can you share the organization chart, mission statement, and policies for your information security unit?					
HLPP-02	Are information security principles designed into the product lifecycle?					
HLPP-03	Do you have a documented information security policy?					
Third Party Assessment		CIS Critical Security Controls v8.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r2
HLTP-01	Will institutional 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)					
HLTP-02	Do you perform security assessments of third-party companies with which you share data? (e.g., hosting providers, cloud services, PaaS, IaaS, SaaS)					
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., telecommunications equipment, export licensing, computing devices)					



https://csrc.nist.gov/publications/detail/sp/800-53/rev-	https://www.trustedci.org/framework/core	https://www.pcisecuritystandards.org/document_library
---	---	---

NIST SP 800-53r5	Trusted CI	PCI DSS 3.2.1
	1: Mission Focus, 2: Stakeholders and obligations	
	10: Evaluation and Refinement	
	7: Cybersecurity Lead, 13: Personnel	
	2: Stakeholders and Obligations	
	2: Stakeholders and Obligations	
		PCI-DSS SAQs - part 2

NIST SP 800-53r5	Trusted CI	PCI DSS 3.2.1
SA-9	10: Evaluation & Refinement	
PE-2, PE-3, PE-5, PE-11, PE-13, PE-14, SA-9	10: Evaluation & Refinement, 14 external resources	
PE-2, PE-3, PE-5, PE-11, PE-13, PE-14, SA-9	10: Evaluation & Refinement	
SA-9	15: Baseline Control Set	
SA-9	2: Stakeholders and Obligations	

SA-9	3: Information Assets	1.1.2
	9: Policy	12.6
	9: Policy	8.1
3.6.1	6: Risk Acceptance, 9: Policy, 10: Evaluation & Refinement	12.10.1
	6: Risk Acceptance, 9: Policy, 10: Evaluation & Refinement	12.10.1
	10: Evaluation and Refinement	6.3.2 & 6.4.6
NIST SP 800-53r5	Trusted CI	PCI DSS 3.2.1
AC-2, AC-3, AC-6	4: Asset Classification, 8: Comprehensive Application, 15: Baseline Control Set	7.1 & 7.1.1
CM-11	4: Asset Classification, 8: Comprehensive Application, 15: Baseline Control Set	
AC-3, CM-7; NIST SP 800-46	8: Comprehensive Application, 15: Baseline Control Set	
CA-9, SC-4	15: Baseline Control Set	
	15: Baseline Control Set	1.1
RA-2	8: Comprehensive Application	2.4
NIST SP 800-53r5	Trusted CI	PCI DSS 3.2.1
IA-5(1)	15: Baseline Control Set	
IA-2, IA-5	14: External Resources, 15: Baseline Control Set	

	14: External Resources, 15: Baseline Control Set	
	15: Baseline Control Set	
AU-2(3), AU-6, AU-12, AC-6(9), CM-3, MA-2, MA-5, PE-3	15: Baseline Control Set	
NIST SP 800-53r5	Trusted CI	PCI DSS 3.2.1
	8: Comprehensive Application	2.2
	2: Stakeholders and Obligations, 9: Policy	
	15: Baseline Control Set	11.2
	10: Evaluation and Refinement	
	6: Risk Acceptance, 9: Policy	11.2.2
NIST SP 800-53r5	Trusted CI	PCI DSS 3.2.1
AC-4, MP-2, MP-4	15: Baseline Control Set	
MP-2, AC-19(5)	2: Stakeholders & Obligations, 15: Baseline Control Set	2.3 & 4.1
MP-2, AC-19(5)	2: Stakeholders & Obligations, 15: Baseline Control Set	8.2.1
CP-9, MP-5	15: Baseline Control Set	
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	
	9: Policy	9.6

	2: Stakeholders & Obligations, 9: Policy	6.4.2 & 7.1 & 7.1.1
NIST SP 800-53r5	Trusted CI	PCI DSS 3.2.1
	1: Mission Focus, 2: Stakeholders and Obligations	9.1
	2: Stakeholders and Obligations	
	2: Stakeholders and Obligations, 10: Evaluation & Refinement, 14: External Resources , 15: Baseline Control Set	
	9: Policy, 15: Baseline Control Set	
	15: Baseline Control Set	9.1.1
NIST SP 800-53r5	Trusted CI	PCI DSS 3.2.1
	15: Baseline Control Set	10.8
	15: Baseline Control Set	
	15: Baseline Control Set	
	15: Baseline Control Set	
	9: Policy	
NIST SP 800-53r5	Trusted CI	PCI DSS 3.2.1
	9: Policy	12.5.3
	9: Policy	12.5.3

	6: Risk Acceptance	
	13: Personnel, 14: External Resources	
	15: Baseline Control Set	
NIST SP 800-53r5	Trusted CI	PCI DSS 3.2.1
	1: Mission Focus, 9: Policy	
	8: Comprehensive Application, 9: Policy	
	9: Policy	12.1
NIST SP 800-53r5	Trusted CI	PCI DSS 3.2.1
	2: Stakeholders & Obligations, 8: Comprehensive Application, 9: Policy	12.8.1
	8: Comprehensive Application, 10: Evaluation & Refinement	12.8.2
	2: Stakeholders & Obligations, 9: Policy	12.8
	8: Comprehensive Application, 9: Policy, 15: Baseline Control Set	

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 who 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 Nebraska Mary 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 who 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
- Niranjana Davray, Colgate University
- Charles Escue, Indiana University
- Carl Flynn, Baylor University